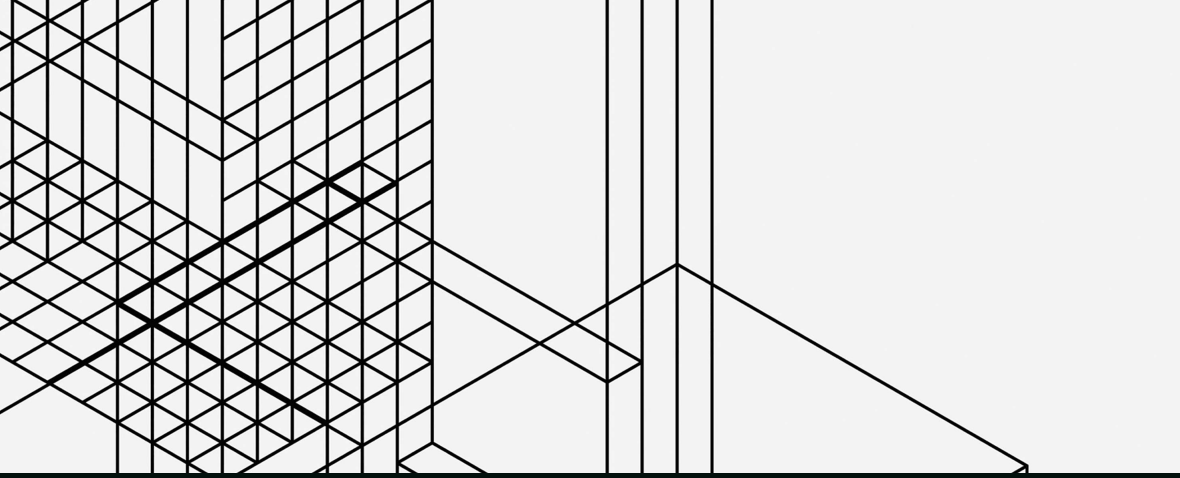
Intelligence Oversight in Times of Transnational Impunity

Didier Bigo, Emma Mc Cluskey, Félix Tréguer

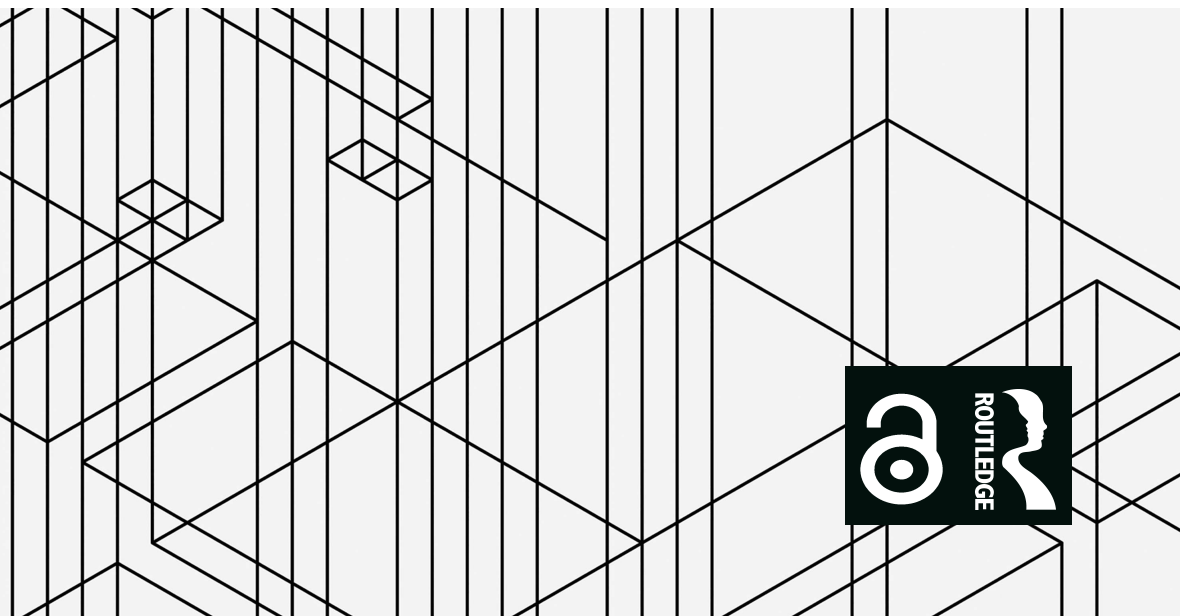


Routledge New Intelligence Studies

INTELLIGENCE OVERSIGHT IN TIMES OF TRANSNATIONAL IMPUNITY

WHO WILL WATCH THE WATCHERS?

Edited by
Didier Bigo, Emma Mc Cluskey, and Félix Tréguer



Intelligence Oversight in Times of Transnational Impunity

This book adopts a critical lens to look at the workings of Western intelligence and intelligence oversight over time and space.

Largely confined to the sub-field of intelligence studies, scholarly engagements with intelligence oversight have typically downplayed the violence carried out by secretive agencies. These studies have often served to justify weak oversight structures and promoted only marginal adaptations of policy frameworks in the wake of intelligence scandals. The essays gathered in this volume challenge the prevailing doxa in the academic field, adopting a critical lens to look at the workings of intelligence oversight in Europe and North America. Through chapters spanning across multiple disciplines – political sociology, history, and law – the book aims to recast intelligence oversight as acting in symbiosis with the legitimisation of the state's secret violence and the enactment of impunity, showing how intelligence actors practically navigate the legal and political constraints created by oversight frameworks and practices, for instance by developing transnational networks of interdependence. The book also explores inventive legal steps and human rights mechanisms aimed at bridging some of the most serious gaps in existing frameworks, drawing inspiration from recent policy developments in the international struggle against torture.

This book will be of much interest to students of intelligence studies, sociology, security studies, and international relations.

Didier Bigo is a professor of International Political Sociology at Sciences-Po Paris-CERI, France, and a part-time professor at King's College London, Department of War Studies. He is the author or editor of many books, including *Data Politics* (2019) and *Extraordinary Rendition* (2018), most recently.

Emma Mc Cluskey is a lecturer in Criminology at the University of Westminster, London. She is the author of *From Righteousness to Far Right; An Anthropological Rethinking of Critical Security Studies* (2019) and co-editor of *Security, Ethnography and Discourse* (2022).

Félix Tréguer is an associate researcher at the CNRS Center for Internet and Society and a former postdoctoral fellow for the GUARDINT project at CERI-Sciences Po. He is a founding member of La Quadrature du Net, an advocacy group dedicated to the defence of human rights in relation to digital technologies.

Routledge New Intelligence Studies

This book series offers a comprehensive and innovative account of contemporary intelligence. It gathers scholarship that takes the study of intelligence professionals and practices as the point of departure, and investigates its current configuration as a heterogeneous practice, overlapping with surveillance, counterterrorism, and broader definitions of security. In doing so, the series provides a renewed understanding of intelligence that conceptually and empirically challenges Intelligence Studies' traditional ontological and epistemological foundations.

Problematising Intelligence Studies
Towards a New Research Agenda
Edited by Hager Ben Jaffel and Sebastian Larsson

Intelligence Oversight in Times of Transnational Impunity
Who Will Watch the Watchers?
Edited by Didier Bigo, Emma Mc Cluskey, and Félix Tréguer

For more information about this series, please visit: https://www.routledge.com/Routledge-New-Intelligence-Studies/book-series/RNIS

Intelligence Oversight in Times of Transnational Impunity

Who Will Watch the Watchers?

Edited by Didier Bigo, Emma Mc Cluskey, and Félix Tréguer

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2024
by Routledge
4 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
605 Third Avenue, New York, NY 10158

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-1-032-40654-1 (hbk)
ISBN: 978-1-032-40655-8 (pbk)
ISBN: 978-1-003-35413-0 (ebk)

DOI: 10.4324/9781003354130

Typeset in Times New Roman
by MPS Limited, Dehradun

Contents

Acknowledgements

This book is the result of a research on "intelligence oversight in democratic spaces" based on a collaboration between three research national teams from Germany, the UK, and France. This research has been funded under the fifth Open Research Area call (Programme 2018 ORAR-0006-01). It started on the first of January 2019 and ended in December 2022. This collaborative research project called GUARDINT (who guards the guardians) had five partners based at King's College London, funded by the Economic and Social Research Council (ESCR), Sciences Po Paris, and University Jean Moulin Lyon 3, funded by the French National Research Agency (ANR), as well as Stiftung Neue Verantwortung and WZB (Berlin Social Science Centre) funded by the Deutsche Forschungsgemeinschaft (DFG). We would like to thank the French ANR for providing the funding necessary for making this book available in open access as a result of the GUARDINT project (project no. ANR-18-ORAR-0006-01).

The results and outputs of the projects – many of which appear in this book – are available at the project website: guardint.org. Although each work package received extensive contributions from all teams, each national team was responsible for specific work streams. The German team conducted a comparative analysis of different types of oversight, both in their official, institutionalised forms and when it is mediated through civil society actors (journalists, NGOs, etc.). It studied the different legal frameworks tied to intelligence oversight and researched best practices across Europe, assessing them in terms of effectiveness and accountability. Based on that work, it has developed the *Intelligence Oversight Index* (IOI).[1] The aim of this index is to measure and compare a variety of oversight practices in democratic countries. The British team has developed research on the conditions for trust between services and the notion of democratic regimes and practices. It has driven the effort on a report gathering case studies of the major political intelligence scandals and a timeline visualisation of the latter.[2] The French team has taken the lead on exploring the difficulties of effective democratic oversight, whether it is due to the concerted strategies of intelligence actors or the effect of socio-historical factors constraining the activity of parliamentarians, journalists or activist groups. The final report of the French team (CERI and Lyon3) tackled

the question of legitimacy in secret services coalitions among democracies and the need for transnational oversight.[3]

Synergies between the three teams were very important, and most of the results are the products of a cross-country and transdisciplinary approach. In addition to this book, and the publications of research reports and many articles, the website guardint.org contains an important tool for the future: the *Surveillance Oversight Database*. The database contains the main public legal texts and court decisions around intelligence oversight in France, Germany and the UK.[4] The project website has also a section on the building and use of an *Intelligence Oversight Index* (IOI).[5] The aim of this index is to measure and compare a variety of oversight practices in democratic countries. More specifically, the IOI is a tool for the systematic mapping of emerging practices of oversight and serves to expose oversight gaps across countries and over time.

As members of the GUARDINT project, we would like to thank all the intelligence oversight actors who made themselves available for interviews in the course of our research, as well as the research assistants and junior researchers who contributed greatly to the research. As editors of this book, we would also like to thank all authors, the directors of the New Intelligence Studies collection at Routledge, Hager Ben Jaffel and Sebastian Larsson.

Notes

1 https://survey.guardint.org/
2 https://guardint.org/timeline-of-intelligence-scandals/
3 The report is available on demand. Please contact toces@proton.me.
4 https://data.guardint.org/
5 https://survey.guardint.org/

Contributors

Claudia Aradau is a professor of International Politics in the Department of War Studies, King's College London. Her research has developed a critical political analysis of security practices. Among her publications are *Algorithmic Reason: The New Government of Self and Other* (co-authored with Tobias Blanke), *Politics of Catastrophe: Genealogies of the Unknown* (co-authored with Rens van Munster, 2011), and *Critical Security Methods: New Frameworks for Analysis* (co-authored with Rens van Munster, 2011).

Didier Bigo is a professor of "Sociologie Politique Internationale" (IPS) at Sciences Po Paris, a researcher at CERI, and was the leader of the French team of the ORA Guardint. He is also a research professor at the Department of war Studies King's College London and co-editor of the journal *Political Anthropological Research on International Social Sciences* (PARISS/ Brill). His research focuses on security professionals, surveillance, and democracy. See https://didierbigo.com

Elspeth Guild is ad personam Jean Monnet Professor in law at the College de Bruges and Emerita professor at Radboud University, Nijmegen, Netherlands. She is also a visiting professor at the College of Europe, Bruges and teaches at Sciences-Po Paris. She regularly advises EU institutions on migration and asylum-related matters and has written studies for the European Parliament on the European dimension of the 2016 refugee crisis, Euro-Mediterranean cooperation on migration. She also advises the Council of Europe and has written two Issue Papers for the Commissioner for Human Rights, one on the right to leave a country the other on criminalisation of migration.

Ronja Kniep is a research fellow in the research group "Politics of Digitalisation" at the WZB Berlin Social Science Center and a PhD candidate at the Freie Universität Berlin (FU). From 2019 until 2022, she has been a researcher in the international project "Intelligence networks and oversight: Who guards the guardians?" (GUARDINT) at the WZB. Her research focuses on digital politics, communications surveillance, transnational intelligence cooperation, and intelligence oversight.

Arnaud Kurze is an associate professor of Justice Studies at Montclair State University. His scholarship focuses on transitional justice in the post-Arab Spring world including human rights, social movements, and memory politics. He is currently working on an international digital archives collaboration called Project AROS, aimed at improving the visualisation of historical documents and data. He is widely published, including the co-authored book *Mapping Global Justice: Perspectives, Cases and Practice* and edited volume *New Critical Spaces in Transitional Justice: Gender, Art & Memory*. He is the recipient of numerous awards and fellowships, including the American Council on Learned Societies, Fulbright, the Library of Congress, and Sciences Po.

Emma Mc Cluskey is a lecturer in Criminology at the University of Westminster. She was previously a Teaching Fellow in International Relations at the Department of War Studies, King's College London. Her research has explored the relations between security, mobility, surveillance, and democracy. She is the author of *From Righteousness to Far Right: An Anthropological Rethinking of Critical Security Studies* and is co-editor in Chief of the bi-annual journal, *Political Anthropological Research on International Social Sciences* (PARISS).

Bernardino León Reyes is a PhD candidate and teaching associate at Sciences Po's Center for International Studies. He is an affiliated researcher at New York University (NYU) and was a team member of the European project GUARDINT ("Guardians of Intelligence"). He holds an MSc in International Relations Theory from the London School of Economics and an MSc in Anthropology of Politics, Violence and Crime from University College London. His research has been funded by a "La Caixa" Fellowship and the French National Research Agency (ANR). He is also a media contributor to newspapers like *EL PAÍS* or *Le Monde*.

Damien Rogers is an associate professor of International Relations and Security Studies at Massey University, New Zealand. He is author of *Postinternationalism and Small Arms Control: Theory, Politics, Security* (Ashgate 2009), *Law, Politics, and the Limits of Prosecuting Mass Atrocity* (Palgrave Macmillan 2017), and *Wars, Laws, Rights, and the Making of Global Insecurities* (Palgrave Macmillan 2022) and is editor of *Human Rights in War* (Springer 2022).

Félix Tréguer is an associate researcher at the CNRS Center for Internet and Society and a former postdoctoral fellow for the GUARDINT project at CERI-Sciences Po. His research blends political history and theory, law as well as media and technology studies to look at the political history of the Internet and computing, power practices like surveillance and censorship, the algorithmic governmentality of the public sphere, and more broadly the digital transformation of the state and of the security field. He is a

founding member of La Quadrature du Net, an advocacy group dedicated to the defence of human rights in relation to digital technologies.

Sophia Soares is a PhD researcher (torture prevention in refugee and asylum seeker detention situations) and a teacher of international law and human rights at the School of Law, University of Bristol. She is a research affiliate with the Refugee Law Initiative, University of London, and conducts regular prison monitoring visits as a Member of the Independent Monitoring Board of His Majesty's Prison Bristol. She has worked with the UN Refugee Agency in Malta and Geneva (on durable solutions and statelessness) and with the UK Home Office's resettlement programme for vulnerable refugees in the UK (on integration). She holds an LL.M. (Human Rights Law) and an LL.B. (Hons) (European Legal Studies).

François Thuillier has held numerous positions within the French security services, both operationally and in terms of foresight. He is now an associate researcher at the Centre d'étude sur les conflits, liberté et sécurité (CECLS – Paris) and author of *L'Europe du secret: mythes et réalité du renseignement politique interne* (La Documentation Française 2000), *La révolution antiterroriste* (Temps Présent 2019), as well as the *Homo Terrorismu*s (Temps Présent 2020).

Thorsten Wetzling heads Stiftung Neue Verantwortung's research on surveillance and democratic governance. He created the European Intelligence Oversight Network (EION) and had given testimony before the European Parliament and the Bundestag on intelligence legislation. He is a member of the advisory board on Europe/Transatlantic of the Heinrich Boell Foundation in Berlin and the scientific committee of the Cyber and Data Security Lab at the Vrije Universiteit Brussel (VUB).

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Introduction

Didier Bigo, Emma Mc Cluskey, and Félix Tréguer

Oversight, democracy, and control: Situating our transdisciplinary dialogue

Intelligence oversight remains an under-investigated object of study. When they exist, academic discussions on this topic are rather heterogeneous and take place in several spaces and within various interstices. Within the subfield of Intelligence Studies – one anchored in political science and international relations –, engagements with this topic have been occupying an interesting "in-between" space; an "add on" or afterthought. Conversations about oversight, more accurately described here as a repertoire of actions ranging from critical evaluation to hierarchical control via monitoring, are also a somewhat demarcated branch of legal studies. Assertions that oversight studies are generally driven by normative concerns largely obfuscate the history and intellectual trajectory of many of these conversations. Indeed, most debates around oversight tend to see the practice as a more applied ethical or practical question, which always involves trade-offs. The departure point is the idea of the supposed inherent and unresolved tension between intelligence and democratic control, where the view is taken that, as "we" cannot uninvent intelligence, it's better to regulate it.

This framing of oversight reveals its deep roots in the parochial mindset largely espoused by Intelligence Studies and a particular interpretation of political science. As Ben Jaffel, Hoffmann, Kearns, and Larsson have so clearly pointed out, Intelligence Studies – with its origins in Anglo-US policy making and a chiefly functionalist epistemology – has served to carefully choreograph the questions asked about intelligence practices, producing "theories for and not of intelligence".[1] This tradition of thought, we argue, overemphasises the effectiveness of state sovereignty in practice and fails to question its relevance today. An imaginary of a world in which state affairs – and in particular foreign affairs – are exempt from democratic rules and are left to opportunistic decisions is left intact, complete with all its misconceptions and fallacies. Such a framing typically downplays the violence carried out by secretive agencies and normalises the right for government authorities to surpass democracy and the rule of law if they deem it necessary.[2] Within

DOI: 10.4324/9781003354130-1

this imaginary, such "right" stems from the notion that a sovereign power has the final say in any quarrel occurring over its territory, and that it can use diplomacy and foreign affairs to extend this power on extraterritorial matters via anti-diplomatic techniques and influence.[3] Such an approach has so often served to justify weak oversight structures and delivered only marginal adaptations of policy frameworks in the wake of intelligence scandals. Overtime, it has helped build a misleading narrative of a linear progress towards the rule of law and often sustained blind analytical spots.

Conversations which speak to the more juridical dimensions of intelligence oversight are more noteworthy. It is partly due to the fact that the role of the courts in overseeing intelligence networks has in some respects become more significant since 9–11.[4] While long compliant with national security and state secrecy doctrines, judicial authorities across many countries have played an important role in defining new contours of the legal landscape, particularly lower courts in the US and the Court of Justice of the European Union.[5] In addition, the judicial arm of the Council of Europe, the European Court of Human Rights (ECHR), has emphasised that executive intelligence policy and oversight bodies are subject to public scrutiny.[6] Studies of the changing role of the judiciary in national contexts are plentiful. This is especially the case for Canada, which suffered from the scandals of the 2002 Maher Arar rendition to Syria and a decision by Judge Mosley on the subcontracting of Canadian Security Intelligence Service (CSIS) surveillance to Five Eyes partners, and the limited legislative accountability in this national context.[7] Such work has been very important in discussions on oversight as controlling and constraining intelligence practices. When framed as a "branch" of oversight, however, the judiciary is seen as the least able of all three branches to hold governments to account for national security activities as it is a reactive institution constrained by national political contexts.

Taking inspiration from these legal scholars, this book builds on some of their arguments. But while the contributions gathered in this volume recognise the achievements of oversight professionals in the juridical realm, our transdisciplinary dialogue attempts to open a broader space in which to interrogate the forms of democratic imaginaries at play within oversight policies and practices. Taking critical distance from a narrow idea of democracy as a technocratic and institutionalised idea represented through various policies,[8] our approach instead looks at how more radical forms of democracy, and more substantive critique and control of intelligence – have been constrained by the "common-sense" approaches put forth in much of the literature. Instead of working within disciplinary silos which take for granted all their respective baggage and blind spots, we have attempted to open a transdisciplinary space in which to analyse the transnational practices of various actors who challenge or implement what democratic regimes ought or ought not to do at any given time. We argue that such an approach allows for an understanding of historical trajectories and an examination of sociological processes by which different

oversight professionals set limits to the surveillance and violence of intelligence, or by which they fail to do so.

Drawing on recent developments in International Political Sociology (IPS), which has proposed a transdisciplinary perspective of analysing practices in transnational fields of power, we have thus sought to unpack institutions and policies of oversight and to differentiate the actors' logics and political judgements[9]. In doing so, we worked to connect Intelligence Studies to legal analysis of human rights, sociology, criminology, public administration, Surveillance Studies, and Security Studies in order to reveal their often contradictory set of assumptions and to work through them to propose alternatives. As the contributors to our volume come from a diversity of disciplines and academic backgrounds, their chapters reflect both the heterogeneity of methods and the plurality of empirical sites explored. We are united however by the willingness to pay attention to the systems of foreclosure and exclusion of certain forms of oversight, as well as the normalisation and enlargement of constraints to the democratic control of intelligence. Our aim is to enact a profound intervention into dominant studies of oversight of intelligence, which take for granted and thus legitimise secret state violence.

From scandals to oversight? Unpacking the practical limits of really existing intelligence oversight

In academia, detailed attention to the actors and practices of intelligence oversight very much remains an open project. But the few quantitative and qualitative studies of the world of institutional oversight tend to confirm that, in most cases, institutional oversight bodies fail to act as an independent and effective counter-power without the support of strong social movements and that of judicial and/or parliamentary bodies. Left to their own administrative logic, they tend either to pay lip service to the very agencies they are supposed to be keeping in check or to produce norms that have no real impact on the workings of such agencies.[10] And while it is true that in some countries, the institutionalisation of intelligence oversight has given way to a growing body of legal rules and formal mechanisms, alleviating a small part of the secrecy and legal limbo that shields the daily operations of intelligence agencies, it remains often partial and fragmented, subject to countless practical hurdles. Regional and transnational mechanisms of oversight may play a role if they can overpass the national barriers, but this is still a challenge (see Chapters 2, 6, 9, and 10).

These practical limits to national intelligence oversight are the products of decades of struggles around the secret violence of intelligence where, for the most part, institutionalised intelligence oversight has been designed and construed in a functionalist way as a means to boost the efficacy and legitimacy of intelligence agencies (on this point, see Chapter 1). In that respect, these limits reflect a contingent yet rather entrenched and problematic equilibrium. Of course, there is another side to the intelligence oversight story: the zealous whistleblower who seeks legal remedies against a shocking case of

systemic abuse they have witnessed, the investigative journalist who has gotten word of an affair, the human rights defenders bringing a case against their government before a supranational human rights court, etc. Through these critical engagements, the symbolic and physical violence of intelligence is exposed, its secret illegal activities and its "collusive transactions" with other sub-fields of power denounced. On occasions, these controversies may even escalate into full-blown scandals in which multiple fields become embroiled, that is when scandals turn into a national or international political crisis.

But historical research suggests that such conjunctures seldom translate into meaningful oversight reform. In two-dozen cases of scandals regarding intelligence surveillance over the past 60 years in the US, the UK, Germany, and France, such cases appear especially scarce.[11] The public policy of intelligence oversight is largely an inheritance of a series of "founding" scandals of the 70s when popular oppositions to digital surveillance as well as powerful and synchronised multi-sectoral mobilisations led to the edification of new norms and principles, such as data protection laws or the progressive case law of human rights courts. Certainly, some national differences – and the more or less advanced stage of democratisation processes – come to the fore when surveying past intelligence scandals. Germany stands largely apart from its counterparts in this regard. Not only can it be deemed the birthplace of modern-day intelligence accountability – with the establishment of the G10 commission to oversee intelligence surveillance and the strengthening of parliamentary oversight in response to the scandal unleashed in 1963 by Werner Pätsch, a clerk at the German domestic intelligence agency, the Bundesamt für Verfassungsschutz (BfV). But Germany also appears to be the country where the careers of intelligence officials and responsible ministers have been the most exposed in response to scandals (see Chapters 3 and 9).

In many cases though, intelligence scandals have failed to significantly affect the field of intelligence, to change its rules of the game (see e.g. Chapter 6). Even in the rare cases where intelligence officials are caught in the act of illegal activity and cannot escape sanctions, the servants of the reason of state are at the very least shown clemency (see Chapter 2). While their impact on democratic oversight is often not very significant, scandals nonetheless have the potential of evidencing changing alliances among power elites, sudden reversals in allegiances and power relations, and in this respect hold a deep heuristic value (see e.g. Chapters 4 and 5). One important object in structuring these changing relations is of course the law. The latter plays an ambivalent role: it can be used by challengers to scandalise intelligence (e.g. through human rights law and associated claims) but it also codifies rules and arrangements that are purveyors of legitimacy and normalisation for the forms of violence caused by intelligence. In fact, to a large extent, the codification of intelligence powers and of intelligence oversight has taken place with the assent – or sometimes even the public demands – of intelligence officials themselves as a way to secure their

prerogatives and sort out their dealings with other players, be they the political sphere, the courts, the media, private companies, or other intelligence agencies (see Chapter 7).

In theory, this means that overtime legal capital should be increasingly important for the intelligence field. But intelligence enjoys characteristics that make law easier to circumvent than in other bureaucratic settings: in a context marked with a deeply ingrained practice of secrecy, very few actors get to know how the interpretation of the rules takes place. Vague legal notions such as "national security", "international communications", "US persons", and the likes are thus open to considerable margins of interpretation. Obscure and apparently insignificant terms can be turned into huge loopholes that might survive for a long time, until yet another scandal will force judges to close them off. In other cases, oversight will be simply made impossible because of the dubious invocations of professional rules, such as the so-called "Third Party rule" often opposed to the attempts of oversight agencies to check the data shared with foreign partners. Finally, through new technologies and tactical moves – such as the forming of transnational guilds – intelligence professionals can also bypass existing oversight mechanisms (see Chapters 2 and 3).

In the face of these challenges, and for all the limitations of past efforts aimed at reining in intelligence abuse and related impunity, the work consisting in closing off pockets of illegality and creating the conditions for more democratic intelligence oversight remains a fundamental endeavour. This is why this book is also concerned with identifying key proposals to help remedy systemic oversight failure and impunity (Chapters 2, 6, 8, 9, and 10).

Presentation of the book's chapters

In order to provide a sense of the historical trajectories that have influenced the practices of various intelligence agencies in democracies and the limits they have placed on the use of secret violence and large-scale surveillance, the first three chapters examine the emergence of the idea of control by non-executive branches of government over the activities of secret services, both abroad and at home. They are inspired by an IPS approach based on relational and processual analytical frames inspired by Norbert Elias and Pierre Bourdieu. Thus, these chapters make use of the notions of "social space" and "field" to understand the relations between the different actors that resort to secret forms of violence and engage in intrusive surveillance – practices that are commissioned, or at least sanctioned, by the executive branches of governments identifying themselves as democracies and based on the separation of powers (Montesquieu, Payne). Traditionally, these actors were part of secret services. But now many other actors from other public administrations and private companies join in the enactment of such violence and of the forms of intrusive large-scale surveillance that target specific segments of the population. Far from being eternal or recent, such a field of practices, which

goes beyond legitimate violence that respects the rules of law, has specific origins that involve challenges and evolutions. A sociogenesis of intelligence oversight is thus necessary to shed light on present-day issues and understand how specific problems or configurations emerge – in this case, the problem of a legitimacy gap that necessitates the creation of surveillance mechanisms and organisations with a certain degree of independence.

In the first chapter, Félix Tréguer goes back to a key moment of intelligence oversight epitomised by the "Church Committee" in the US. Drawing on numerous archives, he revisits the traditional narrative of this so-called "birth of modern oversight", examining the various activities of the US services in relation to computerisation in the 1970s and the controversies that arose at the time. A series of scandals indeed gave rise to radical practices of, and demands for, control over the activities of the services. Bringing these largely forgotten histories to the fore, his sociogenesis challenges both the idea that the services have a discretionary right to be "outside the law" and enjoy a *de facto* impunity, as well as the narrative of some legal and intelligence scholars of an emergence and progress of democratic control from the Church Commission to the present day. Tréguer shows how the domestic surveillance of social movements and technologies of remote surveillance were already intertwined and contested, and how the institutional oversight mechanisms set up in response to these scandals stood in the way of demands for full transparency. Instead, these mechanisms were designed to be the keepers of secrets and the intermediaries between the intelligence field and the politicians, effectively toning down the contestation of intelligence that had been achieved through whistleblowing, advocacy, or litigation. Official oversight ended up securing a supposedly liberal political regime relying extensively on intelligence as a mode of government.

In the second chapter, Didier Bigo analyses how recent major transformations have affected this long-standing relationship between secret services and the institutions in charge of monitoring them. He insists on the conditions under which secret violence and surveillance have been carried out by democratic regimes through networked coalitions of different secret services and the lengthening of the chains of interdependence between the actors who manage suspicion, surveillance, prevention, and prediction. These coalitions are not simply an extension of the policies of US agencies, nor a series of national decisions to cooperate in the fight against a common evil. Instead, they cut across national policies, are highly asymmetrical and claim to have a global reach. The Five Eyes are no longer a sign of fair collaboration between Anglophone countries, if they ever were; they are now transnational guilds that act as nodes in different regional networks, linking numerous services that co-produce actionable information. This transnational dimension is central and is not a collection of national decisions and interests based on national security and sovereignty. Extraordinary rendition and remote torture, large-scale surveillance of Internet users around the world, and the proliferation of spying tools produced by private companies are examples of

this transversal dimension changing the scale of the traditional social universe of spying and counter-spying between state actors. With the combination of an ideology of preventive security based on suspicion and predictive claims with digital technologies that organise digital traces around correlations and trends, the number of people targeted by intelligence services has exploded, as has the number of "false positives". This has created a legitimacy gap that is now systemic. Denied by the politicians, it is increasingly recognised within the services themselves.

In the third chapter, Ronja Kniep illustrates and theorises the contemporary struggles of this transnational field by specifically analysing the collaboration of the Signals Intelligence (SIGINT) agencies disclosed by Edward Snowden in 2013, their relations with their counterparts in Germany, and the degree of participation and interdependence of the German secret service with the five eyes. She explains that a "code of silence" governs the collaboration between these SIGINT agencies and the implications it has for a democratic society, including the role of recently emerging reforms for oversight and judicial decisions. She insists on the relative autonomy of the SIGINT agencies and considers that they represent a field as such (differing in that regard from Didier Bigo). She also develops the complex relations between German Bundesnachrichtendienst (BND), the different oversight existing in Germany and the role of the courts in assessing these triangular relations. Using the recent legal reforms considering a different oversight for analysing the cooperation of the BND with the NSA, she shows that the Third Party rule is challenged, but under less than optimal conditions, to put it mildly. Finally, she examines the extent to which the practices and power relations of SIGINT have destabilised or circumvented democratic oversight.

As we can see, instead of analysing the secret services as institutional actors, one by one, and inside a national framework only, or only as a collaborative network, the approach in terms of field and habitus inherited from Bourdieusian sociology as well as its extension to the international via an approach of interstitials fields that are transversal to the different national scenes appears by far more powerful in explaining the state of play regarding intelligence agencies today. Following these same transversal lines, the second part of the book (Chapters 4–7) is devoted to the various strategies adopted by the secret services of the major countries in order to strengthen their legitimacy vis-à-vis their own domestic public, while at the same time increasing their cooperation with their foreign counterparts. In each case, the attention given to the specific characteristics of the sociology of statecraft, the trajectories of executive-judicial relations, as well as the presence or absence of strong social movements and NGOs willing and able to contest restrictions on fundamental rights, is crucial to decipher the strategies of differentiation of each actor in its national context, despite their structural interdependence.

In chapter four, Emma Mc Cluskey and Claudia Aradau look at the case of the UK, and in particular the strategies and tactics of its SIGINT agency, the Government Communications Headquarters (GCHQ). The UK has always

been very specific, and British governmental elites pride themselves on having a "culture of intelligence". The chapter reframes the originality of the British position and its ambition to be a "model" for others by revisiting the struggles for legitimacy, especially after scandals have politicised the issue of intelligence. The authors are very precise in describing how the terminologies of abuse and trust were used by the various protagonists and how they engaged in disputes over how to frame the logic of democratic oversight in relation to the necessity and effectiveness of the secret services. In doing so, they refuse to fall into the typology of notions that the actors try to claim and, on the contrary, propose to approach these different invocations of trust in the intelligence services historically, in order to show the struggles for the recovery of symbolic power through strategic communication that they use, contrasting different periods and, in the post-Snowden context, insisting on the recent mobilisation of "trust". The latter term, used in relation to intelligence and security services, limits the terrain of possible democratic oversight for civil society actors such as NGOs, rendering some practices of oversight actionable and others not.

In Chapter 5, Bernardino León Reyes further looks at civil society actors and their role in the controversies over the legitimacy of intelligence. Acting as a civic form of "oversight", an oversight from below, coalitions of journalists, activists, think tanks, and academics can force politicians to impose limits on intelligence powers instead of expanding them through legislation. These clusters of civil society players, whose role cannot be reduced to influencing the disputes between institutional actors, have historically played a crucial role in the adoption of past oversight reforms. But as León Reyes shows through a detailed ethnographic account, these three sectors of civil society are themselves fragmented by internal struggles and harbour different interests within their professions. As a result, they can clash both in terms of objectives and strategies, for example when some NGO decide to turn to a risky litigation strategy against the advice of its civil society partners, or when media editorialists decide to write Op-Eds delegitimising the very whistleblower that the same outlet's investigative journalists partner with. These internal struggles help explain the so-called "Snowden paradox", namely, the fact that the outrage of many civil society actors in the aftermath of Edward Snowden's resounding disclosures did not succeed, as politicians found a way out of the scandal by making minimal reforms aimed at reassuring the "public" rather than enacting effective controls.

In Chapter 6, Arnaud Kurze focuses on the US, which stands at the centre of a Global North coalition of intelligence agencies. Taking stock of the previous chapters, he examines in detail the diverse and multifaceted issues raised by US intelligence oversight as part of a larger effort to understand the continuing impunity of leaders in liberal democracies against a backdrop of persistent human rights abuses. He surveys the special power enjoyed by the various US agencies vis-à-vis other countries, the belief of US officials in a "special role" for their country on the world scene, their specific vision of

citizenship and constitutionalism, as well as US courts' doctrine of non-interference with presidential power. These factors explain the different attitudes to oversight and control, especially in comparison with Europe. Of course, the US has numerous oversight mechanisms, both institutionally and through civil society actors. But these are fragmented. According to Kurze, it would be possible to develop a conceptual framework for transversal democratic oversight bodies, both within the US and, more importantly, at the transnational scale (when transnational intelligence coalitions are involved). He argues that while oversight practices remain problematic, transversal legal advances in an increasing number of court cases could potentially prove to be powerful tools on which to build upon so as to promote accountability and fight impunity.

In Chapter 7, Damien Rogers highlights the specific case of New Zealand, a member of the Five-Eyes coalition network. As such, the country's intelligence agencies are well recognised in intelligence circles, but at the same time they have less ambition and fewer resources than their counterparts. The contrast with the US is of course striking, and it reflects the very deep asymmetry in this so-called networked cooperation. In New Zealand, intelligence professionals often act by proxy – more for others than for themselves. For this reason, their position in the national field of power is highly dependent on how they perform in the transnational guilds to which they belong. Rogers argues that, in this specific context, the oversight arrangements established over New Zealand's intelligence activities have been designed to facilitate an ongoing engagement with this transnational guild, offering criminal immunity to those intelligence professionals directly involved in illegal activities as well as political impunity to those professionals of politics who have direct responsibility for New Zealand's intelligence agencies. The author thus elegantly shows how the heterogeneity of the various stakeholders' positions in these ongoing struggles can be traced back to their positions in the relationships between the field of intelligence and that of politics, and how it is reflected in their strategies of legitimation.

All these contributions offer very specific analyses of a particular configurations of power at the national level, without being prisoners of methodological nationalism nor being blinded by faith in the dogma of the triptych of national security, interest, and sovereignty. They show empirically how the strategies of the actors, be they the intelligence agencies, supervisory bodies, politicians, or even the courts, are more accurately framed by the transnational chains of interdependence they have at international scale. The alliances and competitions do not – or at least not only – take place between nations. Crucially, they take place between different categories of guilds with different crafts. Sometimes craft solidarity takes precedence over national loyalties, and this can lead to disputes between some of the national services and their own politicians. Ideology about the choice of forms of security that some of these key actors seek to implement – in particular the extent to which they agree or disagree with preventive, predictive security – is also a key

marker of these struggles. And they are themselves the result of the willingness of various politicians to maximise their discretionary powers and the strength of the coalitions of actors who fight to limit those powers. Such cascades or chains of alliances and struggles will ultimately determine what is or is not accepted in a democratic society and will lead to the promotion or denial of forms of control that can limit this "futuristic" policy initiated by counter-terrorism, taking advantage of the simultaneous development of the Internet.

After these careful assessments of the structural limitations of national intelligence oversights, in a transnational context of impunity and claims for change, the last part of the book is more concerned with the possibilities for strengthening oversight, especially at the transnational scale. Certainly, the various contributors agree that it is not possible to enact democratic limits to secret violence and large-scale surveillance by drawing from a list of technical and organisational "recipes" restricted to national frames. There are already excellent juridical reports out there on how to make official oversight more independent, more effective, and more legitimate, but these are systematically ignored for political reasons stemming from the transnational landscape in which we live. It is rather up to the coalitions of actors engaged in controversies on intelligence to be more reflexive so as to change existing policies. To do so, however, they need to escape the current political imagination simultaneously overdetermined by the intelligence agencies and largely perpetuated by traditional Intelligence Studies in academia, as well as the agencies' strategic communications and the role of private companies in marketing surveillance and working to further the social acceptance of surveillance. If there is to be meaningful reform, it will be through serious alternatives that think outside the narrow political box.

While the functioning of some national oversight bodies is clearly far from optimal, a large part of their personnel is determined to implementing democratic changes. Many operational members of the services also judge that democracies have a necessity to distinguish themselves from authoritarian regimes by taking very seriously the question of legitimacy, and the different possibilities to create mechanisms of control over the services, even when they are organised in coalition. They insist on the importance of monitoring authorities who endowed with the capacity to challenge the executive privilege if necessary.

In Chapter 8, François Thuillier – who has worked both inside the French intelligence services and in research institutions – analyses the development of internal security policies in France. He agreed to talk to us about the various elements that he considers to be central for a change in policy. Drawing on his various reports and books on counter-terrorism – in which he contrasts the "Latin model" of anti-terrorism, based on the logic of criminal justice and intelligence-led policing around very specific targets, with the emergence of a counter-terrorist ideology coming from Anglophone countries and based on preventive, predictive technological beliefs –, Thuillier explains how the latter

was eventually introduced in France by a coalition of interests that seized the moment of the post-2015 bombings. He shows that it would not be so complicated to return to an efficient and more democratic logic that accepts both oversight by external institutions and the possibility for insiders to be protected as whistleblowers when they witness unacceptable behaviour by their colleagues. Such a model would be based on the recognition that freedom and equality mean that intelligence services cannot escape from democratic imperatives. According to the author, many agents would actually prefer clear boundaries to what they can do rather than loose and reductionist legal frameworks that are only useful to the politicians or higher-level intelligence officials who confuse their own interests with those of the "Republic".

In Chapter 9, Thorsten Wetzling, who heads the Berlin-based think-tank Stiftung Neue Verantwortung's research on surveillance and democratic governance and is the coordinator of the overall GUARDINT project, summarises the German team's work on intelligence oversight. Based on his extensive experience, he draws his own conclusions about what can be done, at least in Europe, to improve the way intelligence is overseen. As he explains, while European intelligence agencies are reaching new heights in terms of the depth of their multilateral cooperation, the level of cooperation between European intelligence oversight bodies remains far from as innovative nor advanced. This has widened the gap between the power of the agencies working together and in cooperation with the Five Eyes on the one hand, and the possibilities for real "oversight" of the various national oversight bodies on the other. However, Wetzling explains that some initiatives could easily alter the status quo if they were backed by a more serious political will. In order to give the positive momentum identified by Arnaud Kurze a chance to develop, he lays out a number of achievable benchmarks for closer cooperation between European intelligence oversight bodies.

In the last chapter, Chapter 10, Elspeth Guild and Sophia Soares contend that the ministries of interior, defence, as well as the cabinets of prime ministers and intelligence agencies themselves may continue their opposition to any democratic regulation, because of their doxa and interests in maintaining impunity in these matters, but both authors remind us that these actors' claims to represent the state should not be taken at face value. Civil society, part of the judiciary, foreign ministers, and many other actors who sincerely defend freedom of thought, freedom of movement, and respect for privacy can arguably appear more legitimate spokespersons of our governments claiming to be liberal democracies, considering that many years ago the latter signed international conventions and that they are now committed to respecting them. No one has forced them to do so. To give but one example, the authors examine how the pre-existing commitment of states to the prohibition of torture – contained in Article 7 of the International Covenant on Civil and Political Rights (ICCPR) and the subject of the 1984 Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment – has been given actual effect through the Optional Protocol to

the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment. These international arrangements now provide an increasingly effective system of monitoring, including international and national human rights actors. They suggest following this example to better protect the right to privacy, by strengthening it and limiting the ease with which it can be derogated from. It would be a real test that democratic states are not driven by security imperatives, but that they understand the need for a sense of limits – enforceable limits, and sanctions for those responsible for serious human rights violations.

These are just some of the possible steps to give intelligence oversight practical means to abide by human rights. They form part of the long-standing quest summed up by the Latin formula of the classic Roman poet Juvenal: *"Quis custodiet ipsos custodes?"* This sentence is often translated in English by the expression "watching the watchers". However, it loses part of its original meaning, and a more accurate translation would be: "who will keep me safe from my watchers?" Or "who will watch the watchers?" The latter encapsulates what we regard as the best maxim for thinking about the existence of secret services in democratic countries. As is so often the case, the formulation of the question is of central importance in the search for an answer.

Notes

1 Hager Ben Jaffel, Alvina Hoffmann, Oliver Kearns, and Sebastian Larsson, 'Toward Critical Approaches to Intelligence as a Social Phenomenon', *International Political Sociology*, 14, no. 3 (2020): 323–44.
2 Even though the term intelligence has become accepted in the academic world, some authors of this book prefer to insist on the main characteristic of the services, namely, *the use of secret violence and the surveillance* against groups of people often on the basis of non-individual suspicions. In this book, the term "secret services" is therefore used interchangeably with "intelligence services" to insist on the practices at work.
3 Most of the handbook of intelligence studies begin with this affirmation (see Chapter 6). Among the first scholars to have challenged the overall approach see James Der Derian, 'Anti-diplomacy, Intelligence Theory and Surveillance Practice', *Intelligence and National Security* 8, no. 3 (1993): 29–51.
4 Richard J. Aldrich, 'Global Intelligence Co-operation Versus Accountability: New Facets to an Old Problem', *Intelligence and National Security* 24, no. 1 (2009): 26–56.
5 Didier Bigo, Sergio Carrera, Nicholas Hernanz, and Amandine Scherrer, 'National Security and Secret Evidence in Legislation and before the Courts: Exploring the Challenges', Report, European Parliament, 10 December 2014. Iain Cameron, *National Security and the European Convention on Human Rights,* Brill, 2021. Edoardo Celeste, 'The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios', *European Constitutional Law Review* 15, no. 1 (2019): 134–57. Shirin Sinnar, 'Procedural Experimentation and National Security in the Courts', *California Law Review* 106, no. 4 (2018): 991–1060.
6 The Council of Europe is an international organisation founded in the wake of World War II to uphold human rights, democracy and the rule of law in Europe containing 46 member states.

7 See for example Craig Forcese and Kent Roach, 'Bridging the National Security Accountability Gap: A Three-Part System to Modernize Canada's Inadequate Review of National Security', Ottawa Faculty of Law Working Paper 2016-05 (2016).
8 Ronja Kniep et al., 'Towards Democratic Intelligence Oversight: Limits, Practices, Struggles', *Review of International Studies*, (16 March 2023): 1–21
9 Tuba Basaran, Didier Bigo, Emmanuel-Pierre Guittet, and R. B. J. Walker (eds), *International Political Sociology, Transversal Lines*, London Routledge, 2017.
10 Johnson for instance finds that 'a majority' of congressional overseers of intelligence in the United States have proved to be 'cheerleaders' for intelligence agencies. Loch K. Johnson, 'The Church Committee Investigation of 1975 and the Evolution of Modern Intelligence Accountability', Intelligence and National Security 23, no. 2 (1 April 2008): 198–225. Using Natural Language Processing and other qualitative methods, Kolaszyński and Stolicki find that members of the Polish parliamentary committee for intelligence oversight 'identify with the intelligence apparatus they are supposed to be overseeing.' Mateusz Kolaszyński and Dariusz Stolicki, 'Regulatory Capture of Intelligence Oversight Committees: A New Method Applied to the Polish Case', Available at SSRN, 2023.
11 Shen Ibrahimsadeh et al., 'Timeline of Intelligence Surveillance Scandals', GUARDINT Project Research Report, 1 December 2022, https://hal-sciencespo.archives-ouvertes.fr/hal-03952751.

References

Aldrich, Richard J. "Global intelligence Co-operation versus Accountability: New Facets to an Old Problem." *Intelligence and National Security* 24, no. 1 (2009): 26–56.

Basaran, Tuba, Didier Bigo, Emmanuel-Pierre Guittet, and R. B. J. Walker (Eds). *International Political Sociology, Transversal Lines*. London: Routledge, 2017.

Ben Jaffel, Hager, Alvina Hoffmann, Oliver Kearns, and Sebastian Larsson. "Toward Critical Approaches to Intelligence as a Social Phenomenon." *International Political Sociology* 14, no. 3 (2020): 323–344.

Bigo, Didier, Sergio Carrera, Nicholas Hernanz, and Amandine Scherrer. "National Security and Secret Evidence in Legislation and before the Courts: Exploring the Challenges." Report. Parlement européen, December 10, 2014. https://hal-sciencespo.archives-ouvertes.fr/hal-03429937.

Cameron, Iain. *National Security and the European Convention on Human Rights*. Brill, 2021.

Celeste, Edoardo. "The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios." *European Constitutional Law Review* 15, no. 1 (2019): 134–157.

Der Derian, James. "Anti-diplomacy, Intelligence Theory and Surveillance Practice." *Intelligence and National Security* 8, no. 3 (1993): 29–51.

Forcese, Craig, and Kent Roach. "Bridging the National Security Accountability Gap: A Three-Part System to Modernize Canada's Inadequate Review of National Security." Ottawa Faculty of Law Working Paper 2016-05 (2016).

Ibrahimsadeh, Shen et al. "Timeline of Intelligence Surveillance Scandals." GUARDINT Project Research Report, December 1, 2022. https://hal-sciencespo.archives-ouvertes.fr/hal-03952751.

Johnson, Loch K. "The Church Committee Investigation of 1975 and the Evolution of Modern Intelligence Accountability." *Intelligence and National Security* 23, no. 2 (April 1, 2008): 198–225.

Kniep, Ronja et al. "Towards Democratic Intelligence Oversight: Limits, Practices, Struggles." *Review of International Studies* (March 16, 2023): 1–21

Kolaszyński, Mateusz, and Dariusz Stolicki. "Regulatory Capture of Intelligence Oversight Committees: A New Method Applied to the Polish Case." Available at SSRN (2023). https://www.researchgate.net/publication/370599694_Regulatory_capture_of_intelligence_oversight_committees_A_new_method_applied_to_the_Polish_case

Sinnar, Shirin. "Procedural Experimentation and National Security in the Courts." *California Law Review* 106, no. 4 (2018): 991–1060.

1 From radical contention to deference

A sociogenesis of intelligence oversight in the United States (1967–1981)

Félix Tréguer

Introduction

A few years ago, taking stock of the controversies around intelligence surveillance sprung by the disclosures of NSA whistleblower Edward Snowden, I identified a so-called "Snowden Paradox."[1] The notion stemmed from the observation that, in many countries, scandals around the surveillance practices of intelligence agencies unleashed by Snowden had essentially led to the legalisation and the almost continuous extension of their surveillance capabilities.

But subsequent experience has led me to reconsider whether the Snowden case was in that regard a specific one. As an engaged researcher who, for the past decade, has been involved in sustained efforts by civil society actors aimed at litigating these legalisation processes in Europe, I have slowly come to the conviction that the engagement of human rights advocates in these issues has systematically failed. Sure, there are many cases where thanks to human rights advocacy, pockets of illegality have been adressed. But even in those few cases where the language of rights apparently prevailed over the reason of state, the "victories" of human rights defenders have actually come down to a growing proceduralisation of human rights, as lawmakers or courts have sought to compensate for the continuous extension of the breadth and depth of surveillance powers by enacting new transparency or oversight requirements. In the process, they have overlooked the fact that such "procedural fetishism"[2] comes at the expense of the substantive values that the rule of law is supposed to serve.

Rather than a "Snowden paradox," there seems to be a kind of script at play, a script which with few exceptions or variations keeps repeating itself across time and space when it comes to scandals around state surveillance. Drawing on the sociology of Pierre Bourdieu and taking stock of how his concepts can be mobilised in the context of sudden political changes,[3] that script can be summarised as follows. It first starts with a rapid expansion of the surveillance powers of intelligence agencies, typically in the context of security crises (or at least processes of securitisation). Possibly in partnership with other fields – especially the political field –, intelligence professionals resort to old habitus of surveillance in rather covert ways. If the security crisis

DOI: 10.4324/9781003354130-2

is significant enough, they might also be pressed to resort to new, innovative and/or particularly derogatory means, giving way to new configurations between intelligence and other fields.

The second stage of the script sees nascent insider debates around this expansion of surveillance powers scale up, leading to public denunciations and sudden processes of politicisation. Secret arrangements and practices are being brought to public attention through the media and the doxa of intelligence is contested. The controversy thus degenerates into a scandal, or sometimes even full-blown political crises when it affects the whole "metafield" of power. Such a scandal is characterised by a "synchronisation of the different fields' temporality and the harmonisation of their agenda," which involves a loss of autonomy of the intelligence field and gives rise to "unexpected changes in the configuration of alliances" within and across fields.[4] Routines and habitus are in part suspended, as actors must think more strategically.

Finally, the third and last stage of the script takes place when the scandal fades away, as the legitimacy of intelligence practice is re-established through negotiations and transactions between the field of intelligence and other fields of power. Most often, such processes of symbolic re-legitimation involve legal codification of the contentious surveillance powers as well as the creation of new oversight structures, which in theory decrease the autonomy of the intelligence field.

So far, so good: that script overall matches the descriptions of sociologists who have looked closely at the intelligence field in distinct national and historical contexts.[5] But this chapter seeks to connect this script to a grounded hypothesis, namely, the fact that rather than a victory of the rule of law, intelligence law and oversight structures inherited from past surveillance scandals actually work to shield intelligence against its critiques. To unpack this hypothesis, we need to approach intelligence agencies as bureaucratic organisations dedicated to the practice of the secret and illegitimate violence of the state – both physical and symbolic violence.[6] As such, intelligence agencies are particularly scandal prone: when the opacity and secrecy that normally shield the world of intelligence from scrutiny and preserve the liberal state's official truth are pierced, when previously unknown and inadmissible facts come to public light, a scandal is likely to take place, as various actors join or oppose denunciations of the really existing world of intelligence. As the key locus of illegal and illegitimate state action, the world of intelligence is thus bound to face recurrent legitimacy crises.

However, the legal frameworks developed around intelligence since the 1970s in Western liberal regimes to codify and regulate intelligence powers act as potent stabilisers in the event of scandals. They do so not only by reconciling the "abnormal" secret violence of the state with a reductionist version of the rule of law, giving it a legal façade; most crucially, and although they also arguably reinforce the dependence of intelligence on the dominant players in the legal and political fields, but they also form a set of social structures guaranteeing a large degree of autonomy for the intelligence field

against its most radical critiques. Construed in this way, most policies developed in the name of intelligence oversight thus reinforce the field of power – which is formed by dominant actors in various fields[7] – and the role that intelligence agencies play within it. They may also be said to over-determine the failure of anti-surveillance advocacy.

This chapter aims to explore this hypothesis. Against the tendency of a large part of Intelligence Studies to analyse the history of intelligence surveillance scandals and their aftermath as a linear and cumulative progress of the rule of law,[8] it seeks to frame the institutional response to intelligence scandals as a power tactic weakening opposition to state surveillance. In order to support this interpretation, I will be focusing on a seminal case: that of the US intelligence agencies confronting the social movements of the New Left in the 1960s and 1970s and the ensuing scandals which culminated in 1975, when the US Congress started paving the way for modern-day intelligence oversight.

The "Year of Intelligence" – an expression coined by the *New York Times* in February 1975 in reaction to the launch of committee investigations on Capitol Hill–[9] enjoys a particular status within Intelligence Studies, a sort of point of origin of this academic field, but also a moment when after a series of embarrassing revelations, modern oversight mechanisms were established to reconcile the US "intelligence community" with democratic accountability. Loch Johnson, a leading figure of Intelligence Studies and former staff member of the Church committee, for instance writes that "the Church Committee did nothing less than revolutionize America's attitudes toward intelligence supervision."[10] His point could have been even broader: post-1975 oversight arrangements around intelligence powers actually set a standard that other liberal regimes would follow, so that the developments in the US can be said to have had transnational repercussions.

But as this sociogenesis will show, the Church committee and the "Year of Intelligence" – which too many authors tend to analyse as a silo, failing to place it in a longer and older sequence of events – actually crystallised a set of normative assumptions about what proper intelligence oversight looks like. Ensuing regulations of intelligence drew a boundary around the world of intelligence, delimiting what could be said and what could not. They instituted "rules of the game" for intelligence oversight that protected the official truth and disqualified radical critiques. The "Year of Intelligence" was, in essence, a moment of democratic foreclosure.

Going back to what Bourdieu called "the clarity of beginnings," a sociogenesis of intelligence oversight in the US is "theoretically interesting because what will become taken-for-granted, and will therefore be destroyed in the invisibility of this taken-for-granted" was then "still conscious, still visible."[11] It can help us understand intelligence oversight as a legitimising device, an institutional shield protecting the field of intelligence by setting up a stage through which political struggles around intelligence abuse can be made more manageable. From that perspective, this case study may contribute to a genealogy of authoritarian liberalism, or more precisely of the neo-liberal reaction to the emancipation

movements of the 1960s.[12] It also places the "Snowden paradox" into a larger paradox, namely the fact that scandals and political crises, which various schools of constructivist political sociology typically address in terms of social transformation, can actually end up reinforcing the political *status quo*.

The chapter unfolds with the three-stage script outlined above while adopting an analytical lens grounded in field theory. Drawing on range of archival sources including declassified documents from intelligence agencies (particularly the Central Intelligence Agency (CIA)) and building on the work of intelligence historians, it starts by surveying the formidable extension of intelligence surveillance powers in the 1960s, the extent to which it focused on internal dissent, – in particular various social movements part of the "New Left"–, as well as the increasing resort to computers for surveillance purposes. It then shows how the growing power of intelligence and its strong influence on various social fields was "scandalised," becoming part of a widespread political crisis and leading to the creation of an "interstitial field" dedicated to intelligence oversight. Third, it follows the 1975 congressional investigations and the power plays of the executive branch, showing how intelligence reform eventually contributed to a form of institutionalised deference towards the world of intelligence.

Facing the New Left: The expansion of intelligence powers

It was a chilly night of late September 1968 when five sticks of dynamite went off and shattered the office of a CIA recruiting outpost nearby the campus of the University of Michigan in Ann Arbor.[13] Two weeks later, another bomb exploded, this time on campus, blasting the Institute of Science and Technology Building. Observers quickly concluded that the building had been targeted for its classified research into infrared sensory devices allegedly used to track guerillas around the world.[14] Later on, the bombings would be attributed to an anarchist and community-organising group called The White Panther Party, founded earlier that year in the city in solidarity with the Black Panthers.[15]

Since the mid-sixties, Ann Arbor had been one of the hotbeds of the New Left, the multi-faceted movement of student radicals, Black Power activists, feminists, revolutionary Marxists, and anarchists who gained prominence during the decade. "Everything was abuzz," remembers Bill Ayers, a leading local figure of the Students for a Democratic Society (SDS) and of the revolutionary organisation Weather Underground:

> Some of us organized in poor and working-class neighborhoods; some of us built counter-institutions (schools, clinics, work co-ops) to provide models for a new, more just society inside the decaying husk of the old; some of us built mobilizations against the war [in Vietnam]; some of us stopped US Marines and CIA recruiters on campus and exposed and opposed the war-related research that we thought was immoral and yet enriching our institutions; some of us fought for open admissions for Black students (…).[16]

After two decades of post-war conformism and ideological lockdown, capitalism and structural racism now faltered. The institutions embodying them – including corporations, the military, intelligence, law enforcement as well as science and technology – were subject to an intense critique and numerous assaults.

Intelligence as a "libertarian mode of repression"

In the midst of this generalising political crisis, intelligence agencies appeared as the single most important element of the state's response. Military intelligence as well as other agencies like the Department of Justice's Federal Bureau of Investigation (FBI) and the CIA vastly expanded the spying of American citizens and social movements deemed "subversive."

This response built on prior experience, as multiple security crises had already established intelligence agencies and their political espionage activities as a key pillar of the executive branch. The presidency of Franklin D. Roosevelt was a significant moment in this regard, with a potent domestic intelligence appearing as an acceptable – even necessary – tool of the modern liberal state. For many liberals of the late 1930s, in the build-up to the Second World War, the FBI's aggressive monitoring of groups on the margins of the political spectrum – in particular communist, fascist, and isolationist groups – was indeed seen as a natural and rights-preserving, all in all, a reasonable response compared with the outright repression of dissent through criminal penalties for seditious speech. In the words of Frank Donner, a long-time ACLU lawyer, law professor, and key actor in the controversies around intelligence and surveillance in the sixties and seventies, surveillance appeared as "a libertarian mode of repression," a democratic alternative to the more overtly authoritarian practices in place in other countries or advocated by some US conservatives – such as preventive arrests, deportations or forced internment.[17]

In partnership with private corporations, the federal government had brought "social security" to the population – e.g. with the Social Security Act of 1935.[18] It now sought to establish "national security" – an expression that took off in the late 1930s – both at home and abroad,[19] including by warding off threats to the socio-economic order and putting radical demands for socio-political reforms under the seemingly all-seeing eye of the FBI for targeted interventions and disruptions when necessary. Largely secret and illegal practices of political surveillance – wiretaps, mail-opening, infiltration, etc.– were thus established as one of the pillars of the US' own blend of "authoritarian liberalism," even though the process did not go without strong dissensions from isolated voices in the political and legal fields – e.g. from lawmakers wary that the FBI was turning into an "American Gestapo," or from the Supreme Court when legal backing for these surveillance powers was being sought.

After the adoption of the National Security Act in September 1947 which reorganised US military and intelligence agencies and led to the creation of

the CIA, the installation of the Cold War meant that the "red hunt" could continue unabated, despite the fact that actual communist influence in the US had by then be reduced to a minimum. Intelligence kept being seen as a much lesser evil than the despicable vigilantism practices by outrageous anti-communists like Senator Joseph McCarthy. By the 1950s, the FBI and the CIA enjoyed a broad-ranging support among power elites, a support that, according to political scientist William Keller, tended "to disable rational public debate and legislative oversight of the national security apparatus."[20]

That was particularly true of the US Congress, whose role in overseeing intelligence agencies was, in the words of historian Harry Howe Ransom, "best defined in the dictionary's other meaning of the word – 'overlooking' or the absence of careful attention." "Such attention," wrote Ransom in 1975, "was sporadic, unsystematic, incomplete, and at times casual."[21] Congress' watchdog function fell on the oversight subcommittees of the Armed Services and Appropriations Committees of both houses but, as Ransom sums up, "they appear to have been co-opted by the intelligence system and do not seem to function as independent critics."[22] While a minority congressmen did show some willingness to improve the system of oversight with more than 200 bills tabled to that end between 1947 and 1974, these were systematically rejected – often because of presidential pressure and despite the fact that those pushing for more oversight agreed to abide by rigorous secrecy.[23] With the Cold War and the nuclear age, deference to the executive branch and its secretive intelligence agencies increased, as illustrated by the accelerating decline in widely publicised congressional investigations of the administration from 1946 on.[24] Most people in the power elite seemed happy to allow the White House to centralise power by making unilateral decisions when it came to national security or even by withholding information from Congress.[25]

CIA director Allen Dulles and FBI director J. Edgar Hoover also successfully secured support through informal transactions with politicians on the Hill. Hoover was particularly successful in turning members of Congress into clients, imparting his rising symbolic capital with friendly politicians – especially those sitting on congressional anti-subversive committees which were heavily staffed with FBI agents.[26] Meanwhile, the propaganda flair of intelligence officials helped them secure public opinion and further immunise them from critics. A romanticised and heroic image of intelligence agents as Cold Warriors was conveyed by popular culture, through newspapers, magazines, films, and novels.[27] Cross-socialisation between intelligence and media power holders, who knew each other from their time together in Ivy League schools, was also key in securing public confidence in intelligence agencies.

In some cases, criticisms nevertheless surfaced and embarrassing leaks occasionally appeared in the media. But in the short-term, they mostly served to reinforce the consensus around intelligence agencies and to re-enact the rules of the game. For instance, after his dismissal by Kennedy in 1961 and the failure of the Bay of Pigs operation in Cuba, Dulles insisted that secrecy

was legitimate, saying he trusted Congress and was "confident" that the "American press" would stick to policy of "self-discipline" and "self-censorship" in reporting intelligence-related news.[28] Finally, the very power granted by intelligence collection – information gathering, disruptive tactics such as smearing campaigns, blackmail, harassment, etc. – also proved crucial when intelligence officials had to respond to occasional criticisms. These were used to threaten the few critical congressmen who dared to express concerns regarding the surveillance practices of the US government. Judges, including Supreme Court justices, also had dossiers in Hoover's files.[29] Surveillance of other power holders and political blackmail were thus another tool in the struggle for maintaining the autonomy of the intelligence field.

With such autonomy established, a deeply engrained habitus of surveillance came back to the fore when the US establishment entered the turbulent 60s. The crisis was due not only to the successes of the New Left, but also to what came to be perceived within the executive branch as an instance of intelligence failure. For the most part, intelligence officials failed to grasp the essence of the burgeoning unrest shaking the American socio-political order: their files were full of dossiers on ageing communists, and the new radical milieu – decentralised, self-organised, and evanescent – escaped most of their sensors.[30]

In 1965, as President Lyndon Johnson grew wary of the mounting opposition to the War in Vietnam and the growing interest of SDS and other student groups in anti-war activities, he instructed Hoover to look into it, hoping to find a connection between domestic radicalism and the Soviets.[31] But two years later, evidence of foreign influence was still elusive and the New Left was gaining strength. A frustrated president Johnson thus asked the CIA to investigate the peace movement. In November 1967, CIA director Richard Helms handed out his report, based on an "examination of the Agency's own files as well as access to data in the hands of the Federal Bureau of Investigation and the National Security Agency." Helms stated what should by then have become obvious, namely, that "the anti-war sentiment ha[d] taken root in separate sectors of the society having little else in common."[32] Something else was obvious: "we lack information on certain aspects of the movement." US intelligence was not even able to understand how these groups got their funds, much less find evidence of links to foreign embassies. In yet another sign of inter-agency rivalry, the director noted that such information "could only be met by levying requirements on the FBI, which we have now done."

Expanding and rationalising surveillance

In Fall of 1967, Johnson's advisers indeed told the FBI to find out "how and why demonstrators are so well organized," in essence giving them a blank check to expand surveillance measures as well as more disruptive tactics.[33] The FBI's COINTELPRO programme – started in 1956 to "increase factionalism, cause disruptions and win defections" within the weakened US

Communist Party – already covered the civil rights movement through wiretaps, informants, misinformation, and other such methods. In the summer of 1967, it was extended to so-called "Black Hate" groups, which included Martin Luther King and the Southern Christian Leadership Conference, and then to the white radicals of the New Left in October 1968.[34] As for the CIA, whose scope was supposed to be confined to foreign intelligence, it established new programmes focusing on the student movement.[35] From February 1967 onwards, the agency worked with college administrators and local law enforcement to identify activists (programme RESISTANCE). It developed a mail-opening capability directed at the foreign correspondence of persons and organisations placed on a watchlist (data which could then be shared with the FBI – programme HTLINGUAL) and mapped the alleged foreign collections of US radicals (project CHAOS). It even infiltrated peace groups on the pretence that they might pose a threat to security of CIA property and personnel (project MERRIMAC).[36]

The already powerful but still very secret National Security Agency (NSA) was also thrown into the mix and required by a Department of Defence directive to expand SHAMROCK, its secret programme for intercepting international telegraph traffic initially set-up with foreign intelligence purposes as a justification, to the anti-war and civil rights movements (a subprogramme that would be codenamed MINARET two years later). The FBI or the CIA would add items to the watchlist, and the NSA supplied them with the correspondence of the targets.[37] As for Army intelligence, in immediate response to the Black rebellions that had sparked in urban ghettos, it started setting up its "CONUS intel" programme in late 1967, with 1500 Army intelligence agents monitoring protest groups and events all over the country.[38] All this information-gathering effort ended up in the production of files of "subversive" people and organisations that were fed into the US Army Intelligence Command's Investigative Records Repository.[39] Between 1967 and 1970, the Army had files on "at least 100,000" US citizens.[40]

There was another significant change for the world of intelligence: the growing computerisation of surveillance. Amidst widespread popular fears of computers,[41] the early 60s had seen an explosion of experimental and practical intelligence applications spearheaded by agencies closely tied to the military-industrial complex such as the Pentagon's Advanced Research Projects Agency (ARPA).[42] Research projects increasingly looked into the possibility of modelling cognitive processes and predicting people's behaviours or developing simulations on the evolution of the international system. Whether abroad or at home, "enemies were no longer clearly identifiable," writes historian of technology Jens Wegener, and "there was a demand for tools that would help identify threats and make society more legible."[43] Computerised counter-insurgency systems were among them.

In 1962, sharing his "far-out thoughts on computers" in the CIA journal *Studies in Intelligence*, a CIA analyst wrote about the "rising optimism" and the prospect of seeing behavioural scientists using computers "to foretell the

behaviour of large groups of people."[44] The promise of prediction resurfaced in a much less "far-out" document, the 1965 "long-range plan" of the CIA.[45] Echoing today's often-heard rationale for computerisation of state surveillance, the document spoke of an "information explosion" and an ensuing "an analysis gap'" that could only be solved through computers – a technology bound to profoundly change the political economy of surveillance by allowing for the deeper, wider, seamless use of collected data. Despite the CIA's own admission of some delays in developing automated systems for intelligence analysis, the future seemed bright: current applications would "evolve into true analytical programs from which relationships among various types of events and data through the application of correlation techniques can be derived," "large data bases in analytical programs" would soon be used "to develop new processes having direct application to the substantive intelligence activities of the Agency," and "hopefully, predictive processes will evolve with time and experience."

But experts close to the intelligence field started to worry about the false promises of computers. In 1965, a Pentagon review team had been tasked with surveying "interagency goals for R&D in the processing of intelligence data." The report was damning for intelligence agencies, outlining their failure to drive such an R&D effort.[46] "Although millions of dollars and hundreds of man-years have been expended in applying automatic data processing," the report stressed, "the results to date have been disappointing." "One reason is the gap between 'the designer' of systems and the 'intelligence analysts' who do not know enough about each other's work and lack time to do so," but also the lack of networking of military and intelligence research with universities and the wider scientific community.[47] The committee argued that such organisational silos needed to be broken, calling on expanding trends dating back from the post-war years to create what historian Jens Rohde has called a "grey area" between academia and the national security state, one ripe for collusive transactions between intelligence as well as military agencies and the academic field.[48]

While such efforts got underway, law enforcement and intelligence agencies rushed to roll out more prosaic computer applications – although costly and resource-intensive ones – to alleviate a crisis of visibility. Flows of criminals, dissidents, and foreign agents moved across state lines and international borders, and computers could help track their history, whereabouts, and connections. In 1967, the FBI launched its National Crime Information Center (NCIC) to facilitate information sharing among the various layers of the US law enforcement system. Hoover boasted about it in magazines: "Only a nationwide computerised communications web, such as we will now be operating, can (…) bring crime prevention and control abreast of the criminal element's jet-age mobility," the director claimed.[49] In December of that year, in an attempt to predict future riots and decrease its reliance on the FBI, the DoJ employed student interns to organise cross-department files on individuals and events connected to civil disturbances.[50] Under the tenure of

Attorney General Ramsey Clark, the Inter-Division Information Unit (IDIU) quickly moved into a permanent programme and its files encoded in machine-readable formats. The automated "Subject File" for instance contained information on 26,000 individuals copied from the FBI's own data or from Military Intelligence, but also from other agencies. It could be queried to provide a listing of individuals by affiliation or location, providing up-to-date information to the Attorney General and serving to promote data-sharing and greater collaboration between the DoJ and the CIA.[51]

As part of its CHAOS surveillance programme, the CIA also set up a computer network relying on a time-sharing IBM 360/67 hosting the HYDRA database. Although HYDRA's index contained close to 300,000 names, actual files were only available to analysts for about 7,500 individuals and compiled data received from the FBI and CIA field stations around the world. HYDRA was lauded by CIA director Richard Helms as a way to exert greater control on access to information pertaining to this highly sensitive programme.[52] But it was only a small part of the agency's expanding computer projects. In 1969, an internal memo noted "automatic data processing [had] seen an average annual growth rate of some 30% over the years 1964–1968."[53] Although past programmes had been met with a "lack of results" and frustrations among its participants, many projects that had been in the "development stage" were allegedly "moving into production" and ready to expand.[54]

As for the US Army, it set out to encode the files of its Counterintelligence Records Information System (CRIS) into IBM punch cards to then index them into a computerised system for easy retrieval. As a congressional report would later find out, CRIS "was designed in such a way as to retrieve civil disturbance information rapidly and generate data and statistics."[55] The Army too alleged that the tool would be able "to assist the Continental Army Command in the prediction of civil disturbances which might result in the deployment or commitment of federal troops." Unsurprisingly, none of these sensitive processes of computerisation were subject to any meaningful oversight.

Scandals and disentanglement: The intelligence field faces radical oversight

The expansion of US intelligence apparatus as it reacted to New Left dissidence and its growing entanglement with other fields as a result of the mounting social crises soon gave way to denunciations and a series of scandals. At the turn of the 1960s, it led to cross-field synchronisation and greater fluidity across academia, the media as well as the political, legal, and the intelligence field itself. A new structure of opposition progressively took shape: transgressions associated with the disclosures of hitherto secret knowledge about the activities of intelligence agencies became valued stances anchored in the defence of the rule of law and democratic values. A rather radical "interstitial field" dedicated to intelligence oversight was thus formed – the concept of interstitial field being

used to refer to a "weak" social field with elusive boundaries "subject to contested authority among multiple fields"–[56], putting intelligence officials on the defensive.

Reactivating demands for academic autonomy

The first social space to reactivate open struggles against intelligence and the wider security field was academia. Tensions and attempts at maintaining the autonomy of the academic field against its growing subordination to security politics pre-existed, as illustrated for instance by the figure of Norbert Wiener, the father of cybernetics who blasted the use of his work for militaristic purposes.[57] But in the sixties, such denunciations became much more numerous and overt.

A founding moment in that regard was the scandal around project Camelot, the code name of a counter-insurgency programme started by the US Army in 1964 carried on by the Special Operations Research Office (SORO) at American University, a research centre largely funded by the CIA. Well-meaning social scientists – psychologists, sociologists, anthropologists, economists, etc. – had set out to study countries across the world but particularly in Latin America with the goal of assessing the effectiveness of US propaganda. For several of its key academic protagonists, project Camelot – an unclassified endeavour – was a way to bring pluralism to US foreign policy, creating a counter-power to national security hawks.[58] Still, one of its goals was to develop a computer system capable of automating the prediction of revolutions and insurgencies so as to allow for pre-emptive action, an objective that epitomised the fascination of US elites with anticipation. But when a consultant hired by the project reached out to Chilean social scientists to gauge their interest in participating in a study on their country, the latter made their suspicions of links to the US army public. The Chilean parliament launched an investigation into what was seen as a gross illustration of US imperialism.

Eventually, in June 1965 a source from the State Department leaked the whole story to the American press.[59] Amidst tensions between the State Department – embarrassed by the diplomatic consequences of a research project it did not know about –[60] and the Pentagon, Secretary of Defense McNamara decided to terminate Project Camelot. Officials in charge of "research defence" were quick to plead for more secrecy in the future so as to alleviate the risk of similar scandals reoccurring, but Congress' initial reaction was to cut DoD research funds for the 1966 budget.[61] Project Camelot appeared in a context where popular fears of the privacy-killing and dehumanising potential of data processing machines had become mainstream.[62] What is more, in 1965, SDS had gained momentum on campuses across the country with its anti-war teach-ins against the fast-pace militarisation of the conflict in Vietnam. The scandal thus formed part of a perfect storm that sparked of an intense politicisation of the links between universities and the national security state, re-activating structures of oppositions between social

scientists keen on operating in the "grey area" of social research and those who insisted that sciences needed to remain free of the influence of national security politics.

In this turbulent context, in February 1967, another development marked the beginning of an unprecedented wave of radical denunciations of US intelligence across the academic field. Thanks to a whistleblower, *Ramparts* magazine, created in 1962 and by then already the New Left's unofficial outlet, revealed that the CIA secretly funded the National Students Association (another NSA), a liberal-left organisation, as part of its world-wide anti-communist campaign.[63] In his editorial, *Ramparts*' executive editor Warren Hinckle framed the scoop as a "disturbing" but a "real example of the extent to which this government's secret intelligence apparatus has infiltrated presumably independent American institutions." *Ramparts*' outing of the CIA was not a first either: less than a year earlier, the magazine had disclosed the CIA's role in a programme established by Michigan State University to arm and train South Vietnamese security forces. The magazine had also hired William Turner, a former FBI agent dissatisfied with the agency whose first piece in the magazine denounced the FBI's failure to respond to civil rights violations in the South. *Ramparts*' staff knew they were under heavy surveillance.[64] Still, they were unrepentant: "Until the CIA's most elite operations are brought under the effective control of Congress," Hinckle's 1967 editorial went on, "you can consider this story a serial. We just don't think the CIA has any damn business co-opting Americans, and we plan to expose it every chance we get."

When the CIA learned of the upcoming publication, it reached out to the White House: "The CIA will probably be accused of improperly interfering in domestic affairs, and of manipulating and endangering innocent young people. The Administration will probably come under attack," warned a secret memo.[65] The reaction was planned well in advance of publication alongside the State Department to defuse the scandal,[66] President Johnson would appoint former Attorney General Nicholas Katzenbach to chair a blue-ribbon investigative commission (the latter eventually recommended that the CIA stop funding private voluntary organisations on US soil).[67] In spite of the administration's damage-control strategy, the CIA policy of openly recruiting on campuses was in trouble. "The Central Intelligence Agency has cancelled a two-day recruiting drive at Harvard, apparently to avoid student protest" wrote the main Harvard student newspaper in February.[68] Chapters of SDS even started occupying recruitment outposts. At Columbia University, "19 students sat-in outside an office where the CIA was conducting interviews. The recruiters, who were trapped inside for five hours, decided to discontinue their drive," a campus magazine reported.[69] And a few months later in Ann Arbor, two White Panthers activists went on to blow up one of such offices.

During those years, computer research was also directly attacked by student protestors who led campaigns and organised picket lines to call off

research projects involving computers.[70] Starting in the Fall of 1969, one of the most significant of these mobilisations struck at the heart of the grey area between the security and academic fields: Cambridge, Massachusetts, home of Harvard University and the Massachusetts Institute of Technology (MIT). A programme launched that year by J.C.R Licklider – one of the "founding fathers" of the Internet, who had moved from ARPA to the private sector and was then professor at MIT – and Ithiel de Sola Pool – professor of political science at MIT Center for International Studies – raised serious concerns. Project Cambridge was funded by ARPA with a giant budget of $7.6 million (about $56 million in 2020 dollars). The goal was to design various types of "data banks" and achieve what Licklider called "Robotised Data Analysis." There was a clear counter-insurgency goal to the project, whereby predictions would be derived from diverse sources including "public opinion polls from all countries," "archives on comparative communism," "files on the contemporary world communist movements," Youth movements," or "peasant attitudes and behaviour."[71]

Determined to stop the project, student protestors decided to occupy MIT's Center for International Studies. They circulated leaflets with a portrait picture of Ithiel de Sola Pool and "WANTED FOR MURDER" written underneath. Noam Chomsky joined the opposition,[72] while leading critical theorist Herbert Marcuse wrote a letter from California expressing his regret that he could not join the students for an event while voicing his support. Licklider tried in vain to reassure the demonstrators. He also asked guards posted in his lab to put extra locks on the outside doors as well as wood panelling over the doors leading to the computers.[73] After the controversy, Project Cambridge survived but evolved into something far less grandiose – things like the theoretical foundations for man-machine interactions and architectures for semantic databases.

While it is true that in the long run, the struggles of the academic field actually had an ambivalent effect, rendering research "more clandestine and more militarized" according to Joy Rohde,[74] for years to come, local fights against such projects took place and bans on CIA campus recruitment were adopted by University Boards.[75] A reversal in power dynamics was starting to take place: as the open interventions of US intelligence agencies in other fields were denounced, their political role and the form of political violence they fostered became more visible and exposed. Soon enough, new cross-field alliances would start taking shape to scandalise intelligence, establishing a *de facto* interstitial field dedicated to keeping intelligence agencies in check.

Cross-field coalitions scandalising intelligence

In January 1970, as the war in Vietnam and the debate on American imperialism tore the US apart, the *Washington Monthly* published a 13-page report by a PhD student at the Law School of Columbia University by the name of Christopher Pyle.[76] Born in 1939, Pyle had been a reserve officer and

after graduating from law school, he joined the Army Intelligence School in Baltimore as a young law professor from 1966 to 1968. Although progressively minded, he was anything but a radical. Still, now that he was out of military service, he needed to let the American public know about what he had witnessed: the illegal surveillance carried on under the CONUS Intel programme.

Pyle had contacted the *New York Times* to publish his piece but never heard back from the newspaper. Luckily for him, his *Washington Monthly* article eventually reached a far wider audience that the *Times* would have given that it was syndicated in more than forty other press outlets across the country. Pyle's disclosure of the CONUS Intel programme immediately led to the first full-fledged Congress inquiry into intelligence affairs, two years before the Watergate scandal and five years before the Church committee. "Back then, nobody had ever taken on the intelligence community, so there was some fear of the unknown," Pyle recalled.[77] Some had tried, only to be successfully blackmailed by Hoover. But in 1970, despite yet another rising wave of "law-and-order" politics and the election of Republican candidate Richard Nixon, the careful political manoeuvres of Congress as well as an already reduced autonomy of the intelligence field disrupted those tactics. Immediately after publishing his article, Pyle was contacted by Democratic Senator Sam Ervin from North Carolina, whom Pyle had heard about for his legalistic defence racial segregation. "Not an auspicious beginning," Pyle would comment years later. But he was convinced that the congressman could advance civil rights and that Ervin's conservative credentials and former experience as an Army officer would protect him. Still, through fear of generating backlash from Hoover or other powerful heads of intelligence agencies, the Ervin Committee left out any reference to "intelligence" in its title, instead choosing to call its hearings "Federal Data Banks, Computers, and the Bill of Rights."

Within a month of Pyle's first article on CONUS Intel, the Ervin Committee was holding hearings, with testimonies by prominent representatives of the computer industry or of ACLU, civil servants working on computerised law enforcement databases and most crucially former military intelligence agents. In his work for the committee, Pyle indeed benefited from the input of Army intelligence agents who reached out to share what they knew and tell him about other agents he might want to talk to. In total, he recruited more than 120 agents across the country to supply information about the programme, taking many precautions to protect his sources. In a telling illustration of the immense self-confidence of Army intelligence officials, the bulk of the CONUS programme was not even classified. This allowed Pyle and his sources to document it without breaking any law. In June of 1970, around the time Pyle was put on Nixon's infamous Enemies List, he published another groundbreaking article documenting how the Army had sought to cover-up the programme so as to reinstate it quietly.[78] It stressed that despite orders to destroy the illegal files the Army had

collected, Congress could not ascertain that these destruction orders had been respected.

The world of intelligence was really starting to feel the heat from Congress, the media, and the wider public opinion. With the CONUS scandal and the Ervin committee's disclosures all over the press,[79] it was increasingly on the defensive. Hoover told Bill Sullivan, his head of domestic intelligence operations, that he would not approve of Nixon's so-called Huston Plan to expand illegal surveillance programmes for fear of adverse publicity: "For years and years and years I have approved opening mail and other similar operations," Sullivan recalled the old director saying. Hoover now felt it was much too risky to put it on paper: "It is becoming more and more dangerous and we are apt to get caught."[80] The Army was on the same line, telling Nixon that it could not guarantee that the Huston plan would be immune from leaks.[81] Intelligence officials thus registered their loss of autonomy, and the Huston plan was consequently never really implemented.[82]

From then on, it must have felt like an avalanche of bad news for intelligence insiders: as the historian of US intelligence Rhodri Jeffreys-Jones writes, "one distressing story followed another."[83] The hearings held by the Ervin committee brought to light dozens of ongoing computerised intelligence-gathering operations across federal and local government agencies.[84] It forced the Secretary of Defence to pledge to rein in the Army's domestic surveillance activities and also further inscribed the issue of privacy onto the legislative agenda.[85] Then, in March 1971, as Pyle – who worked with ACLU's Frank Donner to bring an eventually unsuccessful case against CONUS Intel case – as well as other staff wrote the Ervin committee reports, suspicions that the Army's domestic surveillance programme included members of Congress, including Sam Ervin himself and other leading figures of the Democratic Party, were confirmed.[86] The same month, New Left activists who made themselves known as "Citizens' Commission to Investigate the FBI" broke into an FBI field office in Media, Pennsylvania, and gathered several dossiers, passing on the material to news agencies and thus exposing COINTELPRO for the first time.[87] Then in June, in a sign that it was now ready to assume a more adversarial posture, the *New York Times* published the first batch of classified documents known as the Pentagon Papers, offering a grim view of the US war in Vietnam. The whistleblower, Daniel Ellsberg, was a former State Department official and RAND analyst who taught at MIT and had started attending antiwar rallies two years earlier. The administration also tried to prevent the *New York Times* and other newspapers from further publishing the Pentagon Papers, only to see the Supreme Court enshrine the right to publish classified information.[88]

Judges too were now turning with greater resolve against the intelligence field and the rest of the executive branch. A year later, the Supreme Court issued another groundbreaking decision. The case centred on title III of the Omnibus Crime Control and Safe Streets Act of 1968 passed in reaction to the Black rebellions of the summer of 1967, which had marked the come-back

of a "law-and-order" discourse.[89] The statute provided a minimal legislative basis for court-approved and warrantless national security wiretaps. And the defendants were the White Panthers: after the explosion in the CIA outpost in 1968, the FBI had eventually figured out that people affiliated with the White Panther Party might be involved in the bombing. On 7 October 1969, three of them – John Sinclair, Pun Plamondon, and Jack Forrest – were indicted and charged with conspiring to bomb the CIA office. Pun was also charged with carrying out the bombing and immediately went underground, which led the FBI to place him on its "Ten Most Wanted" List until his arrest in July 1970. But in building the case, the FBI had made extensive use of wiretaps and bugs, with no court warrant but Attorney General John Mitchell's approval on the basis of the Safe Streets Act. The presiding district judge, Damon J. Keith, had rejected warrantless wiretapping as an abuse of executive power violating the Fourth Amendment. "We are a country of laws and not men," Keith wrote in his opinion. The Nixon administration appealed in June 1971, and the next year, the Supreme Court issued the unanimous decision – remembered as the Keith decision – declaring the warrantless wiretapping of US citizens unconstitutional, even in the name of national security.[90] From then on, many cases built by the FBI against radical factions of the New Left that used similar warrantless wiretaps as key evidence crumbled. The Keith case was a heavy blow to US intelligence.

Meanwhile, reacting to the revelations that some of its leading figures had been subject to intelligence surveillance by the Army, the Democratic Party's National Committee established a Planning Group on Intelligence and Security which worked in the subsequent months on a plan to reform the intelligence community and later came up with a quite radical list of demands, at least compared to what would eventually come out of the 1975 congressional investigations (quite ironically, Ithiel de Sola Pool was a member of the group, along with Christopher Pyle). Intended to influence the 1972 election cycle, these proposals included the creation of a "permanent Commission on Intelligence, Security, and Individual Rights that would serve as an independent public body with rights of full inquiry" and the power to "recommend changes in policy, legislation, and administration for all agencies engaged in domestic intelligence and security activities." Members of this oversight body would be nominated by the executive as well as Congress, and "possibly by civic professionals, and academic associations."[91] The Planning Group stressed that "indiscriminate data collection and inability to define priority targets contribute[d] to intelligence failures." It called for the protection of reporters' sources and the banning of government agents from masquerading as journalists. It argued for the automatic declassification of government documents after three years except for state secrets as defined by Congress with minimal discretion granted to the executive. Finally, it advocated the expansion of the 1966 Freedom of Information Act and the adoption of a data protection law, with the deletion of "all political dossiers on citizens neither charged nor convicted of criminal acts." The CIA was

obviously appalled by such proposals. When the book presenting the work of the Planning Group came out in 1972, an internal memo giving an overview of recent publications on the agency – a growing number of which were critical – concluded that "basically, all of the essays on foreign intelligence are hostile to CIA, especially its activities in the covert action field, with the exception of the essay by Dr. Ithiel de Sola Pool," wrote the author.[92]

And finally came Watergate. In February 1973, the Senate voted to create a select committee to investigate the burglary and bugging of the Democratic National Committee (DNC) headquarters in Washington. Having already successfully tackled the overreach of the executive branch, Sam Ervin was elected chairman. The committee would go on to document the concealment of wiretap records or the use of FBI intelligence against Nixon's political opponents.[93] All these examples illustrate how, after the radical protests and direct actions of student protestors on campuses, intelligence critiques co-ordinated across the political, legal, and media fields, reinforcing a growing divide in the field of power around the role of intelligence as the purveyor of the executive branch's illegal surveillance and violence. A growing number of intelligence agents soon joined the choir, adopting even more radical stances than Pyle or Ellsberg.

CounterSpy*: the radical campaign of former intelligence insiders*

In the summer of 1972, *Ramparts* magazine unleashed yet another storm over the world of intelligence. This time, the targeted agency was not the CIA, but the even more secretive National Security Agency. Its existence had already been disclosed in 1960, when two of its cryptographers defected to the USSR and held a press conference in Moscow.[94] Chastised as "sexual deviates" by officials in Washington, the two men for the first time shed light on the secretive world of signal intelligence. Still, ten years later, the NSA was still virtually unknown. But now, another NSA whistleblower dared going straight to the New Left's leading magazine to talk about the agency's global surveillance programmes: *Ramparts* ran an interview with Winslow Peck, a young former NSA analyst whose real name was Perry Fellwock:[95] "What we are dealing with is a highly bureaucratized, highly technological intelligence mission whose breadth and technological sophistication appear remarkable even in an age of imperial responsibilities and electronic wizardry," wrote the editor David Horowitz in the interview's introduction. Fellwock had worked on listening posts in Turkey, West Germany, and Vietnam, but he had grown disgusted with the war and joined the anti-war movement in San Diego. Going public with his experience at NSA was part of his activism. "What I wanted to do was stop the war, and I was willing to do anything possible to stop the war," Fellwock would later explain.[96]

After the publication of his interview in *Ramparts*, Fellwock met anti-war leader Rennie Davis who suggested that he pursue his crusade against intelligence abuse. In the Fall of 1972, along with a former Air Force intelligence

officer named Tim Butz who had also become an anti-war and anti-capitalist activist, 30-year-old Fellwock founded a new group: the Committee for Action/Research on the Intelligence Community, or CARIC.[97] Butz and Fellwock reached out to other former intelligence analysts asking them to share public-interest information on covert operations and surveillance. CARIC's activists had experience in groups as diverse as the Peoples Coalition for Peace and Justice, Vietnam Veterans Against the War, the National Peace Action Coalition, and Scientists and Engineers for Social and Political Action. They opened an office in Washington DC and in early 1973, came up with the first issue of *CounterSpy*, their new bulletin. *CounterSpy* was to "serve as an independent 'watchdog' on the government spy apparatus" and its rampant "technofascism," "an independent publicly sponsored source of analysis and information on the practices, organization, and objectives of US Intelligence."[98] Through its disclosures, CARIC would pierce through the opacity of intelligence, put it in the spotlight and create one scandal after the other. Its first issue revealed that Nixon's Committee for the Re-election of the President had hired George Washington University students to spy on anti-war protests – a scoop they passed on to the *Washington Post*.[99] It also alleged that the FBI had infiltrated right-wing groups in San Diego and worked with local police to disrupt non-violent groups on the Left. The issue came with a form intended for readers to fill out and send back asking all the intelligence agencies he or she had been part of, as a way to secure new sources.

In part to avoid legal repercussions, most of CARIC's output came from open sources. But it also mobilised insider knowledge that came as an embarrassment for the heads of intelligence. In May 1973, the second issue of *CounterSpy* charged the soon-to-be-appointed CIA director, William Colby, with lying to Congress about secret CIA programmes in Vietnam, demanding Colby's resignation: "CARIC feels that a man who had a career of directing assassination and torture programs can play no legitimate part in the US government. We encourage all citizens to write to their Congressional representative, the White House, and the Central Intelligence Agency to demand his resignation." With CARIC, secret knowledge and radical denunciations of intelligence were bundled together to exert pressure on institutional oversight. Again, observers at the CIA were worried. With a disdainful tone, an internal memo took notice of CARIC's demands for the resignation of the upcoming director and ended with the prediction that "like many 'bulletins' of this type, [*CounterSpy*] will probably run its course over a few issues and collapse for lack of funds" (actually, *CounterSpy* would not cease publication until 1984).[100] Still, the day after sending the memo, his author called again the office of the Deputy Director, warning that "one of the editors of that publication was on TV last night and said they gave documentation to the Senate Armed Services Committee in an attempt to block Colby's nomination." The connection of CARIC's staff to Congress was a liability for national security officials. Tim Butz had for instance testified before the Senate's Foreign Relations Committee to contradict the testimony of the Secretary of Defense

on the effect of bombings in South-East Asia. In that respect, *CounterSpy* embodied some of the most dangerous alliances possible between former intelligence insiders turned radical and members of the legislative branch.

The influence of CARIC further rose when a journalist from the *Village Voice* brought the group to the attention of writer Norman Mailer, also a leading anti-surveillance advocate of the time who had been separately working on a similar idea.[101] A few months later, Mailer's initiative and CARIC merged: the Organizing Committee for a Fifth Estate (abbreviated OC-5) actually became the fundraising arm boosted by Mailer's celebrity, while Fellwock and Butz worked on successive issues *CounterSpy*. The advisory board further established the credibility of *CounterSpy* by including former CIA agents turned whistleblowers, like Philip Agee or Victor Marchetti, but also ACLU policy officers and lawyers, including Franck Donner. The group became a focal point for investigative journalists wanting to dig up stories on intelligence and receive the help of former intelligence professionals. It launched campus tours to denounce the "technofascist tactics of 'Big Brother'" and seed local branches of the Fifth Estate, trying to build a distributed library of intelligence files. It sent representatives to radio shows to debate former intelligence officials, it spoke before labour groups or national security think tanks. It called its readers to expose CIA recruitments efforts in their community, but also to "organize coalitions to work for police budget cuts" or to use recent Freedom of Information laws to "request copies of the file they may have on you."[102] Later on, through open-source intelligence methods, they would even go on to publish the names of CIA operatives working in US embassies as a way to force the agency to withdraw them and therefore disrupt the covert action they might be engaged in.

Through its investigations and action research, *CounterSpy* was thus at the vanguard of the radical forms of oversight now being exerted on US intelligence. Spearheaded by student radicals, lawyers, congressmen, investigative journalists, even former members of the national security state like Pyle, Ellsberg, Butz, or Fellwock, the critique of the authoritarian drift of intelligence surveillance had become mainstream, marking an "extraordinary concentration of protesting voices" – one which, as historian Kaetren Mistry writes, "highlighted past abuses and framed contemporary crises in US politics and foreign affairs, created informal networks that fostered further revelations and contributed to growing dissenting narratives that were broadly leftist-progressive and anti-imperial in nature."[103] The impact of this radical contention against the intelligence field was real, although in many instances exposures were met with lies and cover-up stories. As a matter of fact, many controversial programmes were brought to an end. COINTELPRO was for instance discontinued in 1971 after the break-in of the Citizens' Commission to Investigate the FBI. CONUS Intel was also disbanded due to the Ervin committee's investigation – not without the Army trying to send the computerised files with the NSA through Arpanet, the Internet's forbearer.[104]

Internally, intelligence officials sought to prevent employee disaffection by

reaffirming the legality and legitimacy of their domestic surveillance activities, but at first it seemed like an uphill battle. In late 1972, just as *CounterSpy* was publishing its first issues, the CIA's Inspector General was voicing concerns that leaks from disaffected employees could lead to the disclosure of the CHAOS programme.[105] In early 1973, as the Watergate scandal was unfolding, the new CIA director James Schlesinger, preparing for the worst, decided to launch an internal investigation into all the "questionable activities" of the agency. William Colby, the head of covert operations who would replace Schlesinger in July, came up with a 693-page memo documenting the most controversial activities – which were internally called the "family jewels" – and included assassination plots, drug experiments, or the bugging of journalists. That summer, it was also decided to terminate the domestic component of the CHAOS programme, "not so much," as the Church reports would later note, "because it was thought to be illegal *per se,* as because the so-called 'flap potential' – the risk of embarrassment to the CIA that stemmed from its dubious legality was seen to outweigh its foreign intelligence and counter-intelligence value to the Agency."[106]

Despite these tactics of damage control, the damage was done. Trust in the intelligence agencies by the US public was at an all-time low, according to historian Kathryn Olmsted:

> The proportion of Americans who had a 'highly favourable' impression of the FBI had fallen from 84% in 1965 to 52% in 1973. In 1975, that figure dropped again to 37%. Although the Gallup organisation did not ask Americans about the relatively anonymous CIA before 1973, the agency at that time was held in lower esteem than the FBI: only 23% of Americans gave the CIA a highly favourable rating. In 1975, the figure fell to 14%. Among college students, the CIA was highly regarded by only 7%.[107]

The Church Committee and its aftermath: Fomenting consensus

In 1974, the impetus for a sweeping reform of US intelligence was strong. Congress was determined to act, and the political context seemed extremely favourable. Yet, over the next two years, the culmination of the political crises around the abuse of intelligence surveillance would give way to a multi-pronged strategy to re-legitimise the intelligence field, leading to what a historian of journalism has called a "new age of deference."[108]

Congress getting serious about intelligence oversight

The year 1974 was marked by important developments to rein in intelligence abuse. In the aftermath of Watergate, some members of Congress, including hawkish Republicans, launched investigations to look into the role that the CIA might have played in Watergate,[109] or established task forces to propose remedies to "the increasing incidence of unregulated, clandestine government surveillance based solely on administrative or executive authority."[110] Democratic

congress members also looked into the surveillance activities legitimised by "national security," requiring the collaboration of intelligence officials.[111]

In September of that year, Seymour Hersh, then a young *New York Times* journalist awarded with the Pulitzer Prize for his scoops on the My Lai massacre in Vietnam, revealed that the CIA and the State Department had lied to congress about their efforts to overthrow Salvador Allende in Chile.[112] This led to another round of uproar on Capitol Hill and several attempts to rein in covert operations. Mike Mansfield, Senate majority leader, took this opportunity to push for his long-time proposal to increase oversight of the CIA. A liberal Republican, Charles Mathias, cosponsored his initiative. Others followed suit. Among them, two liberal lawmakers, Senator James Abourezk and Representative Elizabeth Holzman, sought to ban all covert operations. For Abourezk, "since they are never going to tell us, the only real alternative is to take away their money, abolish their operations so that we shall never have that kind of immoral, illegal activity committed in the name of the American people."[113] But these radical parliamentarians could not find a majority to back their bills.

In the end, Congress settled on more moderate but still quite disruptive proposals to overhaul the Foreign Assistance Act. Adopted in reaction to disclosures of CIA covert operations in Chile and Southeast Asia, the provision directly targeted the core of presidential intelligence powers: the "Hughes-Ryan amendment" (named after its two Democratic sponsors) prohibited the use of funds for covert operations conducted abroad by the CIA or the Defence Department unless the President has issued an official "finding" that such operations were necessary to protect national security. The Amendment thus forbade the President to oppose "plausible deniability" for exposed covert action. But it also increased the number of congressional committees that had to be notified "in timely fashion" of these presidential findings, from four to six. The two new committees, the Senate Foreign Relations and the House Foreign Affairs Committees, were more liberal than the Committee on Appropriations or that on Armed Services, and keen to ensure that covert actions would not overstep on the prerogatives and policies of the State Department. By expanding the so-called "ring of secrecy," the amendment also made contentious covert operations much more likely to "leak" in the media.

Meanwhile, in a separate effort, the Senate's subcommittee on Intergovernmental Relations also held hearings on proposals to restructure legislative oversight of intelligence. In commenting on these efforts, Senator Edmund Muskie noted that:

> Time and again serious proposals – from Congress, from scholars and from Presidential task forces – have been met with little more than indifference. By our efforts here in the subcommittee, I hope we can bring an end to such studied neglect. The […] proposals now before this subcommittee would deal with intelligence oversight in various ways.

> But they all reflect a common concern: That today's intelligence agencies report to far too few people on far too little of their operation.[114]

Some of the proposals put forward by the DNC Planning Group on Intelligence and Security in the run-up to the 1972 presidential election were carried on by the 93rd Congress dominated by Democratic majorities. First, in late 1974, after the midterms, a lame-duck Congress managed to pass the Privacy Act, in part thanks to the dedication of Senator Sam Ervin. Creating a data protection framework for federal databases also significantly expanded the Freedom of Information Act. In particular, it granted citizens with the right to judicial review when target agencies refused to disclose requested documents. President Gerald Ford – who had been appointed Vice-President after the resignation of Spiro Agnew, making him to this day the only US president never to be elected – had vetoed the bill, contradicting his own pledge to run an "open government" because his administration – and intelligence agencies in particular – were concerned that intelligence secrets might be compromised. But in December 1974, both chambers of Congress voted to override Ford's veto.[115]

Congressional elections had been held in November 1974, that is three months into the term of Ford in the wake of Watergate and in the midst of rising inflation due to the 1973 oil crisis. The Democratic Party had substantially increased its majorities, winning the popular vote by a margin of 16.8 points. Many incoming members of Congress were young Democrats with little experience in federal politics. The "screaming Watergate babies," as historian Laura Kalman has referred to them,[116] had run campaigns attacking the "imperial presidency" embodied by Nixon, promising to bring a progressive agenda to Washington. In this context, a couple of days before Christmas Eve, just a week before these more adversarial representatives were supposed to arrive on Capitol Hill, the *New York Times* published another story by Seymour Hersh. The journalist had gotten hold of a copy of the CIA's 1973 report on controversial "family jewels" and was determined to carry his blend of adversarial journalism into the post-Watergate era by outing operation CHAOS. Covering the first page of the December 22nd issue of the *Times*, large prints read: "Huge C.I.A. operation reported in US against anti-war forces [and] other dissidents in Nixon Years."[117] The exposé went on to claim that, "directly violating its charter" barring it from operating on US soil, the CIA had "conducted a massive, illegal domestic intelligence operation during the Nixon administration against the anti-war movement and other dissident groups." Illegal break-ins, wiretaps, and mail openings were all mentioned in the article.

In some ways, Hersh's revelations about the CIA's domestic spying were old news given that the CHAOS programme had been discontinued in 1973. But after years of repeated controversies, the intelligence establishment's support base among political and media elites was stretched thin. Even Ford seemed at first determined to not get the White House tainted by the scandal,

considering that it was up to the CIA Director William Colby to deal with it. But when he got back from his skiing holidays after New Year's Eve, Ford convened a meeting with Colby and his White House Staff and was made aware of the existence of the "family jewels report." Listening to the advice of his staff, he chose to launch a blue-ribbon commission headed by the Vice-President, Nelson Rockefeller, to investigate Hersh's allegations.[118]

Although an internal White House memo had warned against the potential of this commission to appear as an attempt to "whitewash the problem," Richard "Dick" Cheney, then Deputy White House Chief of Staff, would later admit that the strategy was deliberately meant to head off any "congressional efforts to further encroach on the executive branch."[119] With the Vice-President as its head and other pro-intelligence, pro-secrecy members like former California governor Ronald Reagan,[120] the move was indeed widely seen as a way to undercut any aggressive investigation by Congress and alleviate the risk of further leaks. It indicated that Ford and his staff were determined, as the president put it, to "restore the rightful prerogatives of the presidency under the constitutional system," which meant keeping the congressional investigators from exerting a determining influence on intelligence policy.[121]

However, the initial strategy of containing the controversy to the CIA ran into hurdles when the *Washington Post* revealed that the recently defunct J. Edgar Hoover had kept personal records on congressmen.[122] Other damning articles about the NSA and military intelligence came out in January and early March.[123] The new disclosures would force the congressional inquiries to widen their scope to the whole "intelligence community." "The Year of Intelligence" was thus launched.

A tale of two investigations

In her detailed account of the power dynamics at play around the creation of the Church committee and its equivalent at the House of Representatives, Kathryn Olmsted has shown how much the approach of House and Senate Democrats diverged. During the debate on the resolution to create a special committee – passed on 27 January 1975 –, senators insisted on the need to strengthen "the confidence of the people" in US intelligence. The priority of Democratic senators, it seems, was to reassure Republicans that they were not "out to destroy the CIA," as Senator John Pastore stressed during the debate. House Democrats, in contrast, took a much more adversarial position, insisting on the need for a "thorough house cleaning." A leading CIA critic, representative Michael Harrington, for instance contended that the country's security "depends just as much on the maintenance of the rule of law as it does on the preservation of diplomatic secrets."[124]

Both chambers eventually voted to launch their investigations, which unfolded over the following months alongside a separate investigation into the growing use of technology for state surveillance purposes.[125] None of the

committees' chairmen were first choices. Representative Otis Pike was a moderate Democrat appointed chairman only in July 1975 after it was revealed that the first chairman, Lucien Nedzi, had known about the CIA "family jewels" report and had failed to report it to fellow committee members.[126] As for the senator from Idaho Frank Church, who had recently conducted a sensitive investigation on the role of mutlinational corporations in US foreign relations and their secret cooperation with the CIA, he was appointed because Philip Hart was ill with cancer.

Both investigations offered an unprecedented deep-dive into the realm of intelligence, including not only the CIA and the FBI, but also the NSA, the Internal Revenue Service, and the Defense Intelligence Agency. Both committees unearthed many hitherto unknown cases of abuse (e.g. the FBI's blackmailing of Martin Luther King), secret budgets funding sensitive intelligence operations, and serious gaps in executive oversight and chains of command. Still, the strong differences that had presided over the creation of both committees persisted. Where Church was willing to compromise with the executive branch, framing abuse as a consequence of "rogue elephants" rather than systemic abuse, Pike would stick to a more adversarial line, refusing to agree to many procedures that Church had accepted, declining to look at memos and briefs that the full committee could not see, and resisting any private consultation with the executive branch. In total, the Pike Committee held 54 public hearings, or more than three times the number held by the Church Committee.[127] Where Church pursued a theory of "aberrations" and episodic abuses, Pike looked for the systemic factors explaining such abuse. Half-a-year into both investigations, a CIA official quoted by Seymour Hersh in an article summed it up in this way: "The House goes after the arteries, while the Senate goes after the capillaries."[128]

This led the White House to adopt a differential policy towards the committees. Although it pressured the Church committee in many ways, the Ford administration was more inclined to work with the "gentler" of the two investigations. It resisted the Pike Committee in much fiercer ways, and overall tried to play public opinion against Congress, wrongly accusing both committees of leaking or even losing vital information.[129] These manoeuvres of the executive, as well as its way of framing its response to the recommendations of the Rockefeller Commission which handed out its report on the CIA in June 1975,[130] proved to be key in crippling the political ability of both investigations to push for meaningful reforms. From September 1975 onwards, all executive responses to the congressional inquiries were handled by the Intelligence Coordinating Group (ICG). The group, composed of senior officials including Secretary of State Henry Kissinger and Secretary of Defense James Schlesinger, met in the situation room each morning to roll-out a proactive strategy aimed at imposing the executive's own agenda.[131] "We should not view this simply as a 'damage control' operation but, rather, we should seize the initiative and attempt to make something positive out of

this," wrote the main staff of the group in an internal memo.[132] Reform was unavoidable, but the executive should be leading the manoeuvre so as to ensure that such reforms could secure the activities of US intelligence. To roll-out this strategy, the ICG also aimed at influencing the media by placing Op-Eds by administration officials and friendly outsiders. It quickly paid-off: by Fall of 1975, the public support for wide-ranging intelligence reform was waning. CIA officials quoted in the press "expressed surprise at what they said was the inability of the Senate committee (…) to generate public support for its inquiry."[133]

The role of the mainstream media and its willingness to move on from an adversarial posture and side with the executive branch was key in the growing backlash against investigators. Olmsted's central claim is that after the Watergate and resignation of Richard Nixon, the media became "nervous about its newfound power, fearful of a public and governmental backlash, and receptive to government requests for self-censorship."[134] Realising that attacking the government could entail big consequences, many editors and journalists felt like it was the time to focus on "nation-healing stories" – an expression coined by producers at CBS.[135] In other words, most of the Fourth Estate was now keen on restoring confidence in the government, and made that position known through editorials by criticising the committees – Pike's in particular. The representative was accused in the *Tulsa Daily World* of being a "spoiled child" and a "small-mined egoist" for putting pressure on the executive to release State Department memos and threatening to cite Henry Kissinger for contempt of Congress.[136] The *New York Times* political columnist and former Nixon speechwriter William Safire also lashed at Pike for "painting everything in black and white" and making "our Government helpless and contemptible."[137]

And then there was the murder of Richard Welch in Athens on 23 December 1975, shot by a Marxist revolutionary group. A CIA station chief, Welch had been previously identified by a 1968 book – a "who's who" of the CIA – published by two Soviet-bloc intelligence agencies. More recently, the Peruvian press had revealed Welch's name: he was the CIA station chief in Lima before being sent to Athens. That later disclosure had been reproduced in the Winter 1975 issue of *CounterSpy* as part of its advocacy of open-source investigative methods to out CIA agents. Welch's house in Athens was that used by his two predecessors, so that the CIA could have been blamed for not making greater efforts at hiding the identity of its officials. But Welch's burial as a national hero in Washington gave the CIA and the White House an opportunity to play out a public relations strategy of accusing *CounterSpy* and his associates of being responsible for Welch's death. The accusation of "naming names" indirectly extended to the Church committee, because of its willingness to reproduce in its reports the names of CIA agents that had formerly been disclosed in the US press. Church would later comment that the Welch murder had been a "stage-managed" event, and that "an attempt was made to lay the responsibility on the congressional investigation" so as

to "close down the investigation as soon as possible and to try to keep control of whatever remedies were sought."[138]

The investigations indeed drew to a close in early 1976. The Pike Committee's more adversarial stance and a struggle with the executive over the classification of its report's content led the House of Representatives to vote, by a large majority, against its publication. Bipartisan congressional support of wide-ranging intelligence oversight had lapsed, and most representatives now sided with the White House' claims that the committee had gone too far in disclosing intelligence secrets. The report was thus held confidential until CBS reporter Daniel Schorr and journalists at the *New York Times* got a hold of it.[139] It eventually leaked in February 1976 when the New York-based magazine *Village Voice* decided to print it. Everybody could now read Pike's recommendation to abolish the Defense Intelligence Agency and the Internal Security division of the FBI, the request of court orders for FBI infiltration of American organisations, as well as the disclosing of the total budgets of intelligence agencies.[140] Alas, the debate that took place did not relate so much to the substance of the report as to how it had been made public. Daniel Schorr was rapidly identified as the source of this publication by the *Washington Post* and was then called to testify before Congress. Refusing to identify his source alleging First Amendment protection and abandoned by his superiors, Schorr eventually had to resign from his job at CBS.

As for the Church committee's series of reports, they were released in April 1976, as senator Franck Church rushed to the campaign trail in an attempt to secure his party's nomination for the upcoming presidential election, racing around the country with other contenders in the Democratic primaries. The tone of the report already gave a sense of the change of mood in Washington over intelligence issues, harbouring a somewhat benevolent tone towards intelligence agencies – stressing for instance that there was now "an awareness on the part of many citizens that a national intelligence system is a permanent and necessary component of our government."[141] "The system's value to the country," the report continued, "has been proven and it will be needed for the foreseeable future." Overall, the idea was to boost congressional oversight by clarifying the legal basis for the different practices of US intelligence, while largely deferring to executive secrecy. Hence the report pleaded for the creation of a permanent intelligence oversight committee – a proposal that would become the committee's main legacy –, coming out strongly against the Hughes-Ryan amendment and the wide disclosure obligations that it had set forth for covert operations.[142] The Church reports also carried on some of the proposals of the 1972 DNC Planning Group or those recently put forward by the ACLU,[143] leaving aside the most radical ones (e.g. automatic declassification, partial appointment of intelligence overseers by "civil professionals," etc.). It for instance recommended that an Intelligence Oversight Board be established with the Attorney General as a statutory member responsible for ensuring the conformity of intelligence activities with the rule

of law. The Church committee also called on Congress to draft detailed legislative charters laying out the duties, powers, and responsibilities for the main agencies, defending the crucial principle that authorisations for domestic surveillance should be subject to court approval and conditioned on the existence of prior suspicion that such surveillance could document criminal activity in the field of terrorism or espionage, rather than mere "subversive activities."[144] Finally, it was not ignorant of the risk entailed by a growing process of computerisation, calling for "restraints that not only cure past problems but anticipate and prevent the future misuse of technology" to ward off the risk of a "big brother government."[145]

Taken altogether, these recommendations were significant. But by the time of their publication, as the *Washington Post* noted, "the impetus for reform appears to be only a shadow of what it was last year."[146] And indeed, the few recommendations actually enacted were those that fit with the executive branch's strategy for re-legitimising intelligence.

Ensuing reforms: the foreclosure of democratic control over intelligence

In February 1976, that is a few weeks before the publication of the Church reports, Ford had undercut most of the Senate committee's recommendations by making a live speech announcing watered-down versions of it. The executive needed to make concessions, but these had to be minimal. And above all, they needed to reinstate secrecy as an effective boundary between intelligence outsiders and insiders so as to protect the autonomy of the intelligence field and the discretion of the executive branch in defining intelligence policy.

The bulk of the executive's own intelligence reform lied in executive order n° 11905, the first detailed and public legal text laying out the powers and duties of intelligence agencies. Through it, Ford imposed a few restrictions on intelligence agencies, including a ban on assassinations as an instrument of foreign policy (the latter being framed in an ambiguous way that still left the option open).[147] A new Intelligence Oversight Board was also established at the White House, with the duty to report to the Attorney General "any activities that raise serious questions about legality" (rather than making the Attorney General a statutory member of the board like the DNC and the Church committee had proposed). Instead of detailed legislative charters, the executive order called on the Attorney General to issue "guidelines" framing the powers of the FBI, refusing to ban the detection and prevention of mere "subversion."[148] Ford also expressed support for a proposal that had been floating since the Keith decision and taken up by Congress to create what he called "a special procedure for seeking a judicial warrant authorizing the use of electronic surveillance in the US for foreign intelligence purposes" – announcing the secret court at the heart of what would become the Foreign Intelligence Surveillance Act of 1978.[149] Importantly, he also called entrenching secrecy as a means to protect intelligence autonomy, for instance through a new law criminalising the disclosures of state secrets or a joint

congressional committee on intelligence oversight: "The more committees and subcommittees dealing with highly sensitive secrets," Ford said in his address, "the greater the risks of disclosure."[150]

In the aftermath of these announcements, intelligence officials – who had feared, quite rightly considering the tepid response from the mainstream press,[151] that these executive reforms would be open to charges of making only cosmetic changes – successfully pressured Congress to fight back against more rigorous legislation. Proposed amendments to the Privacy Act aimed at ensuring that intelligence agencies notified any person that had been targeted by the COINTELPRO or CHAOS programmes were thus defeated.[152] Instead, the debate rapidly shifted to the proposals that most immediately served to shield intelligence from radical critics.

First, in May 1976, at the urge of the Church committee and the White House, the Senate voted to create a Permanent Select Committee on Intelligence responsible for authorising expenditures for intelligence-related activities. It almost failed to pass when it was put to vote on the Senate floor despite having been the focus of extensive debate in both chambers in 1975.[153] It took the House one year to come to the same result, and both committees were added to the list of those to receive notice of covert actions under the Hughes-Ryan amendment. Representative Michael Harrington, author of the 1975 resolution establishing the Pike Committee, called these new permanent committees a "sham of oversight,"[154] knowing that, rather than boosting oversight, their main purpose was to eventually better protect executive secrets.[155] As a journalist correctly summed up after the creation of the Senate Permanent Select Committee on Intelligence:

> Some hope the Senate's creation of an oversight committee will persuade Congress to repeal the Hugues-Ryan amendment, which obliges the CIA director to report all covert activities to at least six committees. Over the past 16 months, virtually none of the information conveyed to Congress under the amendment has been kept secret.[156]

It would take a few more years, but that was the eventual outcome: just before the arrival of Reagan at the White House and with the support of the Carter administration,[157] the 1980 Intelligence Oversight Act was adopted to repeal the Hughes-Ryan amendment. While expanding the range of information shared with congressional overseers, the number of informed committees was reduced from six to just two. During Senate committee hearings, the *New York Times* reported that a young liberal Democrat from Delaware by the name of Joe Biden warned civil rights advocates that the momentum for reform had passed and that "opinion in Congress and throughout the country was running strongly against them."[158]

The second lasting legacy of the Church committee came from its condemnation of warrantless surveillance, which inspired the 1978 Foreign Intelligence Surveillance Act (FISA). FISA's initial and rather narrow goal

was to remedy the subsiding forms of warrantless national security surveillance of foreign powers or their agents – an issue left unaddressed by the Supreme Court's 1972 Keith decision which focused solely on cases of "wholly domestic" security issues.[159] In early 1976, the Ford administration had come out in favour of such a federal law and President Carter also supported it.[160] The system would rely on the so-called Foreign Intelligence Surveillance Court (FISC), a court acting in secret where foreign intelligence surveillance authorisations issued by the DoJ would be minimally reviewed by judges, with differing standards based on the identity of the target and the now widely accepted notion of intelligence law that foreigners deserve lesser protection than "US persons." Praised by its drafters as exemplary of the kind of constitutional checks and balances needed for intelligence in a democracy, critiques worried that the FISC might quickly "become captive of the national security establishment and serve only to encourage executive officials, now protected by judicial approval, to conduct activities that would otherwise never have been proposed."[161] In 1980, the press was forced to report that the FISC "granted every request to bug spies,"[162] while the Department of Justice Counsel for Intelligence Policy admitted three years later that "to date, the court ha[d] not rejected a single application," framing it as a sign that the executive branch was careful in its use of such surveillance powers.[163] FISA's founding principles, such as the prohibition on warrantless surveillance and the foreign–domestic distinction, would be undermined by later reforms, especially under George W. Bush's "war on terror" and the boost it gave to NSA-operated large-scale warrantless surveillance.[164]

Lastly, the autonomy of the intelligence field would rely on a third strategy: stopping the outpouring of disclosures by journalists and whistleblowers and re-activating the barrier of secrecy protecting intelligence agencies' relative autonomy. Attempts to pursue such disclosures through the Espionage Act had run into legal hurdles – as illustrated by the failed prosecution of Daniel Ellsberg –, and so Ford's executive order had sketched another course of action, one based on contractual law whereby all intelligence professionals would now have to sign non-disclosure agreements.[165] Approximately at the same time, agencies were establishing formal procedures to review the publications of former agents – the CIA for instance created its Publications Review Board in 1976. A moral panic about the use of "marijuana-hashish epidemic" and the risks it entailed for information security in intelligence further served to legitimise the use of drug testing in a veiled attempts to keep whistleblowing "hippies" at a distance.[166]

More significantly, the period also marked the beginning of a regulatory process called for by the Church committee and epitomised by the 1978 Civil Service Reform Act, whereby whistleblowers were forced to report internally the wrongdoings they might become aware of. As Gurman and Mistry note, executive-branch whistleblowing was defined narrowly in relation to "fraud, waste, and egregious crime." The role of whistleblowers was to "improve the functioning of the state rather than question the underlying tenets of national

security policy or the culture of secrecy," thus being confined to the role of "organisational defenders" rather than public advocates against intelligence abuse.[167] Such strengthening of secrecy effectively curtailed what had been a prime driver in stopping illegal surveillance programmes: as Morton Halperin and his colleagues from the Center for National Security Studies wrote at the time in their public advocacy against US intelligence, it was indeed the "exposure or the possibility of it" that had "moved the agencies to end some of their illegal programs": "no internal mechanism was so effective."[168]

In practice, little changed for intelligence agencies after the Year of Intelligence. There were immediate attempts to "clean house" and bring surveillance practices in conformity with the law.[169] An internal review launched at the CIA in 1975 concluded that they was a "lack of legal expertise in the field of electronic surveillance and a general uncertainty and inexperience in the area of Federal criminal law."[170] Internal workshops were organised to accommodate the new 'external constraints' but also think about how the "climate of public opinion" weighed on the Agency and how the latter could foster "creativity" under such constraints.[171] But as early as August 1976, the CIA was already challenging a Justice Department opinion interpreting the limits of Ford's Executive Order, with George Bush, the new CIA director, claiming that it was too restrictive.[172] A few months later, Carter's quite progressive CIA director, Stansfield Turner, was already looking at ways to improve its damaged relationship with the academic world by working with the outgoing president of the International Studies Association, Vincent Davis,[173] a strategy that apparently bore fruit.[174] By the mid-1980s, the press would note that "the C.I.A. [was] once again attractive to many college students."[175]

"Signal intelligence" and computerisation also appeared as a strategy aimed at expanding more discreet forms of surveillance. In an increasingly tense budgetary context (with the notable exception of the FBI whose budget kept rising), several agency departments faced restrictions in personnel, and overall a low morale. They sought to cope with this decreased manpower by enacting productivity gains through computerisation. A commission established by the Department of Defense to look into intelligence issues declared that it was "impressed with capabilities of our technical collectors as an essential input to the intelligence data base, and we believe that comparison of the data base today with that available 10 years ago illustrates the detail and precision to which we have become accustomed."[176] By then, as an internal paper put it, the NSA was "almost totally dependent on computer systems to aid our analysts," these systems being seen as necessary to "handle the increasing volume of work that grows more sophisticated while our people power is shrinking." CIA director Turner fired 800 operational agents, enacting the vision sketched by his one of his predecessors, James Schlesinger, who believed that SIGINT and computers rather than HUMINT and clandestine operations were the future of intelligence and conducive to better command-and-control.[177] The Army similarly was able to cope with shortages in personnel by increasing the roll-out of new computer installations

dedicated to intelligence.[178] Congressional investigations into computer surveillance in the mid-1985 registered the proliferation of these technologies and the lack of appropriate oversight.[179] In retrospect, computerisation – as part of what sociologist Gary T. Marx would soon term "the new surveillance" –[180] formed part of a strategy aimed at expanding surveillance capabilities while escaping oversight, and therefore constituted a way to defend the autonomy of the field.

None of the more ambitious proposals for intelligence reforms that came out of Congress prior to or after the 1975 investigations would see the light of day. During his campaign, Democratic candidate Jimmy Carter had pledged to support "charter" legislation for the Bureau and the CIA, but his administration eventually listened to those who feared that it would overly constrain the operations of intelligence agencies.[181] Quite ironically, even as Carter's 1980 State of the Union address called on removing restraints on the CIA and as Congress got rid of the Hugues-Ryan amendment while protecting classified information used in criminal trials through the 1980 Classified Information Procedures Act, Republican presidential candidate Ronald Reagan attacked the Democrats' legacy, accusing them of having weakened intelligence agencies. His election would mark yet-another return of a "law-and-order" discourse, with increasing budgets and personnel for intelligence agencies. In line with a report of the Heritage Foundation co-written by his advisors during the transition called on "unleashing" intelligence agencies,[182] the Reagan administration was quick to pass reforms increasing intelligence powers. To give just a few examples, in December 1981 Reagan issued an executive order relaxing rules that precluded the CIA from collecting foreign intelligence in the US.[183] In 1982, the Intelligence Identities Protection Act, passed with *CounterSpy* as the main scapegoat, made it a crime to reveal the names of covert intelligence personnel. In 1983, the administration relaxed rules on domestic intelligence operations against protest groups."[184] And in October 1984, after a battle of several years, Congress exempted certain operational files of the CIA from disclosure under the Freedom of Information Act.[185]

The "old boys" of the intelligence field were on a come-back. In passing these regressive reforms, executive supporters of intelligence could rely on complicit members of Congress whose permanent committees on intelligence had grown supportive of intelligence agencies, practising "institutional" rather than "investigative" oversight.[186] By the mid-1980s, congressional committees on intelligence were largely staffed by former CIA officials.[187] In fact, many executive branch and intelligence officials remained unimpressed with the legacy of the Church committee. Just a few months before the Iran-Contra affair that would taint Reagan's intelligence policy for months, *New York Times* reporter Leslie Gelb concluded that congressional oversight of the CIA had produced "a decade of support" for the agency by Congress.[188] Daniel Patrick Moynihan, former vice chairman of the intelligence committee told Gelb that, "like other legislative committees, ours came to be an advocate for the agency it was

overseeing." William Colby himself acknowledged in February 1976 that the congressional investigations had actually strengthened the CIA and clarified the boundaries "within which it should, and should not, operate."[189] In 1984, he maintained during a public conference that "the American public has benefited from a transition in the CIA from the cloak and dagger days to modern electronic surveillance," and that the CIA "has been strengthened by laws passed in the 1970s which give Congress more authority over the agency."[190]

While the latter part of the quote should be nuanced, Colby was right in saying that the "Year of intelligence" and the intelligence reforms passed in its aftermath had indeed normalised the practices of intelligence agencies. Mostly through executive orders, part of the legal basis for intelligence policy was now public. Through the prerogatives of the Permanent Select Committees, through their open hearings and reports as well as the wider media coverage, more official information now filtered out of the realm of secrecy. Such "staged transparency" helped boost public confidence and gave these agencies a newfound legitimacy, as likely did the occasional fights staged between intelligence officials and their institutional overseers. Meanwhile, secrecy had been strengthened and whistleblowers dissuaded from going public. In the back rooms, secret programmes could resume, and laws again be disregarded.

Conclusion

In the context of a proliferating and radical opposition to intelligence and state surveillance, the institutionalisation of intelligence oversight as it was designed in the US in the mid-70s – and then appropriated by other liberal democracies in response to national or transnational scandals –[191] can be framed as a legitimising device, a power tactic aimed at securing a level of consensus around intelligence agencies and governing anti-surveillance critique.[192] As I have argued, the Year of Intelligence is most accurately framed as a moment of struggle when the intelligence field successfully strategised to re-establish its autonomy whilst making minimal concessions. Rather than a victory of the rule of law, it was a moment for the "internalisation" of unfolding scandals and for the depoliticisation of oppositions by giving them new technical objects – mostly legal in nature – through the development of "new state capacities to manage constitutional checks and balances."[193]

As the central "rule of the game" for intelligence oversight, secrecy complemented such procedural arrangements to enact a boundary between insiders and outsiders, In turn, this effectively cut off professional overseers – be they members of the permanent committees on intelligence or judges – from the more radical and diverse range of critiques that had played such an important role in bringing to the fore the range and depth of intelligence abuse over the previous years. Although over time, some lawmakers sitting on the permanent committees on intelligence have proven themselves critical of intelligence agencies, these committees have been dominated by what Johnson has called "cheerleaders"

of intelligence agencies, that is politicians acting as these agencies' spokespersons in Congress and before the wider public.[194] As for external critics, they either had to join the institutional oversight game through more technically oriented advocacy or litigation at the risk of irrelevance, or be repressed and disqualified as reckless whistleblowers and radicals. What is more, such critics could easily be framed as not being "in the know," and not knowledgeable enough to appear as legitimate actors in intelligence policy debates.

Although a detailed socio-history of this process of depoliticisation through institutional intelligence oversight would be needed, it seems reasonable to suggest that, in the past forty years, the oversight structure established in the US after 1975 has given intelligence officials a working configuration to pass regressive reforms, on the long run weakening the already-tepid procedural arrangements adopted in the aftermath of the Year of Intelligence. And that in the aftermath of other scandals and in the midst of other crises, such structures largely worked to shield intelligence autonomy. Radical, "non-reformist reforms" of the kind debated in the first half of the seventies does not seem to have resurfaced in later intelligence policy debates, much less gained the prominence they had then. For all the spectacular massive disclosures of the likes WikiLeaks or Edward Snowden, and except in perhaps a few localised instances, the coalitions sparked by such disclosures to rein in intelligence abuse never got close to exerting the kind of political force that intelligence agencies had to resist in the 70s.

As for Franck Church, regardless of his motives and intentions, or the merits of many of the recommendations put forward by his committee, he was largely made in retrospect a kind of what Bourdieu called a "bureaucratic hero," a "prophet" who "rescued the possibility of believing in the official truth despite everything," a "person whose major function is to enable the group to continue to believe in the official, that is, in the idea that there is a group consensus on a certain number of values that are indispensable in dramatic situations in which the social order is deeply challenged."[195] Modern intelligence oversight emerged in the midst of such a moral crisis, whereby a growing network of actors holding increasingly powerful positions in their respective fields coalesced to scandalise intelligence. It is when they got to their maximal influence on the field of power that the Year of Intelligence took place, in turn giving way to impromptu strategies aimed at depoliticising intelligence oversight while Church and his co-investigators passed to history as the symbols of the reconciliation of US intelligence with the rule of law and democratic standards.[196] The tepid reforms adopted in their names, which set aside the most ambitious proposals of the time, would be both the product and reproducer of a procedural understanding of democracy, one losing sight of the substantive meaning of a democratic regime and of the dangers of political surveillance, conflating what Tarrow, Ginsburg and Mustafa have called "rule *by* law" with the rule *of* law.[197]

Of course, many developments took place from 1975 on that would help explain why a more radical agenda for intelligence oversight never came to pass: besides the manoeuvring and internal strives within the executive branch under the Ford and Carter administrations (which would deserve a more detailed analysis), there was the expanding economic crises, the eviction in the late-1970s elections of many congress members who had worked on national security issues, the fatigue of the public and the media in confronting the abuses of their government, the loosening of the ephemeral alliance between radicals and reformers, as well as new pressing issues on the international scene. For his part, Christopher Pyle, the Army intelligence whistleblower, made in 1979 the following commentary – a quite discerning if bitter one:

> As inflation makes the public more conservative, demand of reform of the intelligence agencies will wane, only to prove once again that ours is a 'democracy,' but it is a democracy of moods and sentiments, as indifferent to constitutional principles as Hoover and his agents.[198]

More research would be needed to explore the relevance of these and other possible causal factors in the eventual failure to enact meaningful democratic oversight of intelligence agencies. But by giving evidence of the forms of radical opposition to US intelligence in the decade preceding 1975, this sociogenesis has recast institutional intelligence oversight in its wider historical setting. While offering a glimpse of the paths not taken, the process of institutionalisation it covers helps explain why the interstitial field concerned with intelligence oversight in the 70s has become largely dependent on, and subservient to, the intelligence field, crystallising a set of normative assumptions about what proper intelligence oversight should be.

This doxa is still prevalent in parliamentary oversight committees, many courts, the bulk of Intelligence Studies, or even many think tanks or NGOs working on intelligence. It is marked by a procedural and technocratic understanding of democracy, whereby supposedly ill-informed outsiders are excluded, partisan and radical criticisms of intelligence policy discredited, and whistleblowers – who have historically played a key role in intelligence – oversight demonised.[199] By having a better sense of its origins, by unearthing the invisibilised histories of the courageous actors who resisted intelligence abuse and by drawing inspiration from them, perhaps can we better inform the contemporary struggles aimed at reining in the ongoing and systemic violence committed in the name of intelligence, and by doing so help open new pathways towards emancipatory social change.

Notes

1 Félix Tréguer, 'Intelligence Reform and the Snowden Paradox: The Case of France', *Media and Communication* 5, no. 1 (22 March 2017): 17–28.

2 Monika Zalnieriute, 'Procedural Fetishism and Mass Surveillance under the ECHR', *Verfassungsblog* (blog), 2 June 2021, https://verfassungsblog.de/big-b-v-uk/.
3 See for instance Bridget Fowler, 'Pierre Bourdieu on Social Transformation, with Particular Reference to Political and Symbolic Revolutions', *Theory and Society* 49, no. 3 (1 April 2020): 439–63; Isaac Ariail Reed, 'Can There Be a Bourdieusian Theory of Crises? On Historical Change and Social Theory', *History and Theory* 54, no. 2 (2015): 269–76; Gisèle Sapiro, 'Structural History and Crises Analysis', in *Bourdieu and Historical Analysis*, ed. Philip S. Gorski (Durham, NC: Duke University Press Books, 2013), 266–85.
4 Sapiro, 'Structural History and Crises Analysis', 266–68.
5 See for example Laurent Bonelli, Hervé Rayner, and Bernard Voutat, 'Contestations et (re)légitimations du renseignement en démocratie', *Cultures Conflits* 114–115, no. 2 (2019): 7–28.
6 Didier Bigo, 'Violence Performed in Secret By State Agents: For an Alternative Problematisation of Intelligence Studies', in *Problematising Intelligence Studies*, ed. Hager Ben Jaffel and Sebastian Larsson (Routledge, 2022), 220–40.
7 Frédéric Lebaron, 'Pouvoir', in *Dictionnaire d'économie politique: Capitalisme, institutions, pouvoir*, ed. Colin Hay and Andy Smith (Presses de Sciences Po, 2018), 358–64.
8 Bernardino León-Reyes, 'Towards a Reflexive Study of Intelligence Accountability'. In *Problematising Intelligence Studies*, edited by Hager Ben Jaffel and Sebastian Larsson, 30–47. Routledge, 2022, 35.
9 'Year of Intelligence', *The New York Times*, 8 February 1975, sec. Archives.
10 Loch K. Johnson, 'The Church Committee Investigation of 1975 and the Evolution of Modern Intelligence Accountability', *Intelligence and National Security* 23, no. 2 (1 April 2008): 198–225.
11 Pierre Bourdieu, *On the State: Lectures at the College de France, 1989–1992*, 1 edition (Cambridge Malden, MA: Polity Press, 2014), 56, 46.
12 Grégoire Chamayou, *The Ungovernable Society: A Genealogy of Authoritarian Liberalism* (John Wiley & Sons, 2021).
13 '1968 Bomb Explosions at U-M', *The History of the University of Michigan* (blog), 19 December 2019, https://historyofum.umich.edu/panther-by-the-tail/.
14 Michael Dover, 'U of M Bombed', *Fifth Estate Magazine*, 13 November 1968, https://www.fifthestate.org/archive/65-october-31-november-13-1968/u-of-m-bombed/.
15 Jeff A. Hale, 'The White Panthers' "Total Assault on the Culture"', in *The American Counterculture of the 1960's and 70's*, ed. Peter Braunstein and Michael William Doyle (Routledge, 2001), 125–56.
16 Bill Ayers, *Fugitive Days: Memoirs of an Antiwar Activist* (Beacon Press, 2009), 63.
17 'To many liberals,' Donner writes, 'the notion of dealing with Communists by measures short of outright repression held a strong appeal. It would be wrong to jail them, but to identify and watch them seemed unobjectionable.' Some of these measures were still established on the eve of during WWII. Frank J. Donner, *The Age of Surveillance: The Aims and Methods of America's Political Intelligence System* (Vintage Books, 1980), 61–63.
18 Jennifer Klein. *For All These Rights: Business, Labor, and the Shaping of America's Public-Private Welfare State*. Politics and Society in Modern America. Princeton University Press, 2006.
19 Mark Neocleous, 'From Social to National Security: On the Fabrication of Economic Order', *Security Dialogue* 37, no. 3 (September 2006): 363–84.
20 William Keller, *The Liberals and J. Edgar Hoover: Rise and Fall of a Domestic Intelligence State* (Princeton, N.J: Princeton University Press, 1989), 36, 27.

21 Harry Howe Ransom, 'Congress and the Intelligence Agencies', *Proceedings of the Academy of Political Science* 32, no. 1 (1975): 159.
22 Ibid., 160.
23 See e.g. 'Congress Can Keep a Secret', Congressional Records (U.S. Congress, 28 March 1963), https://www.cia.gov/readingroom/document/cia-rdp75-00149r000700040034-7.
24 On the decline of congressional investigations of the executive branch, see David R. Mayhew, *Divided We Govern: Party Control, Lawmaking and Investigations, 1946-2002* (Yale University Press, 2005); On the rise of secrecy in the context of the nuclear arms race, see Alex Wellerstein, *Restricted Data: The History of Nuclear Secrecy in the United States*, First edition (Chicago: University of Chicago Press, 2021).
25 Kathryn S. Olmsted, *Challenging the Secret Government: The Post-Watergate Investigations of the CIA and FBI*, Illustrated edition (Chapel Hill: University of North Carolina Press, 1996), 43.
26 Donner, *The Age of Surveillance*, 102.
27 Powers has called the FBI 'one of the greatest publicity-generating machines the country had ever seen,' Richard Gid Powers, *G-Men, Hoover's FBI in American Popular Culture* (Southern Illinois University Press, 1983), 95; see also Simon Willmetts, *In Secrecy's Shadow: The OSS and CIA in Hollywood Cinema 1941–1979* (Edinburgh University Press, 2017).
28 'Self-Discipline Tied to Secrecy', *Baltimore Sun*, 25 February 1962, CIA CREST Record, https://www.cia.gov/readingroom/document/cia-rdp70-00058r000200100088-2.
29 Anthony Summers, *Official and Confidential: The Secret Life of J. Edgar Hoover* (Open Road Media, 2012), chap. 20.
30 Donner, *The Age of Surveillance*, 27.
31 Hoover memorandum dated 28 April 1965, quoted in '"Church Report": Supplementary Detailed Staff Reports on Intelligence Activities and Rights of Americans (Book III)', Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (Washington, D.C: U.S. Senate, 1976), 485.
32 Richard Helms, 'International Connections of U.S. Peace Groups', Memorandum for the President (CIA, 15 November 1967), https://aavw.org/special_features/govdocs_cia_abstract02_excerpts.html.
33 Rhodri Jeffreys-Jones, *The FBI: A History*, 6/28/08 edition (New Haven, Conn.: Yale University Press, 2008), 173.
34 James K. Davis, *Assault on the Left: The FBI and the Sixties Antiwar Movement* (Westport, Conn: Praeger, 1997).
35 For a chronology of the programme, see 'Chronology of Significant MHCHAOS Correspondence' (CIA, 14 October 1975), https://www.cia.gov/readingroom/document/01481988; For an insider account of the operation see Frank J. Rafalko, *MH / CHAOS: The CIA's Campaign Against the Radical New Left and the Black Panthers* (Annapolis, MD: Naval Institute Press, 2011); See also '"Church Report": Supplementary Detailed Staff Reports on Intelligence Activities and Rights of Americans (Book III)', 679; Nelson A. Rockefeller, 'Report to the President by the Commission on CIA Activities Within the United States' (Washington, D.C: White House, June 1975), chap. 11, CIA CREST Record, https://www.cia.gov/readingroom/document/cia-rdp80m01133a000900130001-5.
36 '"Church Report": Supplementary Detailed Staff Reports on Intelligence Activities and Rights of Americans (Book III)', 515; Goldstein, *Political Repression in Modern America from 1870 to 1976*, 457; See also the critical report of a former CIA undercover operative by Verne Lyon, 'Domestic Surveillance:

The History of Operation CHAOS', *Covert Action Information Bulletin*, 1990, https://newtotse.com/oldtotse/en/politics/central_intelligence_agency/166323.html; John Prados, *The Family Jewels: The CIA, Secrecy, and Presidential Power* (University of Texas Press, 2014), 71.

37 Prados, *The Family Jewels*, 82–4.

38 On the genesis of the CONUS Intel programme, see Scott, *Reining in the State*, 51–66.

39 'Army Surveillance of Civilians: A Documentary Analysis', Committee on the Judiciary (Washington, D.C.: U.S. Senate, August 1972), 21.

40 '"Church Report": Supplementary Detailed Staff Reports on Intelligence Activities and Rights of Americans (Book III)', 803.

41 Sarah E. Igo, *The Known Citizen: A History of Privacy in Modern America*, Illustrated edition (Cambridge, Massachusetts: Harvard University Press, 2018), 221–46.

42 Joy Rohde, *Armed with Expertise: The Militarization of American Social Research during the Cold War*, American Institutions and Society (Ithaca, NY: Cornell University Press, 2013); Sharon Weinberger, *The Imagineers of War: The Untold Story of DARPA, the Pentagon Agency That Changed the World* (New York: Knopf, 2017); Jill Lepore, *If Then: How the Simulmatics Corporation Invented the Future* (New York: Liveright, 2020).

43 Jens Wegener, 'Order and Chaos: The CIA's HYDRA Database and the Dawn of the Information Age', *Journal of Intelligence History* 19, no. 1 (2 January 2020): 77–91.

44 Orrin Clotworthy, 'Some Far-out Thoughts on Computers', *Studies in Intelligence (CIA Journal)* 6, no. 4 (1962), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-56-no-4/some-far-out-thoughts-on-computers.html. See also how CIA officials claimed that computers could help solve the case of Kennedy's assassination. Jeremieah O'Leary, 'McCone Claims Computers Could Aid in Investigations', *Evening Star*, 5 October 1964

45 Central Intelligence Agency. 'The Long Range Plan of the Central Intelligence Agency', 31 August 1965. http://archive.org/details/TheLongRangePlanOfTheCentralIntelligenceAgency.

46 CODIB, 'R&D for Intelligence Processing: Recommendations for Invigorating and Coordinating the Community's Development of Data-Handling Systems' (U.S. Intelligence Board, 1965), https://www.cia.gov/readingroom/document/cia-rdp80b01139a000500140001-3.

47 A 1969 internal memo on 'computer skills development programs' would also complain of an intergenerational divide with more experienced analysts 'able to see the big picture' but lacking computer skills, and 'generally young, inexperienced and junior' officers well-versed in computer techniques. It also bemoaned the lack of results of teams tasked with developing computer programs. 'Computer/Operations Research Skill Development Program', September 1969, CIA CREST Record, https://www.cia.gov/readingroom/docs/CIA-RDP78-04723A000100160006-3.pdf.

48 Rohde, *Armed with Expertise*.

49 J. Edgar Hoover, 'Now: Instant Crime Control in Your Town', *Popular Science*, January 1967.

50 'Inter-Division Information Unit (IDIU)' (Department of Justice, 5 December 1978), U.S. National Archives, https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0060/nc1-060-79-02_sf115.pdf. Katherine Anne Scott, *Reining in the State: Civil Society and Congress in the Vietnam and Watergate Eras*. University Press of Kansas, 2013, 34, 42–47.

51 '"Church Report": Supplementary Detailed Staff Reports on Intelligence Activities and Rights of Americans (Book III)', 495; Rafalko, *MH / CHAOS*, chap. 5.

52 Jens Wegener, 'Order and Chaos: The CIA's HYDRA Database and the Dawn of the Information Age', *Journal of Intelligence History* 19, no. 1 (2 January 2020): 77–91; Rafalko, *MH / CHAOS*.
53 Chief of Information Processing Staff, 'Briefing for the DCI on Automatic Data Processing in the Agency', 25 October 1969, CIA CREST Record, https://www.cia.gov/readingroom/document/cia-rdp78-04723a000100100032-0; See also: Chief of Information Processing Staff, 'Strengthening the Information Processing Structure of the Agency' (CIA, 15 September 1969), CIA CREST Record, https://www.cia.gov/readingroom/docs/CIA-RDP78-04723A000100100029-4.pdf.
54 Directorate of Sciences and Technology, 'Office of Computer Services: Computer Systems Plan for the Period 1971-1975' (Central Intelligence Agency, February 1971), https://www.cia.gov/readingroom/document/cia-rdp80-01003a000100070001-7.
55 'Military Surveillance of Civilian Politics: Report of the Subcommittee on Constitutional Rights', Committee on the Judiciary (Washington, D.C.: U.S. Senate, 1973), 71.
56 Lisa Stampnitzky. 'Experts, States, and Field Theory: Learning from the Peculiar Case of Terrorism Expertise'. *Critique Internationale* 59, no. 2 (2013): 89–104.
57 Norbert Wiener, 'A Scientist Rebels', January 1947.
58 Rohde, *Armed with Expertise*, 55.
59 Ibid., 71.
60 Kalman H. Silvert, 'American Academic Ethics and Social Research Abroad: The Lessons of Project Camelot', in *The Rise and Fall of Project Camelot: Studies in the Relationship Between Social Science and Practical Politics*, ed. Irving Louis Horowitz (M.I.T. Press, 1967), 87.
61 John Chamberlain, 'Camelot Equaled "Costalot"', *The Times Herlad*, 14 August 1965, CIA Crest Record, https://www.cia.gov/readingroom/document/cia-rdp73-00475r000102540004-2; '"Project Camelot" Fizzle Brings Cut in Army Funds', *The Latin American Times*, 27 August 1965, https://www.cia.gov/library/readingroom/document/cia-rdp75-00149r000500320018-6; Rohde, *Armed with Expertise*, 112.
62 Igo, *The Known Citizen*; Lepore, *If, Then*.
63 Sol Stern, 'A Short Account of International Student Politics & the Cold War with Particular Reference to the NSA, CIA, Etc.', *Ramparts*, March 1967.
64 Peter Richardson, 'The Perilous Fight: The Rise of Ramparts Magazine, 1965–1966', *California History* 86, no. 3 (2009): 22–69.
65 Tim Weiner, *Legacy of Ashes: The History of the CIA* (Knopf Doubleday Publishing Group, 2008), 311.
66 Jack Rosenthal, 'Memo for the White House: CIA-NSA Flap' (Department of State, 15 February 1967), DNSA collection: CIA Covert Operations III.
67 Tity de Vries, 'The 1967 Central Intelligence Agency Scandal: Catalyst in a Transforming Relationship between State and People', *The Journal of American History* 98, no. 4 (2012): 1086.
68 Gerald M. Rosberg, 'CIA Recruiting Cancelled To Avoid Student Protest', *The Harvard Crimson*, 27 February 1967.
69 Ibid.
70 Agis Salpukas, 'Stony Brook Computer Center Occupied by S.D.S. Protesters', *The New York Times*, 9 May 1969, sec. Archives.
71 Quoted in Yasha Levine, *Surveillance Valley: The Secret Military History of the Internet* (PublicAffairs, 2018), chap. 2.
72 Lepore, *If, Then*, 295.
73 M. Mitchell Waldrop, *The Dream Machine: J.C.R. Licklider and the Revolution That Made Computing Personal* (Penguin Books, 2002), chap. 7.
74 Rohde, *Armed with Expertise*, 89.

75 See e.g. 'A Good Move by U-Mass', *Herald Traveler*, 30 April 1972, https://www.cia.gov/readingroom/docs/CIA-RDP80-01601R000200050002-6.pdf.
76 Christopher H. Pyle, 'CONUS Intel: The Army Watches Civilian Politics', *The Washington Monthly*, January 1970.
77 Christopher Pyle, Looking back at the CONUS Intel Scandal, interview by Félix Tréguer, Telephone, 20 May 2022.
78 Christopher H. Pyle, 'CONUS Revisited: The Army Covers Up', *The Washington Monthly*, July 1970.
79 See e.g. Ben A. Franklin, 'Federal Computer Amass Files on Suspect Citizens', *The New York Times*, 27 June 1970, https://www.cia.gov/readingroom/document/cia-rdp80-01601r001400120001-6.
80 '"Church Report": Supplementary Detailed Staff Reports on Intelligence Activities and Rights of Americans (Book III)', 942.
81 Pyle, Looking back at the CONUS Intel Scandal.
82 Some of the reports' recommendations were nonetheless carried on by the FBI, such as lowering the age for Black informants from 21 to just 18. J. Edgar Hoover et al., 'Special Report of the Interagency Committee on Intelligence (Ad Hoc) (Huston Plan)' (Washington, D.C., 25 June 1970).
83 Jeffreys-Jones, *The FBI*, 183.
84 The committee report was eventually published in 1973 after Ervin fought the Department of Defence to authorise its declassification. 'Military Surveillance of Civilian Politics: Report of the Subcommittee on Constitutional Rights'; See also the companion reports: 'Federal Data Banks, Computers, and the Bill of Rights', Hearings before the Subcommittee on Constitutional Rights of the Committee on the Judiciary (Washington DC: U.S. Senate, March 1971); See also the companion report 'Army Surveillance of Civilians: A Documentary Analysis', Committee on the Judiciary (Washington, D.C.: U.S. Senate, August 1972).
85 Ben A. Franklin, 'Surveillance of Citizens Stirs Debate', *The New York Times*, 27 December 1970, sec. Archives. This process culminated with the adoption of the Privacy Act in 1974. In 1973, Ervin had also tabled the "Freedom From Surveillance Bill", which sought to make domestic surveillance by the Army a criminal offence, but it was never adopted.
86 Scott, *Reining in the State*, 84–87, 106–107. On Ervin's decade-long battle for privacy, see *131–133.*
87 Betty Medsger, *The Burglary: The Discovery of J. Edgar Hoover's Secret FBI*, 1st edition (New York: Knopf, 2014).
88 Steve Sheinkin, *Most Dangerous: Daniel Ellsberg and the Secret History of the Vietnam War* (Roaring Brook Press, 2015).
89 On the passage of the Act and the objections of the Johnson administration to Title III, see Scott, *Reining in the State*, 47–49. On the wider political context, see Elizabeth Hinton. *America on Fire: The Untold History of Police Violence and Black Rebellion Since the 1960s*. New York, NY: Liveright, 2021.
90 For an insider account of the Keith case by the White Panthers' lawyer, see Hugh 'Buck' Davis, 'A People's History of the CIA Bombing Conspiracy (the Keith Case); Or, How the White Panthers Saved the Movement', Ann Arbor District Library, 2010, https://aadl.org/freeingjohnsinclair/essays/peoples_history_of_the_cia_bombing_conspiracy; See also Trevor W. Morrison, 'The Story of United States v. United States District Court (Keith): The Surveillance Power', Presidential Power Stories - Columbia Public Law Research Paper (Foundation Press, 2008); Jeff Hale, 'Wiretapping and National Security: Nixon, the Mitchell Doctrine, and the White Panthers' (PhD in History, Louisiana State University, 1995); Brian Hochman, *The Listeners: A History of Wiretapping in the United States* (Harvard University Press, 2022), 216.

91 Richard H. Blum, ed., *Surveillance and Espionage in a Free Society* (New York: Praeger Publishers, 1972), 310–14.
92 'Some Books on the CIA' (CIA, 23 March 1973), https://www.cia.gov/readingroom/document/cia-RDP75-00793R000300050002-0.
93 Jeffreys-Jones, *The FBI*, 183.
94 David M. Barrett, 'Secrecy, Security, and Sex: The NSA, Congress, and the Martin–Mitchell Defections', *International Journal of Intelligence and CounterIntelligence* 22, no. 4 (4 September 2009): 699–729.
95 David Horowitz, 'U.S. Electronic Espionage: A Memoir', *Ramparts*, August 1972.
96 Adrian Chen, 'After 30 Years of Silence, the Original NSA Whistleblower Looks Back', Gawker, 12 November 2013, https://www.gawker.com/after-30-years-of-silence-the-original-nsa-whistleblow-1454865018.
97 On the founding and operation of CARIC, see 'Subversion of Law Enforcement Intelligence Gathering Operations: Organizing Committee for a Fifth Estate' (U.S. Government Printing Office, 1976).
98 Excerpts of the second issue, quoted in Nat Hentoff, 'Afte Ellsberg: Counter-Spy', The Village Voice, 19 July 1973.
99 Dorothy McGhee, 'Counterspy Exposes "Techno-Fascism"', *Daily Rag*, 20 April 1973, https://www.cia.gov/readingroom/docs/CIA-RDP88-01314R000100370024-9.pdf.
100 Walter Pforzheimer, 'Memo from the Historical Intelligence Collection on Counterspy for the Deputy Director of Central Intelligence' (CIA, 14 May 1973).
101 See a chapter dedicated to Counter-Spy in David McCarthy, 'The CIA & the Cult of Secrecy' (PhD in History, College of William & Mary, 2008), chap. 1.
102 *CounterSpy (2:3)*, vol. 2 (Fifth Estate, 1975), 16.
103 Kaeten Mistry, 'The Rise and Fall of Anti-Imperial Whistleblowing in the Long 1970s', in *Whistleblowing Nation: The History of National Security Disclosures and the Cult of State Secrecy*, ed. Kaeten Mistry and Hannah Gurman (Columbia University Press, 2020), 125.
104 Levine, *Surveillance Valley*, chap. 3.
105 Memo by Richard Ober, "Meeting with the Director on MHCHAOS," 5 December 1972, quoted in Wegener, 'Order and Chaos'.
106 '"Church Report": Supplementary Detailed Staff Reports on Intelligence Activities and Rights of Americans (Book III)', 604 On the termination of the CHAOS program, see p. 706.
107 Olmsted, *Challenging the Secret Government*, 17.
108 James Boylan, 'Declarations of Independence', *Columbia Journalism Review* 25, no. 4 (1986): 44; Quoted in Olmsted, *Challenging the Secret Government*, 193.
109 John M. Crewdson, 'CIA Is Criticized Over Watergate', *The New York Times*, 3 July 1974, sec. Archives.
110 'Report of the Republican Task Force on Privacy', Congressional Records (Washington, D.C.: U.S. House of Representatives, 12 September 1974), https://www.cia.gov/readingroom/document/cia-rdp76m00527r000700140101-6.
111 'Warrantless Wiretapping and Electronic Surveillance', Joint Hearings Before the Subcommittee on Administrative Practice and Procedure, the Subcommittee of Constitutional Rights and the Subcommittee on Surveillance of the Committee on Foreign Relations, 93-2, Apr. 3, 8, 1974; May 8, 9, 10, and 23, 1974 (U.S. Senate, 1974); See the letter of senator Edmund Muskie asking the CIA for its collaboration with the investigation: Edmund S. Muskie, 'Letter to DCI on the Creation of a Joint Investigation of Warrantless Wiretapping and Electronic Surveillance', Congressional Records (Washington, D.C, 2 July 1974), https://www.cia.gov/readingroom/docs/CIA-RDP80M01009A003100010030-9.pdf.

112 Seymour M. Hersh, 'C.I.A. Is Linked to Strikes In Chile That Beset Allende', *The New York Times*, 20 September 1974, sec. Archives.
113 Quoted in Olmsted, *Challenging the Secret Government*, 45.
114 Quoted in Frederick M. Kaiser, 'Legislative History of the Senate Select Committee on Intelligence' (Congressional Research Service, The Library of Congress, 1978).
115 Dan Lopez et al., 'Veto Battle 30 Years Ago Set Freedom of Information Norms', Electronic Briefing Book (National Security Archive, November 2004).
116 Laura Kalman, *Right Star Rising: A New Politics, 1974–1980* (New York: W. W. Norton & Company, 2010), 38.
117 Seymour M. Hersh, 'Huge CIA Operation Reported in US Against Antiwar Forces, Other Dissidents, In Nixon Years', *The New York Times*, 22 December 1974, sec. Archives.
118 Seymour M. Hersh, 'Ford Names Rockefeller to Head Inquiry into CIA: Wants Report in 90 Days', *The New York Times*, 6 January 1975, sec. Archives.
119 Quoted in Kathryn Olmsted, 'Reclaiming Executive Power: The Ford Administration's Response to the Intelligence Investigations', *Presidential Studies Quarterly* 26, no. 3 (1996): 725–37.
120 Anthony Ripley, 'Views and Background of Ford Commission Investigating C.I.A.', *The New York Times*, 14 January 1975, sec. Archives.
121 Ford quoted in Olmsted, *Challenging the Secret Government*, 49.
122 Ronald Kessler, 'FBI Had Files on Congress, Ex-Aides Say', *The Washington Post*, 19 January 1975.
123 First was the revelation in January by NBC journalist Ford Rowan that the Army CONUS Intel files had been sent to the NSA via the Arpanet. See a CIA memo mentioning the broadcast: Director of Central Intelligence, '"Interagency" Computers' Reported by NBC News', 13 January 1975, CIA CREST Record, https://www.cia.gov/readingroom/document/cia-rdp80m01133a000600080005-0; See also: Ford Rowan. *Technospies: The Secret Network That Spies on You, and You*. New York: Putnam, 1978, 49-56; Levine, Surveillance Valley, chap. 3. Then, in March 1975, the *Washington Post* published a long article on the NSA: Douglas Watson, 'NSA: America's Huge Vacuum Cleaner of Intelligence', The Washington Post, 2 March 1975. Rowan's disclosure in particular sparked another investigation into the technological systems used by law enforcement and intelligence agencies for surveillance purposes: 'Surveillance Technology: Joint Hearings', Subcommittee on Constitutional Rights of the Committee on the Judiciary and the Special Subcommittee on Science, Technology, and Commerce of the Committee on Commerce (Washington, D.C.: U.S. Senate, 10 September 1975); 'Surveillance Technology: Policy and Implications (An Analysis and Compendium of Materials)', Staff Report of the Subcommittee on Constitutional Rights of the Committee on the Judiciary and the Special Subcommittee on Science, Technology, and Commerce of the Committee on Commerce (Washington, D.C.: U.S. Senate, 1976).
124 Olmsted, *Challenging the Secret Government*, 56.
125 'Surveillance Technology', 1976; 'Surveillance Technology', 10 September 1975.
126 Olmsted, *Challenging the Secret Government*, 115.
127 Ibid., 118.
128 Seymour M. Hersh Special to The New York Times, 'C.I.A's Work Unimpeded By Inquiries and Reports, Officials of Agency Assert', *The New York Times*, 10 November 1975, sec. Archives.
129 Olmsted, *Challenging the Secret Government*, 127–43; Dafydd Townley, 'Spies, Civil Liberties, and the Senate: The 1975 Church Committee' (PhD, University of Reading, 2018), 63–67.

130 'In the summer of 1975, President Ford ordered the implementation of 20 of the 30 recommendations of the Rockefeller Commission, to include measures to provide improved internal supervision of CIA activities; additional restrictions on CIA's domestic activities; a ban on mail openings; and an end to wiretaps, abuse of tax information, and the testing of drugs on unsuspecting persons. Ford did not agree to public disclosure of the intelligence budget, however, nor did he readily agree to a separate congressional oversight committee.' 'The Evolution of the U.S. Intelligence Community-An Historical Overview', Intelligence Resource Program (Federation of American Scientists, 1996); 'Report to the President by the Commission on CIA Activities Within the United State ("Rockefeller Report")' (Washington, D.C: White House, 1975); Nicholas M. Horrock, 'Rockefeller Inquiry Clears C.I.A. of Major Violations', *The New York Times*, 3 June 1975, sec. Archives.

131 Jack Marsh, 'Organization of the Intelligence Co-Ordinating Group'. White House, 30 October 1975. https://www.cia.gov/readingroom/docs/CIA-RDP80M01066A000800250009-0.pdf. See also Townley, 'Spies, Civil Liberties, and the Senate', 70.

132 Mike Duval to John Marsh, October 23, 1975, folder "Draft Plan for ICG, 10/75," Box 11, Michael Raoul-Duval Papers, Gerald R. Ford Presidential Library. Quoted in Olmsted, *Challenging the Secret Government*, 148.

133 *Times*, 'C.I.A's Work Unimpeded By Inquiries and Reports, Officials of Agency Assert'.

134 Olmsted, *Challenging the Secret Government*, 184.

135 Ibid., 27.

136 *Tulsa Daily World*, 17 November 1975. Quoted in Ibid., p. 138.

137 William Safire. 'The Blowsoft'. *The New York Times*, 4 December 1975, sec. Archives. https://www.nytimes.com/1975/12/04/archives/the-blowsoft.html.

138 Quoted in Frank John Smist, *Congress Oversees the United States Intelligence Community, 1947-1994* (University of Tennessee Press, 1994), 64.

139 Olmsted, *Challenging the Secret Government*, chap. 7.

140 House Select Committee on Intelligence. The Unexpurgated Pike Report: Report of the House Select Committee on Intelligence (1976). McGraw Hill, 1992. http://archive.org/details/PikeCommitteeReportFull. For a CIA perspective on the Pike report, see Gerald K. Haines. 'The Pike Committee Investigations and the CIA: Looking for a Rogue Elephant'. *Studies in Intelligence*, Winter 1998-1999. https://www.cia.gov/static/688ed924c2cec7a35d79051ab51bc4b5/CIA-Pike-Committee-Investigations.pdf.

141 '"Church Report": Foreign and Military Intelligence (Book I)', Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (Washington, D.C: U.S. Senate, 1976), 1–2.

142 The report for instance stated that 'the Hughes-Ryan Amendment (22 USC, 2422) should be amended so that the foregoing notifications and presidential certifications to the Senate are provided only to that [intelligence oversight] committee.' Ibid., 431.

143 In December 1975, the ACLU had proposed "sweeping legislative reforms to drastically reduce secrecy with new classification rules; a statutory definition of all intelligence agencies through new charters; legislation to limit surveillance, wiretapping, and other techniques (…)." Scott, *Reining in the State*, 158.

144 The Church committee's main list of recommendations can be found in '"Church Report": Supplementary Detailed Staff Reports on Intelligence Activities and Rights of Americans (Book III)', 289–339; See also '"Church Report": Foreign and Military Intelligence (Book I)', 423–74.

145 '"Church Report": Intelligence Activities and Rights of Americans (Book II)'. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Washington, D.C: U.S. Senate, 1976, 290.
146 Laurence Stern, 'Panel details Abuses on Domestic Spying', *The Washington Post*, 29 April 1976.
147 Luca Trenta, '"An Act of Insanity and National Humiliation": The Ford Administration, Congressional Inquiries and the Ban on Assassination', *Journal of Intelligence History* 17, no. 2 (3 July 2018): 121–40.
148 Subsequent guidelines would get rid of the reference to 'subversion' but, according to Poveda, they allowed for 'many of the same kinds of investigations that led to the abuses of the past.' Tony G. Poveda, 'The FBI and Domestic Intelligence: Technocratic or Public Relations Triumph?', *Crime & Delinquency* 28, no. 2 (April 1982): 208.
149 John M. Crewdson, 'Ford Asks Intelligence Disclosure Curb', *The New York Times*, 19 February 1976, sec. Archives.
150 'Text of Ford Plan on Intelligence Units and Excerpts From His Executive Order', *The New York Times*, 19 February 1976, sec. Archives.
151 Townley, 'Spies, Civil Liberties, and the Senate', 72–73, 201.
152 George Bush, 'Letter of DCI to Honorable Jack Brooks, Chairman Committee on Government Operations House of Representatives on Amending the Privacy Act' (CIA, 28 April 1976), CIA CREST Record, https://www.cia.gov/readingroom/document/cia-rdp77m00144r000800070028-0.
153 Townley, 'Spies, Civil Liberties, and the Senate', 213. Scott, *Reining in the State*, 168-169. For an overview of the proposed bills creating an intelligence oversight committee, see this CIA memo: 'From George to Don (on Pending Congress Legislation)' (CIA, 3 June 1975), CIA CREST Record, https://www.cia.gov/readingroom/document/cia-rdp77m00144r001100180006-8.
154 'Congressional Record', 95th Congress, 1st Session, 14 July 1977.
155 Besides footnote 148, see the commentary of Senator Barry Goldwater on the perils of the Hugues-Ryan amendment. '"Church Report": Foreign and Military Intelligence (Book I)', 577. See also pp. 430, 588, 599.
156 Bartlett, 'Congress Still Wants to Hear about CIA Secret Operations … ...'
157 Townley, 'Spies, Civil Liberties, and the Senate', 219.
158 "The folks don't care," Biden is quoted as saying, in essence arguing that he agreed with the concerns of civil rights advocates but that the bill was better than nothing and far better than other proposals seeking to legalise controversial surveillance practices. "If you had a referendum on whether to 'unleash' the C.I.A., Biden further alleged, more than 50% of the people, not knowing what 'unleash' meant, would vote 'yes'." Quoted in Charles Mohr, 'A.C.L.U. Testifies Intelligence Bill Would Legalize "Abuses" by C.I.A.', *The New York Times*, 26 March 1980.
159 Meanwhile, the D.C. Court of Appeals ruled in 1975, in the Zweibon v. Mitchell case, that foreign intelligence electronic surveillance should be conducted pursuant to a warrant. See Americo R. Cinquegrana, 'The Walls (And Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978', *University of Pennsylvania Law Review* 137, no. 3 (1989): 793–828; Trevor Morrison, 'The Story of United States v. United States District Court (Keith): The Surveillance Power', *Columbia Public Law & Legal Theory Working Papers*, 20 November 2008; Ira S. Shapiro, 'The Foreign Intelligence Surveillance Act: Legislative Balancing of National Security and the Fourth Amendment', *Harvard Journal on Legislation* 15, no. 1 (1978 1977): 142.
160 Thomas Blanton, 'Wiretap Debate Déjà Vu: Electronic Surveillance From the Cold War to Al-Qaeda', *The National Security Archive*, 4 February 2006, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB178/index.htm.

161 Cinquegrana, 'The Walls (And Wires) Have Ears', 815.
162 "Secret Court Said to Grant Every Request to Bug Spies," *The Washington Post*, March 4, 1980. Quoted in Hochman, *The Listeners*.
163 Quoted in Cinquegrana, 'The Walls (And Wires) Have Ears', 815.
164 Mitra Ebadolahi, 'Warrantless Wiretapping Under the FISA Amendments Act', *Human Rights* 39, no. 3 (2013): 11–16. On how computerised surveillance experimented in the 1960-1970s – in particular the CIA's HYDRA database – foreshadowed the forms of surveillance that came to characterise the "War on Terror," see Jens Wegener, 'Order and Chaos." According to Wegener, "beyond personnel and technological continuities, one of the main legacies of the HYDRA-experience was its role in spurning the development of new systems of knowledge linking the investigation of transnational threats to quantitative computer-aided forms of analysis […]. These systems encouraged officers to think in terms of transnational social structures that had long existed at the intersection of several blind spots of the national security paradigm: fixed distinctions between internal and external security, the training of single area experts, and the legal gaps between national jurisdictions.'
165 According to the executive order, 'in order to improve the protection of sources and methods of intelligence, all members of the Executive branch and its contractors given access to information containing sources or methods of intelligence shall, as a condition of obtaining access, sign an agreement that they will not disclose that information to persons not authorized to receive it.' Gerald Ford, 'Executive Order 11905: United States Foreign Intelligence Activities, February 18, 1976', President of the United States, 18 February 1976, https://www.fordlibrarymuseum.gov/library/speeches/760110e.asp; The new strategy was based on the realisation that 'NDAs could prove a more effective means than the Espionage Act to censor authors because they did not leave it to the courts to determine the legality of the government's conduct, the extent to which the disclosure of information damaged national security, or whether arriving at a verdict required the disclosure of additional—including classified—information.' Sam Lebovic, 'From Censorship to Classification: The Evolution of the Espionage Act', in *Whistleblowing Nation: The History of National Security Disclosures and the Cult of State Secrecy*, ed. Kaeten Mistry and Hannah Gurman (Columbia University Press, 2020), 189.
166 William E. Colby, 'Letter from DCI on "Marihuana-Hashish" Epidemic on Personnel Security and Secrecy', 4 March 1975, https://www.cia.gov/readingroom/document/cia-rdp78-04163r000100130001-6; That policy developed over the years. An executive order adopted under the Reagan presidency generalised drug-testing, finding that 'The use of illegal drugs, on or off duty, by Federal employees in certain positions evidences less than the complete reliability, stability, and good judgment that is consistent with access to sensitive information and creates the possibility of coercion, influence, and irresponsible action under pressure that may pose a serious risk to national security, the public safety, and the effective enforcement of the law.' Ronald Reagan, 'Executive Order 12564: Drug-Free Federal Workplace', President of the United States, 15 September 1986, https://www.archives.gov/federal-register/codification/executive-order/12564.html.
167 Hannah Gurman and Kaeten Mistry, 'The Paradox of National Security Whistleblowing: Locating and Framing a History of the Phenomenon', in *Whistleblowing Nation: The History of National Security Disclosures and the Cult of State Secrecy*, ed. Kaeten Mistry and Hannah Gurman (Columbia University Press, 2020), 22.
168 Morton H. Halperin et al., *The Lawless State: The Crimes of the U.S. Intelligence Agencies* (Penguin Books, 1976), 10.

169 On the FBI's cover-up of its illegal investigations, see Scott, *Reining in the State*, 166.
170 'Report on Inquiry Into CIA-Related Electronic Surveillance Activities'.
171 John F. Blake 'Investigating the Topic of Creativity and Controls Within CIA (Memo from the Deputy Director for Administration)'. CIA, 7 October 1976. https://www.cia.gov/readingroom/document/cia-rdp80-00473a000700100009-9.
172 Letter, Director of Central Intelligence, Bush to Marsh, August 18, 1976. Quoted in Digital National Security Archive, 'Chronology: CIA Covert Operations II: The Year of Intelligence, 1975'.
173 Vince Davis and Stanfield Turner. "Comments on a Memo on Relationships Between CIA and Private Scholars" CIA, 31 May 1977. CIA CREST Record. https://www.cia.gov/readingroom/document/cia-rdp86b00985r000300080015-5.
174 Becker, 'CIA Ties with Academics: Dangerous Implications'.
175 David Wise, 'Campus Recruiting and the CIA', *The New York Times*, 8 June 1986, sec. Magazine.
176 Anonymous, 'The Yawn of the Computer Age', *Cryptolog*, January 1975.
177 Christopher Moran, 'Nixon's Axe Man: CIA Director James R. Schlesinger', *Journal of American Studies* 53, no. 1 (February 2019): 95–121.
178 Office of the Deputy Chief of Staff, Operations, 'Annual Historical Review U.S. Army Intelligence and Security Command, Fiscal Year 1978.' (Washington, D.C.: Department of Defense, 1 September 1978), 47, Digital National Security Archive.
179 'Federal Government Information Technology: Electronic Surveillance and Civil Liberties', Office of Technology Assessment, CIT-283 (Washington D.C.: U.S. Congress, October 1985), Digital National Security Archive.
180 Gary T. Marx. *Undercover: Police Surveillance in America*. Berkeley: University of California Press, 1988, 208.
181 The Carter administration had proposed a charter legislation, the National Intelligence Act of 1980, which would have 'largely authorized past abuses,' according to Poveda. Some congressmen still fought for more stringent restrictions. The Federal Intelligence Agencies Control Act of 1977, for instance, would have 'prohibited political surveillance and preventive action against U.S. citizens, protected whistleblowers, banned intrusive investigative methods, repealed the Smith Act, and terminated the authority of the attorney general to authorize domestic intelligence investigations. The use of paid informants in political groups was also banned.' See Poveda, 'The FBI and Domestic Intelligence', 208; George Lardner, 'Missing Intelligence Charters: No Reforms Enacted since Congressional Investigation', *The Nation* 227 (1978): 168. See also Townley, 'Spies, Civil Liberties, and the Senate', 21; on Carter's Vice-President and former Church committee member Walter Mondale's strategy to dodge the issue of charter legislations, see Scott, *Reining in the State*, 158.
182 The report is summarised in Judith Miller. 'Report to Reagan Aides Urges Ending Many Restrictions on U.S. Spying; First Meeting With Turner'. *The New York Times*, 21 November 1980, sec. Archives.
183 Ronald Reagan. 'Executive Order 12333: United States Intelligence Activities'. President of the United States, 81/12/4; Judith Miller. 'Reagan Broadens Powers of C.I.A., Allowing Spying Activities in the U.S.' *The New York Times*, 5 December 1981, sec. U.S.
184 "The new rules say Federal agents may investigate statements advocating criminal activity or indicating 'an apparent intent to engage in crime, particularly crimes of violence.'" Robert Pear. 'U.S. Agents Get Wider Latitude in Investigations'. *The New York Times*, 8 March 1983, sec. U.S.
185 For an overview of Reagan's intelligence oversight policy, see Stansfield Turner and George Thibault, 'Intelligence: The Right Rules', *Foreign Policy*, no. 48 (1982): 122–38.

186 The distinction is borrowed from Smist, *Congress Oversees the United States Intelligence Community, 1947–1994*.
187 Olmsted, *Challenging the Secret Government*, 175-178.
188 Leslie H. Gelb, 'Overseeing of CIA By Congress Has Produced a Decade of Support', *The New York Times*, 7 July 1986, sec. U.S.
189 Quoted in Johnson, *A Season of Inquiry Revisited*, 273.
190 United Press International. 'Summary of William Colby's Address at Casper College, Wyoming'. *United Press International*, 2 March 1984. https://www.cia.gov/readingroom/document/cia-rdp90-00806r000100200018-9.
191 Shen Ibrahimsadeh, Ibtehal Hussain, Bernardino León-Reyes, Ronja Kniep, Félix Tréguer, Emma Mc Cluskey, and Claudia Aradau. 'Timeline of Intelligence Surveillance Scandals'. GUARDINT Project Research Report, 1 December 2022. https://hal-sciencespo.archives-ouvertes.fr/hal-03952751.
192 The expression "governing anti-surveillance critique" is inspired by Science and Technology Studies scholar Sezin Topçu's work on techno-scientific controversies. See Sezin Topçu. 'From Resistance to Co-Management?: Rethinking Scientization in the Contestation of the Technosciences'. *Engaging Science, Technology, and Society* 8, no. 1 (2022): 128.
193 Katherine Anne Scott, *Reining in the State*, 7.
194 Johnson, 'The Church Committee Investigation of 1975 and the Evolution of Modern Intelligence Accountability'.
195 Pierre Bourdieu, *On the State: Lectures at the Collège de France, 1989–1992*, ed. Patrick Champagne et al., trans. David Fernbach (Cambridge Malden, MA: Polity, 2014), 29.
196 For a most recent illustration of this narrative, see: Risen, James. *The Last Honest Man: The CIA, the FBI, the Mafia, and the Kennedys—and One Senator's Fight to Save Democracy*. New York: Little, Brown and Company, 2023.
197 Tom Ginsburg and Tamir Moustafa, eds., *Rule by Law: The Politics of Courts in Authoritarian Regimes*, Illustrated edition (Cambridge UK; New York: Cambridge University Press, 2008); Sidney Tarrow, *War, States, and Contention: A Comparative Historical Study*, 1 edition (Ithaca; London: Cornell University Press, 2015).
198 Christopher H. Pyle, review of *'Spying on Americans: Political Surveillance from Hoover to the Houston Plan'*, by Athan Theoharis, *Political Science Quarterly* 94, no. 3 (1979).
199 Kniep, Ronja, Lina Ewert, Bernardino León-Reyes, Félix Tréguer, Emma Mc Cluskey, and Claudia Aradau. 'Towards Democratic Intelligence Oversight: Limits, Practices, Struggles'. *Review of International Studies*, 16 March 2023, 1–21

References

Anonymous. "The Yawn of the Computer Age." *Cryptolog* (January 1975).

"Army Surveillance of Civilians: A Documentary Analysis." Report by the Staff of the Subcommittee on Constitutional Rights, Committee on the Judiciary. Washington, D.C.: U.S. Senate, August 1972. https://famguardian.org/Subjects/PropertyPrivacy/GovSurv/senate-judiciary_army-surveillance-civilians.pdf

Baltimore sun. "Self-Discipline Tied to Secrecy." February 25, 1962. CIA CREST Record. https://www.cia.gov/readingroom/document/cia-rdp70-00058r000200100088-2.

Barrett, David M. "Secrecy, Security, and Sex: The NSA, Congress, and the Martin–Mitchell Defections." *International Journal of Intelligence and CounterIntelligence* 22, no. 4 (September 4, 2009): 699–729. 10.1080/08850600903143320.

Bigo, Didier. "Violence Performed in Secret By State Agents: For an Alternative Problematisation of Intelligence Studies." In *Problematising Intelligence Studies*, edited by Hager Ben Jaffel and Sebastian Larsson, 220–240. Routledge, 2022.

Blanton, Thomas. "Wiretap Debate Déjà Vu: Electronic Surveillance From the Cold War to Al-Qaeda." *The National Security Archive*. February 4, 2006. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB178/index.htm.

Blum, Richard H. ed. *Surveillance and Espionage in a Free Society*. New York: Praeger Publishers, 1972.

Bonelli, Laurent, Hervé Rayner, and Bernard Voutat. "Contestations et (re) légitimations du renseignement en démocratie." *Cultures Conflits* 114–115, no. 2 (2019): 7–28.

Bourdieu, Pierre. *On the State: Lectures at the Collège de France, 1989–1992*, edited by Patrick Champagne, Remi Lenoir, Franck Poupeau, and Marie-Christine Rivière, translated by David Fernbach. Cambridge Malden, MA: Polity, 2014.

Bourdieu, Pierre. *On the State: Lectures at the College de France, 1989–1992* 1 edition. Cambridge Malden, MA: Polity Press, 2014.

Bourdieu, Pierre. *The Field of Cultural Production: Essays on Art and Literature*. Columbia University Press, 2011.

Boylan, James. "Declarations of Independence." *Columbia Journalism Review* 25, no. 4 (1986): 29.

Bush, George. "Letter of DCI to Honorable Jack Brooks, Chairman Committee on Government Operations House of Representatives on Amending the Privacy Act." CIA. April 28, 1976. CIA CREST Record. https://www.cia.gov/readingroom/document/cia-rdp77m00144r000800070028-0.

Chamayou, Grégoire. *The Ungovernable Society: A Genealogy of Authoritarian Liberalism*. John Wiley & Sons, 2021.

Chamberlain, John. "Camelot Equaled "Costalot"." *The Times Herlad*. August 14, 1965. CIA Crest Record. https://www.cia.gov/readingroom/document/cia-rdp73-00475r000102540004-2.

Chen, Adrian. "After 30 Years of Silence, the Original NSA Whistleblower Looks Back." Gawker, November 12, 2013. https://www.gawker.com/after-30-years-of-silence-the-original-nsa-whistleblow-1454865018.

Chief of Information Processing Staff. "Briefing for the DCI on Automatic Data Processing in the Agency." October 25, 1969. CIA CREST Record. https://www.cia.gov/readingroom/document/cia-rdp78-04723a000100100032-0.

Chief of Information Processing Staff. "Strengthening the Information Processing Structure of the Agency." CIA, September 15, 1969. CIA CREST Record. https://www.cia.gov/readingroom/docs/CIA-RDP78-04723A000100100029-4.pdf.

"Chronology of Significant MHCHAOS Correspondence." CIA, October 14, 1975. https://www.cia.gov/readingroom/document/01481988.

""Church Report": Foreign and Military Intelligence (Book I)." Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Washington, D.C: U.S. Senate, 1976.

""Church Report": Intelligence Activities and Rights of Americans (Book II)." Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Washington, D.C: U.S. Senate, 1976.

""Church Report": Supplementary Detailed Staff Reports on Intelligence Activities and Rights of Americans (Book III)." Senate Select Committee to Study

Governmental Operations with Respect to Intelligence Activities. Washington, D.C: U.S. Senate, 1976.

Cinquegrana, Americo R. "The Walls (And Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978." *University of Pennsylvania Law Review* 137, no. 3 (1989): 793–828. 10.2307/3312277.

Clotworthy, Orrin. "Some Far-out Thoughts on Computers." *Studies in Intelligence (CIA Journal)* 6, no. 4 (1962). https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-56-no-4/some-far-out-thoughts-on-computers.html.

CODIB. "R&D for Intelligence Processing: Recommendations for Invigorating and Coordinating the Community's Development of Data-Handling Systems." U.S. Intelligence Board, 1965. https://www.cia.gov/readingroom/document/cia-rdp80b01139a000500140001-3.

Colby, William E. "Letter from DCI on "Marihuana-Hashish" Epidemic on Personnel Security and Secrecy." March 4, 1975. https://www.cia.gov/readingroom/document/cia-rdp78-04163r000100130001-6.

"Computer/Operations Research Skill Development Program." September, 1969. CIA CREST Record. https://www.cia.gov/readingroom/docs/CIA-RDP78-04723A000100160006-3.pdf.

"Congress Can Keep a Secret." Congressional Records. U.S. Congress, March 28, 1963. https://www.cia.gov/readingroom/document/cia-rdp75-00149r000700040034-7.

CounterSpy (2:3) Vol. 2. 3 vols. Fifth Estate, 1975.

Crewdson, John M. "CIA Is Criticized Over Watergate." *The New York Times* (July 3, 1974): sec. Archives. https://www.nytimes.com/1974/07/03/archives/cia-is-criticized-over-watergate-minority-staff-in-senate-says.html.

Crewdson, John M. "Ford Asks Intelligence Disclosure Curb." *The New York Times* (February 19, 1976): sec. Archives. https://www.nytimes.com/1976/02/19/archives/ford-asks-intelligence-disclosure-curb.html.

Davis, Hugh 'Buck'. "A People's History of the CIA Bombing Conspiracy (the Keith Case); Or, How the White Panthers Saved the Movement." Ann Arbor District Library, 2010. https://aadl.org/freeingjohnsinclair/essays/peoples_history_of_the_cia_bombing_conspiracy.

Davis, James K. *Assault on the Left: The FBI and the Sixties Antiwar Movement*. Westport, Conn: Praeger, 1997.

Director of Central Intelligence. ""Interagency" Computers' Reported by NBC News." January 13, 1975. CIA CREST Record. https://www.cia.gov/readingroom/document/cia-rdp80m01133a000600080005-0.

Directorate of Sciences and Technology. "Office of Computer Services: Computer Systems Plan for the Period 1971–1975." Central Intelligence Agency, February 1971. https://www.cia.gov/readingroom/document/cia-rdp80-01003a000100070001-7.

Donner, Frank J. *The Age of Surveillance: The Aims and Methods of America's Political Intelligence System*. Vintage Books, 1980.

Dover, Michael. "U of M Bombed." *Fifth Estate Magazine* (November 13, 1968). https://www.fifthestate.org/archive/65-october-31-november-13-1968/u-of-m-bombed/.

Duval, Mark. Memo to John Marsh, folder "Draft Plan for ICG, 10/75," Box 11,. Michael Raoul-Duval Papers, Gerald R. Ford Presidential Library, October 23, 1975.

Ebadolahi, Mitra. "Warrantless Wiretapping Under the FISA Amendments Act." *Human Rights* 39, no. 3 (2013): 11–16.

"Federal Government Information Technology: Electronic Surveillance and Civil Liberties." Office of Technology Assessment. CIT-283. Washington D.C.: U.S. Congress. Digital National Security Archive, October 1985. https://nsarchive.gwu.edu/sites/default/files/documents/6442924/National-Security-Archive-Office-of-Technology.pdf.

"Federal Data Banks, Computers, and the Bill of Rights." Hearings before the Subcommittee on Constitutional Rights of the Committee on the Judiciary. Washington DC: U.S. Senate, March 1971.

Ford, Gerald. "Executive Order 11905: United States Foreign Intelligence Activities, February 18, 1976." President of the United States, February 18, 1976. https://www.fordlibrarymuseum.gov/library/speeches/760110e.asp.

Fowler, Bridget. "Pierre Bourdieu on Social Transformation, with Particular Reference to Political and Symbolic Revolutions." *Theory and Society* 49, no. 3 (April 1, 2020): 439–463. 10.1007/s11186-019-09375-z.

Franklin, Ben A. "Federal Computer Amass Files on Suspect Citizens." *The New York Times* (June 27, 1970). https://www.cia.gov/readingroom/document/cia-rdp80-01601r001400120001-6.

Franklin, Ben A. "Surveillance of Citizens Stirs Debate." *The New York Times* (December 27, 1970): sec. Archives. https://www.nytimes.com/1970/12/27/archives/surveillance-of-citizens-stirs-debate-government-surveillance-of.html.

"From George to Don (on Pending Congress Legislation)." CIA, June 3, 1975. CIA CREST Record. https://www.cia.gov/readingroom/document/cia-rdp77m00144r001100180006-8.

Gelb, Leslie H. "Overseeing of CIA By Congress Has Produced a Decade of Support." *The New York Times* (July 7, 1986): sec. U.S. https://www.nytimes.com/1986/07/07/us/overseeing-of-cia-by-congress-has-produced-decade-of-support.html.

Ginsburg, Tom, and Tamir Moustafa, eds. *Rule by Law: The Politics of Courts in Authoritarian Regimes*, Illustrated edition. Cambridge UK; New York: Cambridge University Press, 2008.

Gurman, Hannah, and Kaeten Mistry. "The Paradox of National Security Whistleblowing: Locating and Framing a History of the Phenomenon." In *Whistleblowing Nation: The History of National Security Disclosures and the Cult of State Secrecy*, edited by Kaeten Mistry and Hannah Gurman, 9–44. Columbia University Press, 2020. 10.7312/mist19416-003.

Haines, Gerald K. "The Pike Committee Investigations and the CIA: Looking for a Rogue Elephant." *Studies in Intelligence* (Winter 1998–1999). https://www.cia.gov/static/688ed924c2cec7a35d79051ab51bc4b5/CIA-Pike-Committee-Investigations.pdf.

Hale, Jeff. "Wiretapping and National Security: Nixon, the Mitchell Doctrine, and the White Panthers." PhD in History, Louisiana State University, 1995. https://digitalcommons.lsu.edu/gradschool_disstheses/6015.

Hale, Jeff A. "The White Panthers' "Total Assault on the Culture"." In *The American Counterculture of the 1960's and 70's*, edited by Peter Braunstein and Michael William Doyle, 125–156. Routledge, 2001. 10.4324/9780203615171-8.

Halperin, Morton H., Jerry J. Berman, Robert L. Borosage, and Christine M. Marwick. *The Lawless State: The Crimes of the U.S. Intelligence Agencies*. Penguin Books, 1976.

Helms, Richard. "International Connections of U.S. Peace Groups." Memorandum for the President. CIA, November 15, 1967. https://aavw.org/special_features/govdocs_cia_abstract02_excerpts.html.

Hentoff, Nat. "After Ellsberg: Counter-Spy." *The Village Voice* (July 19, 1973).

Herald Traveler. "A Good Move by U-Mass." April 30, 1972. https://www.cia.gov/readingroom/docs/CIA-RDP80-01601R000200050002-6.pdf.

Hersh, Seymour M. "C.I.A. Is Linked to Strikes In Chile That Beset Allende." *The New York Times* (September 20, 1974): sec. Archives. https://www.nytimes.com/1974/09/20/archives/cia-is-linked-to-strikes-in-chile-that-beset-allende-intelligence.html.

Hersh, Seymour M. "Ford Names Rockefeller to Head Inquiry into CIA: Wants Report in 90 Days." *The New York Times* (January 6, 1975): sec. Archives. https://www.nytimes.com/1975/01/06/archives/ford-names-rockefeller-to-head-inquiry-into-cia-wants-report-in-90.html.

Hersh, Seymour M. "Huge CIA Operation Reported in US Against Antiwar Forces, Other Dissidents, In Nixon Years." *The New York Times* (December 22, 1974). https://www.cia.gov/readingroom/document/cia-rdp77-00432r000100340001-9.

Hersh, Seymour M. "C.I.A's Work Unimpeded By Inquiries and Reports, Officials of Agency Assert." *The New York Times* (November 10, 1975): sec. Archives. https://www.nytimes.com/1975/11/10/archives/cias-work-unimpeded-by-inquiries-and-reports-officials-of-agency.html.

Hinton, Elizabeth. *America on Fire: The Untold History of Police Violence and Black Rebellion Since the 1960s*. New York, NY: Liveright, 2021.

Hochman, Brian. *The Listeners: A History of Wiretapping in the United States*. Harvard University Press, 2022.

Hoover, J. Edgar. "Now: Instant Crime Control in Your Town." *Popular Science* (January 1967).

Hoover, J. Edgar, Rcihard Helms, William Bennett, and Noel Gayler. "Special Report of the Interagency Committee on Intelligence (Ad Hoc) (Huston Plan)." Washington, D.C., June 25, 1970. https://nsarchive.gwu.edu/document/20423-national-security-archive-doc-01-special-report.

Horowitz, David. "U.S. Electronic Espionage: A Memoir." *Ramparts* (August 1972).

Horrock, Nicholas M. "Rockefeller Inquiry Clears C.I.A. of Major Violations." *The New York Times* (June 3, 1975): sec. Archives. https://www.nytimes.com/1975/06/03/archives/rockefeller-inquiry-clears-cia-of-major-violations.html.

House Select Committee on Intelligence. *The Unexpurgated Pike Report: Report of the House Select Committee on Intelligence (1976)*. McGraw Hill, 1992. http://archive.org/details/PikeCommitteeReportFull.

Ibrahimsadeh, Shen, Ibtehal Hussain, Bernardino León-Reyes, Ronja Kniep, Félix Tréguer, Emma Mc Cluskey, and Claudia Aradau. "Timeline of Intelligence Surveillance Scandals." GUARDINT Project Research Report, December 1, 2022. https://hal-sciencespo.archives-ouvertes.fr/hal-03952751.

Igo, Sarah E. *The Known Citizen: A History of Privacy in Modern America*, Illustrated edition. Cambridge, Massachusetts: Harvard University Press, 2018.

"Inter-Division Information Unit (IDIU)." Department of Justice. U.S. National Archives, December 5, 1978. https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0060/nc1-060-79-02_sf115.pdf.

Jeffreys-Jones, Rhodri. *The FBI: A History* 6/28/08 edition. New Haven, Conn.: Yale University Press, 2008.

Johnson, Loch K. *A Season of Inquiry Revisited: The Church Committee Confronts America's Spy Agencies*. Lawrence: University Press of Kansas, 2015.
Johnson, Loch K. "The Church Committee Investigation of 1975 and the Evolution of Modern Intelligence Accountability." *Intelligence and National Security* 23, no. 2 (April 1, 2008): 198–225. 10.1080/02684520801977337.
Kaiser, Frederick M. "Legislative History of the Senate Select Committee on Intelligence." Congressional Research Service, The Library of Congress, 1978. https://sgp.fas.org/crs/intel/leghist.pdf.
Kalman, Laura. *Right Star Rising: A New Politics, 1974–1980*. New York: W. W. Norton & Company, 2010.
Keller, William. *The Liberals and J. Edgar Hoover: Rise and Fall of a Domestic Intelligence State*. Princeton, N.J: Princeton University Press, 1989.
Kessler, Ronald. "FBI Had Files on Congress, Ex-Aides Say." *The Washington Post* (January 19, 1975).
Klein, Jennifer. *For All These Rights: Business, Labor, and the Shaping of America's Public-Private Welfare State*. Politics and Society in Modern America. Princeton University Press, 2006.
Kniep, Ronja, Lina Ewert, Bernardino León-Reyes, Félix Tréguer, Emma Mc Cluskey, and Claudia Aradau. "Towards Democratic Intelligence Oversight: Limits, Practices, Struggles." 1–21 March 16, 2023. 10.1017/S0260210523000013.
Lardner, George. "Missing Intelligence Charters: No Reforms Enacted since Congressional Investigation'. *The Nation* 227 (1978): 168.
Lebaron, Frédéric. "Pouvoir." In *Dictionnaire d'économie politique: Capitalisme, institutions, pouvoir*, edited byColin Hay and Andy Smith, 358–364. Presses de Sciences Po, 2018. https://www.cairn.info/dictionnaire-d-economie-politique–9782724623109-page-358.htm.
Lebovic, Sam. "From Censorship to Classification: The Evolution of the Espionage Act." In *Whistleblowing Nation: The History of National Security Disclosures and the Cult of State Secrecy*, edited by Kaeten Mistry and Hannah Gurman, 123–152. Columbia University Press, 2020. 10.7312/mist19416-003.
León-Reyes, Bernardino. "Towards a Reflexive Study of Intelligence Accountability." In *Problematising Intelligence Studies*, edited by Hager Ben Jaffel and Sebastian Larsson, 30–47. Routledge, 2022.
Lepore, Jill. *If Then: How the Simulmatics Corporation Invented the Future*. New York: Liveright, 2020.
Levine, Yasha. *Surveillance Valley: The Secret Military History of the Internet*. PublicAffairs, 2018.
Lopez, Dan, Thomas Blanton, Meredith Fuchs, and Barbara Elias. "Veto Battle 30 Years Ago Set Freedom of Information Norms." Electronic Briefing Book. National Security Archive, November 2004. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB142/index.htm.
Marx, Gary T. *Undercover: Police Surveillance in America*. Berkeley: University of California Press, 1988.
Mayhew, David R. *Divided We Govern: Party Control, Lawmaking and Investigations, 1946–2002*. Yale University Press, 2005.
McCarthy, David. "The CIA & the Cult of Secrecy." PhD in History, College of William & Mary, 2008. https://scholarworks.wm.edu/etd/1539623335.
McGhee, Dorothy. "Counterspy Exposes "Techno-Fascism"." *Daily Rag*, April 20, 1973. https://www.cia.gov/readingroom/docs/CIA-RDP88-01314R000100370024-9.pdf.

Medsger, Betty. *The Burglary: The Discovery of J. Edgar Hoover's Secret FBI* 1st edition. New York: Knopf, 2014.

"Military Surveillance of Civilian Politics: Report of the Subcommittee on Constitutional Rights." Committee on the Judiciary. Washington, D.C.: U.S. Senate, 1973. https://ia601906.us.archive.org/18/items/Military-Surveillance-Civilian-Politics-1973/MilitarySurveillanceCivilianPolitics.pdf.

Mistry, Kaeten. "The Rise and Fall of Anti-Imperial Whistleblowing in the Long 1970s." In *Whistleblowing Nation: The History of National Security Disclosures and the Cult of State Secrecy*, edited byKaeten Mistry and Hannah Gurman, 123–152. Columbia University Press, 2020. 10.7312/mist19416-003.

Mohr, Charles. "A.C.L.U. Testifies Intelligence Bill Would Legalize "Abuses" by C.I.A." *The New York Times* (March 26, 1980).

Moran, Christopher. "Nixon's Axe Man: CIA Director James R. Schlesinger." *Journal of American Studies* 53, no. 1 (February 2019): 95–121. 10.1017/S002187581700086X.

Morrison, Trevor. "The Story of United States v. United States District Court (Keith): The Surveillance Power." *Columbia Public Law & Legal Theory Working Papers* (November 20, 2008).

Morrison, Trevor W. "The Story of United States v. United States District Court (Keith): The Surveillance Power." Presidential Power Stories - Columbia Public Law Research Paper. Foundation Press, 2008.

Muskie, Edmund S. "Letter to DCI on the Creation of a Joint Investigation of Warrantless Wiretapping and Electronic Surveillance." Congressional Records. Washington, D.C, July 2, 1974. https://www.cia.gov/readingroom/docs/CIA-RDP80M01009A003100010030-9.pdf.

Neocleous, Mark. "From Social to National Security: On the Fabrication of Economic Order." *Security Dialogue* 37, no. 3 (September 2006): 363–384.

Office of the Deputy Chief of Staff, Operations. "Annual Historical Review U.S. Army Intelligence and Security Command, Fiscal Year 1978." Digital National Security Archive. Washington, D.C.: Department of Defense, September 1, 1978. https://nsarchive.gwu.edu/document/16792-office-deputy-chief-staff-operations.

O'Leary, Jeremieah. "McCone Claims Computers Could Aid in Investigations." *Evening Star* (October 5, 1964).

Olmsted, Kathryn. "Reclaiming Executive Power: The Ford Administration's Response to the Intelligence Investigations." *Presidential Studies Quarterly* 26, no. 3 (1996): 725–737.

Olmsted, Kathryn S. *Challenging the Secret Government: The Post-Watergate Investigations of the CIA and FBI*, Illustrated edition. Chapel Hill: University of North Carolina Press, 1996.

Pear, Robert. "U.S. Agents Get Wider Latitude in Investigations." *The New York Times* (March 8, 1983): sec. U.S. https://www.nytimes.com/1983/03/08/us/us-agents-get-wider-latitude-in-investigations.html.

Pforzheimer, Walter. "Memo from the Historical Intelligence Collection on Counterspy for the Deputy Director of Central Intelligence." CIA, May 14, 1973.

Poveda, Tony G. "The FBI and Domestic Intelligence: Technocratic or Public Relations Triumph?" *Crime & Delinquency* 28, no. 2 (April 1982): 194–210. 10.1177/001112878202800202.

Powers, Richard Gid. *G-Men, Hoover's FBI in American Popular Culture*. Southern Illinois University Press, 1983.

Pyle, Christopher. "Looking back at the CONUS Intel Scandal." Interview by Félix Tréguer. Telephone, May 20, 2022.
Pyle, Christopher H. "CONUS Intel: The Army Watches Civilian Politics." *The Washington Monthly* (January 1970).
Pyle, Christopher H. "CONUS Revisited: The Army Covers Up." *The Washington Monthly* (July, 1970).
Pyle, Christopher H. "Review of *'Spying on Americans: Political Surveillance from Hoover to the Houston Plan'*, by Athan Theoharis." *Political Science Quarterly* 94, no. 3 (1979): 542–544. 10.2307/2150470.
Rafalko, Frank J. *MH/CHAOS: The CIA's Campaign Against the Radical New Left and the Black Panthers*. Annapolis, MD: Naval Institute Press, 2011.
Ransom, Harry Howe. "Congress and the Intelligence Agencies." *Proceedings of the Academy of Political Science* 32, no. 1 (1975): 153–166. 10.2307/1173624.
Reagan, Ronald. "Executive Order 12564: Drug-Free Federal Workplace." President of the United States, September 15, 1986. https://www.archives.gov/federal-register/codification/executive-order/12564.html.
Reed, Isaac Ariail. "Can There Be a Bourdieusian Theory of Crisis? On Historical Change and Social Theory." *History and Theory* 54, no. 2 (2015): 269–276.
"Report of the Republican Task Force on Privacy." Congressional Records. Washington, D.C.: U.S. House of Representatives, September 12, 1974. https://www.cia.gov/readingroom/document/cia-rdp76m00527r000700140101-6.
"Report to the President by the Commission on CIA Activities Within the United States ("Rockefeller Report")." Washington, D.C: White House, 1975. https://www.cia.gov/library/readingroom/docs/CIA-RDP80M01133A000900130001-5.pdf. https://www.aarclibrary.org/publib/contents/church/contents_church_reports_rockcomm.htm.
Richardson, Peter. "The Perilous Fight: The Rise of Ramparts Magazine, 1965–1966." *California History* 86, no. 3 (2009): 22–69.
Ripley, Anthony. "Views and Background of Ford Commission Investigating C.I.A." *The New York Times* (January 14, 1975): sec. Archives. https://www.nytimes.com/1975/01/14/archives/views-and-background-of-ford-commission-investigating-cia.html.
Risen, James. *The Last Honest Man: The CIA, the FBI, the Mafia, and the Kennedys—and One Senator's Fight to Save Democracy*. New York: Little, Brown and Company, 2023.
Rockefeller, Nelson A. "Report to the President by the Commission on CIA Activities Within the United States." CIA CREST Record. Washington, D.C: White House, June 1975. https://www.cia.gov/readingroom/document/cia-rdp80m01133a000900130001-5.
Rohde, Joy. *Armed with Expertise: The Militarization of American Social Research during the Cold War*. American Institutions and Society. Ithaca, NY: Cornell University Press, 2013.
Rosberg, Gerald M. "CIA Recruiting Cancelled To Avoid Student Protest." *The Harvard Crimson* (February 27, 1967). https://www.thecrimson.com/article/1967/2/28/cia-recruiting-cancelled-to-avoid-student/.
Rowan, Ford. *Technospies: The Secret Network That Spies on You, and You*. New York: Putnam, 1978.
Salpukas, Agis. "Stony Brook Computer Center Occupied by S.D.S. Protesters." *The New York Times* (May 9, 1969): sec. Archives. https://www.nytimes.com/1969/05/09/archives/stony-brook-computer-center-occupied-by-sds-protesters.html.

Sapiro, Gisèle. "Structural History and Crisis Analysis." In *Bourdieu and Historical Analysis*, edited by Philip S. Gorski, 266–285. Durham, NC: Duke University Press Books, 2013.

Scott, Katherine Anne. *Reining in the State: Civil Society and Congress in the Vietnam and Watergate Eras*. University Press of Kansas, 2013.

Shapiro, Ira S. "The Foreign Intelligence Surveillance Act: Legislative Balancing of National Security and the Fourth Amendment." *Harvard Journal on Legislation* 15, no. 1 (1978 1977): 119–204.

Sheinkin, Steve. *Most Dangerous: Daniel Ellsberg and the Secret History of the Vietnam War*. Roaring Brook Press, 2015.

Silvert, Kalman H. "American Academic Ethics and Social Research Abroad: The Lessons of Project Camelot." In *The Rise and Fall of Project Camelot: Studies in the Relationship Between Social Science and Practical Politics*, edited by Irving Louis Horowitz, 80–106. M.I.T. Press, 1967.

Smist, Frank John. *Congress Oversees the United States Intelligence Community, 1947–1994*. University of Tennessee Press, 1994.

"Some Books on the CIA." CIA, March 23, 1973. https://www.cia.gov/readingroom/document/cia-RDP75-00793R000300050002-0.

Stampnitzky, Lisa. "Experts, States, and Field Theory: Learning from the Peculiar Case of Terrorism Expertise." *Critique Internationale* 59, no. 2 (2013): 89–104.

Stern, Sol. "A Short Account of International Student Politics & the Cold War with Particular Reference to the NSA, CIA, Etc." *Ramparts* (March 1967).

"Subversion of Law Enforcement Intelligence Gathering Operations: Organizing Committee for a Fifth Estate." U.S. Government Printing Office, 1976.

Summers, Anthony. *Official and Confidential: The Secret Life of J. Edgar Hoover*. Open Road Media, 2012.

"Surveillance Technology: Joint Hearings." Subcommittee on Constitutional Rights of the Committee on the Judiciary and the Special Subcommittee on Science, Technology, and Commerce of the Committee on Commerce. Washington, D.C.: U.S. Senate, September 10, 1975.

"Surveillance Technology: Policy and Implications (An Analysis and Compendium of Materials)." Staff Report of the Subcommittee on Constitutional Rights of the Committee on the Judiciary and the Special Subcommittee on Science, Technology, and Commerce of the Committee on Commerce. Washington, D.C.: U.S. Senate, 1976.

Tarrow, Sidney. *War, States, and Contention: A Comparative Historical Study*, 1 edition. Ithaca; London: Cornell University Press, 2015.

"The Evolution of the U.S. Intelligence Community-An Historical Overview." Intelligence Resource Program. Federation of American Scientists, 1996. https://www.govinfo.gov/content/pkg/GPO-INTELLIGENCE/html/int022.html.

The History of the University of Michigan. "1968 Bomb Explosions at U-M." December 19, 2019. https://historyofum.umich.edu/panther-by-the-tail/.

The Latin American Times. ""Project Camelot" Fizzle Brings Cut in Army Funds." August 27, 1965. https://www.cia.gov/library/readingroom/document/cia-rdp75-00149r000500320018-6.

The New York Times. "Text of Ford Plan on Intelligence Units and Excerpts From His Executive Order." sec. Archives. February 19, 1976. https://www.nytimes.com/1976/02/19/archives/text-of-ford-plan-on-intelligence-units-and-excerpts-from-his.html.

The New York Times. "Year of Intelligence." sec. Archives. February 8, 1975. https://www.nytimes.com/1975/02/08/archives/year-of-intelligence.html.

Topçu, Sezin. "From Resistance to Co-Management?: Rethinking Scientization in the Contestation of the Technosciences." *Engaging Science, Technology, and Society* 8, no. 1 (2022): 128.

Townley, Dafydd. "Spies, Civil Liberties, and the Senate: The 1975 Church Committee." PhD, University of Reading, 2018. http://centaur.reading.ac.uk/83873/.

Tréguer, Félix. "Intelligence Reform and the Snowden Paradox: The Case of France." *Media and Communication* 5, no. 1 (March 22, 2017): 17–28.

Trenta, Luca. "'An Act of Insanity and National Humiliation': The Ford Administration, Congressional Inquiries and the Ban on Assassination." *Journal of Intelligence History* 17, no. 2 (July 3, 2018): 121–140. 10.1080/16161262.2018.1430431.

Turner, Stansfield, and George Thibault. "Intelligence: The Right Rules." *Foreign Policy* no. 48 (1982): 122–138. 10.2307/1148270.

Vries, Tity de. "The 1967 Central Intelligence Agency Scandal: Catalyst in a Transforming Relationship between State and People." *The Journal of American History* 98, no. 4 (2012): 1075–1092.

Waldrop, M. Mitchell. *The Dream Machine: J.C.R. Licklider and the Revolution That Made Computing Personal*. Penguin Books, 2002.

"Warrantless Wiretapping and Electronic Surveillance." Joint Hearings Before the Subcommittee on Administrative Practice and Procedure and the Subcommittee of Constitutional Rights Of …, and the Subcommittee on Surveillance of the Committee on Foreign Relations, 93-2, Apr. 3, 8, 1974; May 8, 9, 10, and 23, 1974. U.S. Senate, 1974.

Watson, Douglas. "NSA: America's Huge Vacuum Cleaner of Intelligence." *The Washington Post* (March 2, 1975).

Wegener, Jens. "Order and Chaos: The CIA's HYDRA Database and the Dawn of the Information Age." *Journal of Intelligence History* 19, no. 1 (January 2, 2020): 77–91. 10.1080/16161262.2019.1697539.

Weinberger, Sharon. *The Imagineers of War: The Untold Story of DARPA, the Pentagon Agency That Changed the World*. New York: Knopf, 2017.

Weiner, Tim. *Legacy of Ashes: The History of the CIA*. Knopf Doubleday Publishing Group, 2008.

Wellerstein, Alex. *Restricted Data: The History of Nuclear Secrecy in the United States*, First edition. Chicago: University of Chicago Press, 2021.

Wiener, Norbert. "A Scientist Rebels." (January 1947).

Willmetts, Simon. *In Secrecy's Shadow: The OSS and CIA in Hollywood Cinema 1941–1979*. Edinburgh University Press, 2017.

Zalnieriute, Monika. "Procedural Fetishism and Mass Surveillance under the ECHR." *Verfassungsblog* (blog) (June 2, 2021). https://verfassungsblog.de/big-b-v-uk/.

2 Transformations of the transnational field of secret services

The reasons for a systemic crisis of legitimacy?

Didier Bigo

Introduction

A problem of legitimacy at the international scale

My central claim in this chapter is this: the transformation of the scale of action in terms of secret violence and surveillance of large segments of the population has disrupted the tacit agreement that the use of secret services, alone or in coalition, among democracies is a necessity for peace and stability in the world. Their legitimacy is at stake in a systemic way, and not just, as it used to be, for a brief moment after an operation that went beyond what was tolerated. This radically changes the current situation. The denial of transnational control of operations, led in coalition by the most powerful countries of the global North, is increasingly untenable. Proposals are on the table and need to be discussed. If there is strong resistance from some governments and some of the doctrine, the practitioners are aware of the seriousness of the problem.[1]

Certainly, there have been disputes and demands for greater oversight in the past, but, as the previous chapter has shown, they have not been very effective because they have always been limited to a few national rules and have not touched on the arrangements between different intelligence services. Oversight and monitoring were limited to the national realm, based on the idea of the supremacy of state sovereignty and the acceptance of a discretionary power in matters of national security to use force in covert operations abroad (and sometimes within the territory).[2] But after the episodes of extraordinary rendition and remote torture programmes carried out by the CIA and its accomplices around the world, the large-scale surveillance of Internet users organised by the NSA and the so-called Five Eyes Plus network disclosed by Edward Snowden, and more recently the use of spyware marketed by private companies that allows the targeting of opponents, journalists and human rights defenders, it is impossible not to admit that the core of the problem of secret violence and surveillance based on suspicion by multiple actors needs to be regulated internationally.

For decades, the transnational field of intelligence, which links the US agencies with most of the services of the Global North and operates largely

DOI: 10.4324/9781003354130-3

outside the Anglophone Five Eyes network, has benefited from a lack of control by supervisory authorities, based on specific arrangements, such as the third-party rule, which prohibit their access to the exchange of information from foreign sources.[3] Now, with the change in the scale of the activities of the secret services, their interconnections with issues far removed from espionage and their impact on everyday life, it is urgent to redraw the boundaries between covert action, war, policing, and travel controls to show that democracies act differently from other regimes.

Beyond the traditional universe of espionage abroad and the surveillance of potential enemies at home by means of infiltration techniques, whose cleavage between military and police, foreigner and citizen, and abroad and national territory has been both consistent and regulatory for the life of the so-called intelligence services at the national level, the last 30 years have seen a widening of the activities of the various intelligence services, especially with their strong involvement in "non-geographical" threats and the specialisation in counter-terrorism and even counter-globalised crime. Secrecy, once confined to defence matters, has been extended to other domains of security. Numerous activities of security management professionals have been "intelligentified", and the agents involved in these controls, as well as their various targets, have become constitutive parts of this universe of "suspicion and prediction" in expansion, destabilising the relations and boundaries that the previous universe of secret services had with politics, security, law, justice, and the nation.[4] On the basis of our research over the last eight years, we can condense our various findings into the current combination of four main factors (transnational coalition, preventive ideology, digital capacities, and marketization) that contribute to this qualitative transformation of the field of transnational secret services and its current dynamic of expansion, diversification, deepening and diffraction, modifying its relations with all the other professional fields that constitute politics, security, and law in democracies.[5]

Reframing the problem outside intelligence studies, why? And how?

From a methodological point of view, and before presenting these four factors in detail, it is important to take a step sideways from classical intelligence studies. The way in which authors who consider themselves to be intelligence scholars frame the problem of the legitimacy of secret services in democracies at the international level is by naturalising as essential facts of human nature the existence of competition between states and clandestine forms of violence between them.[6] The argument, when exposed, claims that the survival of the nation-state requires violence that is exempt from moral and legal judgement. This is supposed to be true and to continue forever, but this transhistorical "Hobbesian performativity of violence as necessity" works very badly when sovereignty today is diffracted into a coalition of different states of the Global North, because it reveals by default the question of leadership and responsibility, and the shared and unequal elements of mixed sovereignties

brought into the alliances. To the argument of necessity, these authors add what we can call a veil of wishful ignorance based on "secrecy" and "trust".[7] This relationship implies a blind obedience to the decision of the executive under the advice of the secret services in return for the protection of the "people". This framework therefore limits the questions about the role of the secret services and their contribution to peace in the world, or their role as an accelerator of violence and escalation of conflicts. The only choice is to assign the protection of peace to the secret services of democracies and aggression to the secret services of other regimes. This summa division into two camps may have a historical basis, but only if observations show that the difference in the political regime reveals a series of practices in which the norms of democracy and the rule of law effectively limit the use of violence and surveillance. It is impossible to ignore the reality of the mimesis between the actions of the services when they have to confront undemocratic regimes and their reluctance to respect limits. There is often a feeling within the services that agents can work "freely" if they have been validated by the executive to carry out an illegal action, even if they knew it was against international human rights, thus protecting impunity on both sides (services and politicians). Insisting on dualism and refusing to verify practices, as classical intelligence studies do, has consequences. It obscures the reality of intermediate categories such as illiberal democracies, democracies with neo-despotic executives through the lack of power of the judiciary. It silences intermediate effective situations where representative democracies use quasi-permanent regimes of exception and derogation for their military and police operations, as well as their regional and neo-colonial ambitions, often renamed under the label of their responsibility for world or regional stability.

With this doxa, they produce what some critical researchers have called a policy of non-knowledge or forgetting, which from the outset repeats a predicate, a dogma, that cannot be challenged by empirical verification and questioning.[8] In this framework of intelligence studies, the services are, by definition, and forever, legitimate instruments, and when scandals emerge, they are about the "excesses" of some individuals or a service, but they are never a sign of de-legitimisation. This question is immediately rhetorically dismissed as "unrealistic" and coming from "dreamers". If there is any "excess" in the actions of the services, it is only because governments and secret services have been too quick to treat some of their own citizens who claim their rights as if they were foreign spies and agents of revolution and chaos. The ideas of the fight against impunity, of redress, of supervision, and of control, may exist, but they must protect the services themselves from destabilising investigations; they must be exercised strictly within a sovereign territory, and they must be organised as forms of control to check that the services do not exceed the order and mandate given to them by the executive of their country. There may be monitoring of shadow fights, but it is always limited in scope and applies only to internal struggles between professionals, never to the politics of a country and even less to a coalition between democratic countries.

Contrary to this series of assumptions that construct the doxa of intelligence studies, an international political sociology (IPS) reopens the question of the practices of secret services worldwide, thinking about the limits and the boundaries of this social universe of democracies that use force, in which democratic legitimacy presupposes imposing on each country and on the coalition itself, self-limitations in terms of force, forms of surveillance, and a permanent control against forms of despotism of the executive and/or of the transnational guilds of the services themselves.[9] Instead of accepting the frame of national sovereignty, national security, and state secrets as taken for granted, it is highly relevant to question the international politics as such.[10] Internal critics within intelligence studies have already raised the question of the proper level of analysis when speaking of the activities of secret services in the Western world, mainly through the lens of transgovernmentalism, but they have not dared to abandon the nationalist doxa and its methodological bias.[11] This explains the absence of studies on the coalitions of secret services, apart from the narratives of some former agents or informants. Despite its central importance, it is reduced to an additional layer of a "big" actor, a national state policy, often the United States. On the other side, some recent critiques revive a neo-colonialism accusation but are prisoners of the same nationalist bias and fail to understand the transversal and transnational process by which the expansion of coalition activities takes place and creates major problems in the world. A recent book has made a synthesis of these limitations of "intelligence" studies in general and has proposed alternative frames of understanding, including that of IPS.[12]

The first part of this paper will describe how the practices of the coalitions of secret services of democratic countries went wrong and will analyse the main reasons and factors of the current transformations of the transnational field of professionals of security services working together in the global North, beyond the label of the Five Eyes or Five Eyes+. By examining the recent evolution in which the coalition network has extended its asymmetrical chains of collaborators to the point where many scholars speak of 12 or 19 eyes, including beyond the number of secret services, private companies selling technologies or data, and contributions to the intelligence process by law enforcement and border control agencies, this first part will insist on the lengthening of the chains of interdependence between actors, the existence of which Norbert Elias had already made an essential criterion for analysing the soundness of institutions.[13] The second part will explain the diffraction of responsibilities and authorities, breaking the power of traditional sovereign actors and destabilising the links between security and national borders in the collection, interception, storage, sorting, and exploitation of information. As we will see, most actors do not have the capacity to do everything on their own. They produce information together, they share procedures, and the number of cases in which they deal with each other's little secrets rather than big state secrets breaks the so-called ring of secrecy. This transnational dimension is therefore of the utmost importance and cannot be reduced to

occasional cooperation between different national security communities. On the contrary, it is this transnational dimension that today organises relations between the various national groups of secret services and explains their fights and solidarities. Having established this as one of the most important problems for social science research into the use of covert force and surveillance by such a conglomerate of diverse actors, that we can call transnational guilds, the final part of the paper will discuss the legitimacy gap that exists at the transnational level and its implications for democratic politics internationally and nationally. I will examine why some top actors continue to deny the problem and the arguments and tools they use to avoid it, but I will also show that from within the profession itself, at the operational level, a project is emerging for an effective form of democratic control that would redraw effective boundaries between what is permissible and what is unacceptable as acts of violence perpetrated by democratic regimes.

Widening, deepening, entanglement, and diffraction of the boundaries of the transnational field of secret violence in democracies

Looking at the recent past: what went wrong? Extraordinary rendition and torture, large-scale intrusive digital surveillance, and worldwide selling of spying tools

Extraordinary rendition and torture

Countless cases of gross human rights abuses against innocent people have been labelled after the fact as "collateral damage" or "false positive" targets by secret services who refuse to accept their mistakes or the consequences of their actions. If this was an implicit rule in the days of espionage and applied to very limited cases, it is no longer the case. Denial covers thousands of cases, sometimes for years. The continued detention of people in Guantanamo Bay 20 years after the fact, in order to prevent the services from being held accountable and at least to make amends or apologise for the torture committed at the time, is just one example. These forms of injustice are not the work of a few overzealous individuals but are often the result of flawed institutional assessments based on poorly organised intelligence sharing, inadequate patterns of suspicion, arbitrary calculations of anticipation. Consequently this ends up to reframe the status of innocence which is no longer sufficient to prevent the use of covert violence against individuals.

In recent years, some Global North governments and their services have conveniently chosen to ignore and even erase major crises – including extraordinary rendition, torture, and the National Security Agency's mass surveillance of targets, including their close allies, revealed by Edward Snowden. We know that in this context, national intelligence services have chosen to loyally protect their cooperation with US agencies, rather than cooperate with national political, oversight, and judicial authorities and question the legality of what they have been asked to do by these international intelligence alliance networks and collaborations.

Indeed, there have been several cases of intelligence officers and/or private actors spying on their superiors and even heads of state. What could be considered treason has had far-reaching consequences for the stability of the intelligence alliance, which have generally not been properly investigated. In the United States, for example, CIA personnel have been exempted from any legal consequences, and some of the highest legal and political authorities continue to teach in major universities, including John C. Yoo.[14] These examples illustrate the lack of justice and impunity for perpetrators of gross human rights violations.

Torture has been used, albeit as one of the non-derogable rights, after attempts were made to justify it as part of an effective fight against threats to national security.[15] This has also been the case with unnecessary forms of surveillance, in particular the extension of intrusive techniques to large groups of suspects without necessarily having any analytical knowledge of them beyond algorithmic correlations, and often without effective direct or indirect links in terms of causality assessed by means other than electronic data.

The case of the CIA's programme of extraordinary rendition and torture by proxy is less exceptional than it appears. It has created a pattern of behaviour that has been adopted by illiberal or authoritarian regimes that have seen it as a relaxation of the rules on this issue. Kenya, for example, has adopted this practice to the detriment of its neighbours. Let us briefly recall that these practices are precisely linked to the structuring of international coalitions that include the participation of so-called allied services that are also based in authoritarian regimes and/or dependent on funds allocated by the United States. These ad hoc collaborations with the CIA were based on a series of regional networks involving allied services abroad, archipelagos of detention centres in South Asia, the Horn of Africa, and even Eastern Europe – Poland, Romania, Kosovo, and among others. These practices, once exposed, have led to a significant change in public acceptance of the activities of democratic intelligence services. They have also affected the trust, credibility, and legitimacy of democratic intelligence activities beyond the United States. Close allies of the United States, including Germany, Italy, Switzerland, Sweden, the United Kingdom, and, to some extent, France, have been negatively affected.[16]

Large-scale intrusive surveillance by the NSA

Another case, less blatant in terms of intensity of violence but affecting millions of people around the world, concerns the large-scale surveillance operated by the so-called Five Eyes alliance around the NSA, which has formalised secret laws between itself in order to rationalise, outside of a public legal framework, forms of cooperation between its various agencies. As the Snowden disclosures of its practices have shown, the NSA has largely operated beyond the so-called Five Eyes countries (US–UK–Canada–Australia–New Zealand), with the involvement of many other countries (Sweden, Germany, France, Belgium …),

for a large-scale intrusive surveillance in which the ratio between the people under surveillance and the flimsy elements of evidence was so high that it can be considered that this type of surveillance has indiscriminately affected large groups of the population in their fundamental rights to thought, opinion, expression, and private life, beyond any form of necessity and proportionality regarding the operation and its consequences for the rule of law and the existence of a democratic regime. This has largely been studied by the best specialists over the last 10 years and cannot be denied, despite the efforts of some revisionist journalists and the strategic communications of the services to minimise what happened.[17]

Spying software

More recently, the sale of low-cost "spyware" by private companies has further undermined the belief in a democratic space, with the almost systematic targeting of human rights defenders, investigative journalists, and intellectuals by governments or authoritarian political parties to whom companies based in democratic countries have sold this software, one of the best known, but not the only one, being Pegasus.

In fact, in recent years, the Israeli company NSO has been selling various software for spying on mobile phones, adding a new crucial element to the fear of permanent surveillance that threatens all forms of freedom, equality, and rights that democracies consider to be enshrined in their laws and practices. By making it possible in practice for many actors in the world (authoritarian governments in the Third World, political parties, private companies …) to obtain, at a low cost, the capabilities to target their opponents or competitors by means of intrusive surveillance that is very difficult to trace, they have generalised the number of entities that can carry out illegitimate surveillance. Some analysts have ironically spoken of the "democratisation of surveillance tools", pointing to the huge proliferation of these tools and the fact that "spying" and malevolent manipulation, sometimes leading to killing, are now "on the market" and no longer restricted to the world's major secret services.

Thanks to the capacities of some NGOs (Amnesty Lab, Citizen Lab …), the tools used by the NSOs have been discovered. The number of journalists and human rights organisations targeted by these tools shows that this is not an anti-terrorist tool reserved for such cases, but a general and decentralised attack on fundamental freedoms. This is not as new as the public believes, but this "third wave" of illegitimate practices strengthens the opposition to the use by the secret services of democratic countries of tools that are authoritarian by design. A subterranean but very strong current of anger is now rising against this use of surveillance tools, and the whole legitimacy of the various regimes that allow their services to use these tools, or do not prevent private companies from doing so, is at stake.

Even before the Pegasus scandal, as shown in the case of Amesys, German and French companies were helping the authorities to track their opponents

in countries such as Syria, Libya, and Egypt. A veritable market for intrusive surveillance has emerged, increasing the ability of all political groups, not just governments, to spy on and track their citizens and political opponents.

The proliferation of this type of software and the ease with which it can be used has fundamentally changed the scope of spying, the threshold for defining suspicious targets, and the use of targeted surveillance practices in large numbers and on a routine basis. These changes are so drastic that one can speak of an effective de-monopolisation, or de-oligopolisation, of a nation-state's secret intelligence services over this kind of activity.[18] Unless mechanisms of international control beyond the Wassenaar Arrangement are put in place, all countries, including the most powerful, risk losing fundamental principles of state sovereignty.[19]

Taken together, these three elements (impunity for torture, large-scale intrusive surveillance, and the spyware womb) justify the idea, defended in this chapter, that the legitimacy of the actions of the various coalitions of actors can no longer be immune to democratic control. Nevertheless, this seems to be the case, and we need to explain why and how impunity persists by examining the four main factors of transformation that lead to a significant expansion of the field and its de-responsibility.

Factors of transformation: Coalition of services, preventive–predictive ideology, digital capacities, privatisation, and marketisation

Coalitions of secret services

The first element is the systematisation of coalitions of secret services, working together in asymmetrical chains of interdependence on a Global North scale, diffracting political responsibilities internationally, and targeting countless groups of individuals who are sorted out and placed on watch lists. If their origins go back to the Second World War, and if they were the backbone of the Cold War and NATO, their informal organisational arrangements under the name of "Five Eyes" (FIVEYS) specifically linked the intelligence services of the United States, the United Kingdom and, to a lesser extent, Canada, Australia, and New Zealand. The clandestine foreign and signals intelligence services of these countries worked closely together and used the same technologies against their adversaries, but also against some of their allies.[20]

Since the end of the 1990s, and especially since 2001, they have developed into a series of powerful asymmetric networks, which, on a regional or global scale, bring together almost all the intelligence services in a given area, according to their specific crafts, but with very different "privileges" within the coalition, depending on past collaboration and present usefulness. Under US leadership (NSA, CIA), they have been a key vector for implementing the idea that, against the spread of terror and other transversal threats, it was necessary to achieve a global reach in terms of co-production of information. Cooperation was no longer a choice concerning the results of the various

information collections acquired at national level, but a necessity in the accumulation of traces and interception of data, structuring an effective awareness against multiple potential dangers. Each US agency has made its technology available and allows its use to varying degrees, but as a counterpart they will have a say in the priorities of the objectives of the various networks. It has been said that this "common good" is mutually beneficial, but it has also signed the death of the control of the acquisition of secret information by one government alone, and with it the belief in an autonomy of national security and national sovereignty, even if some governments are denying this structural change.

Today, the term "Five Eyes" should be replaced by the concept of highly structured networks that regularly involve France, Germany, and Sweden with the Anglo-Saxon "Five", based on specific crafts, as in the old notion of guilds.[21] It exists with the SIGINT services around the NSA, but not only. The CIA, despite the bad memories of the 2000s, also has a highly structured network of correspondents in Europe and, in addition to information from the NSA and its correspondents, has its own system for monitoring Internet and telephone communications around the world. Finally, we must not forget the very important network of the FBI and its police correspondents around the world and in Europe, as well as the regularity of its links with Interpol and Europol, where a great deal of data also circulates. So, as analysts, we are faced with this multiplicity of transnational networks, or as we propose, with different "transnational guilds" whose solidarity is based on a specific type of craft, and we have to work on the extent to which they themselves are interoperable or maintain very specific access rights. What is clear, however, is that the strictly national scale, and with it the idea of national security communities facing each other, is obsolete. However, daring to say so and publishing information about co-production of information sharing does not sit well with politicians and certain services whose very existence could be questioned in smaller countries such as New Zealand.[22]

This major shift in the emergence of transnational networks for the co-production and exchange of data for surveillance purposes explains the correlative increase in the number of staff employed by these agencies, and some have spoken of an industrial complex of surveillance for intelligence purposes, bringing together several million actors in the Global North. While it is dangerous to make such an aggregation of different missions and agencies, it is clear that there has been massive recruitment in all agencies, not just those specialising in SIGINT. New professional skills have been demanded by all agencies and are closely linked to digitisation and the construction of suspicious data. They are the operators of the key strategic move that organises the fight against the unpredictable risks and threats of our time, which begin with the ease of tracing people's activities on the net (data and metadata), even if identification is more complex, especially due to online anonymity.

Preventive ideology of security: Suspecting the present, in order to know the future by totalising the past data

The second element, which accompanies and reinforces the first, is the ideological move to claim that a preventive security, acting coercively before the facts, can anticipate risks and accurately predict the future actions of potential perpetrators implicated in worst-case scenarios.[23] This preventive dimension is not the opposite of a repressive one, which acts with non-security means on the causes of the problems, but, on the contrary, a future-oriented coercion based on different categories of suspicion, organised through correlations of structural positions and trajectories of previous behaviours, where some series of data make it possible to sort them according to criteria of danger, in order to put these "suspicious objects" (persons, money) under surveillance and, finally, to act coercively on some of the targets. This belief in achieving predictive knowledge and detecting the unknown through a global awareness of the totality of movements has been developed by neo-conservative thinkers who believe that "trends" in human nature trump the possibility of change at the last moment. They have tried to validate a "science of prediction" and its truth value, which is justified by the fact that, in the case of mass destruction, catching one dangerous terrorist among a hundred people justifies detaining ninety-nine innocent people for a while. Even if this argument has often been ridiculed, it has captured the imagination of almost all secret services, justifying that their "art" is now supported by "science".[24] It has also, and this may be a reason for its generalisation beyond one kind of ideology, been contemporary with the development of the digital realm and its legitimisation as a new tool for politics in general.

Digital technologies: Tracing the past, calculating big data, finding correlations

The third element is the advent of digital technologies and their extraordinary capacity to leave traces of past actions that can be retrieved afterwards, thus improving a time machine that can be used for surveillance purposes. Activities on computers, smart phones, and the Internet can be collected, intercepted, and stored very easily, and the data, if sufficiently large, can be analysed by algorithms that organise a rationality between different a priori aleatory correlations. Weak signals of potential relationships between different elements can emerge from the visualisation of millions of activities and can be used to design algorithms about a specific danger. These correlations are not causalities, the profiles of suspicion are not evidence, and the trends are not accurate knowledge of the future, especially when people know that they are being analysed from their past routines and trends, but this pretence of knowing the future as if it were already known from the past, as a grammatically perfect future, is used by security professionals as one of their strongest justifications for organising large-scale intrusive surveillance. This

data politics of surveillance is cheap, easy, does not require human infiltration, and simulates a global reach of the "big data" apparatus, which gives some credibility to their conclusions about potential dangers and avoids them being seen as contemporary astrologists. Even if there are doubts in most intelligence services about their capacity for the future, especially in policing, the SIGINT services have seen politicians agreeing to invest in them far more than any other intelligence services. This has changed the internal balance of power between the different types of services and contributed hugely to the dynamic of expansion.[25] It has also brought new types of actors from non-public activities into the field of secret services.[26]

Marketisation and privatisation

The fourth element is this privatisation and marketisation of personnel acting in secret for governmental interests, whose numbers and types of activities have multiplied and diversified the practices of violence and surveillance based on suspicion. As long as the globalisation of the threat was fought only between states and ultra-minority clandestine groups, there was the impression of a shared monopoly of the resources of covert violence by states and their intelligence services. One could then say that, despite the diversity of regimes, each state had a common interest. However, when one considers the role of private companies that sell surveillance technologies, the question arises of a lucrative and non-strategic use of surveillance tools that goes far beyond counter-terrorism and contributes to the de-monopolisation of sovereign spying tools. In selling such technologies, which have very often been classified as dual-use cybersecurity technologies, it was expected that companies selling their technologies to other regimes would verify that the use of these cybersecurity weapons would not be used as a tool for activities that threaten civil societies and democratic processes. But recent practice shows the opposite, and these companies have not verified or, more problematically, have obtained compliance licences from their "line" ministries or commissions responsible for verifying the legality of arms sales before selling these technologies.[27] More broadly, beyond the suppliers of surveillance technologies, the emergence of large transnational private companies with their own agendas has for many years interfered at the highest scale with this vision of politics reduced to interstate activities and considering private companies as "contractors". The number of people directly or indirectly involved in surveillance operations, which are linked to a preventive logic of security rather than economic profit, has structurally transformed the former field of secret violence. Surveillance has an industrial character, it is a routine activity, especially in terms of storage, even in countries that fight against these practices through privacy laws. The number of companies working to develop algorithms specifically designed for "risk analysis" and data profiling of suspects is constantly increasing, especially in North America. This is the same phenomenon regarding the number of companies that act as data

brokers and sell their results to various services and design new categories for organising suspicion.[28] Susan Strange has shown the extent to which large private companies have their own diplomatic games, and we can continue by showing that they are also in capacity to design their own "anti-diplomacy".[29] Some so-called private actors, including but not limited to the GAFAs, are in a strong position vis-à-vis many states when it comes to design, frame, and conduct surveillance on a transnational scale. Obviously, the main digital platforms and the organisers of the diffusion of social networks are not only working for, but are also co-producing innovations in terms of the possibilities of remote surveillance and coercion. In addition, few specialised companies advertise that their results can be used for "true" prediction with a very reduced number of "false positives" and claim that machine learning as well as artificial intelligence will realise the dream of a "pre-crime society, monitoring the future", and they are believed by all the actors who want to see such a world of total control that they call peace and order.[30]

A dynamic of expansion with centrifugal effects? Assessment of the limits and trajectories at work, mutual reinforcement, de-responsibilisation of core actors, and rise of the periphery

Enlargement, diversification, widening, and deepening implications

Each of these elements has contributed to the gradual development of the others, generating an expansion of the field of secret services, whose new logic colonises or at least destabilises military, police, and judicial institutions and practices. The increase in personnel, the lightness of the tools, the multiplication of targets, and the intrusion into the everyday life of citizens give the impression of an "unbound" security logic of prevention and prediction.[31] But this spiral does not strengthen the traditional actors in the field. Certainly, espionage and counter-espionage activities are still considered by many to be the most prestigious acts by actors in the field, but they are outnumbered by cybersecurity specialists, private companies and think tanks that analyse so-called open sources (OSINT) and reject the "old secrets" and their know-how. The ecosystem of espionage, which was the core activity of very specialised professionals, is now only a very small part of what is at stake in forms of secret violence and surveillance.[32] Some of the actors interviewed speak of a decline in the core speciality of (counter)espionage, which has recently been reinvigorated by the return to what they call the serious fight: the invasion of Ukraine, but they despair of the evolution of the "profession" and the disappearance of its codes of honour and rituals of secrecy. The external military services have their geospatial technologies almost intact, but even in this field they are already in competition with private companies, and they are increasingly obliged to cooperate with agencies specialising in the SIGINT Internet surveillance and localisation of targets. The number of civilians within their services is changing their habits. They see the development of internal whistleblowers as a consequence of this opening of the field

to non-public agents. On the internal security side, the techniques of infiltration, of proactive policing by human means, are only valued when they are complemented by the use of digital technologies, which accelerate the speed of investigations but also undermine the work on evidence and the transmission to the judiciary of reasonable suspicions calibrated by causalities and facts. On the contrary, the agencies that were (and in some countries still are) dependent on other agencies for their services are in any case on the rise in terms of autonomy, budget, and staff. They have more links with the new actors coming from the control of travellers and money, the private companies, and the digital entrepreneurs. Once on the periphery, these actors have more and more influence on the priorities of the field in terms of the hierarchy of threats and dangers. The newcomers are thus becoming more and more autonomous from the dominant groups which have asked them to contribute to this expansion of secret activities, because they believed (mostly wrongly) that they could manage the full chain of interdependencies along their own interests. This creates a centrifugal dynamic that distorts and entangles different logics of practices in many places but at the cost of the loss of control of the previously dominant agents.[33]

Diffraction and centrifugal effects in interstitial spaces

The penetration and entanglement of activities due to the combination of a preventive and predictive approach, with methods of data totalisation, sorting according to categories of suspicion and danger, and inscription on watch lists, have created a diffraction of secret violence and surveillance in all fields related to the purpose of identifying individuals (travellers, Internet users in particular). The detective logic of locating and identifying individuals in order to track them down before they do something wrong has opened up, beyond traditional proactive policing, a suspicion of unknown (to the police) people. Counter-terrorist investigation units, which already had specific powers and were shrouded in secrecy, joined the preventive, predictive logic, which often allowed them to respond immediately after a bombing that they were not without resources but on the trail of suspects. Sometimes, through the collection of video cameras and digital traces in public travel, they were able to arrest members of clandestine actions on the spot or very soon after. Even if it was not a prediction, the speed of discovery after the fact was considered a great success and attributed to the services. The New York marathon, the 2015 Brussels attacks were celebrated, even if in some cases other rapid actions led to mistakes, and Jean Charles de Menezes, a Brazilian electrician was killed in the London Underground due to false identification parameters.[34] Nobody insisted on the number of "false positives", when people were investigated, threatened, and arrested for no reason other than a weak correlation, a hairdresser in a suspect's phone book, the owner of an old mobile phone, and so on.

Calculations about the coefficient of links between two people, based on the notion of degree of separation, were used by the various services to justify

searches at a level of three, but the Guardian reminded people that at six degrees of separation, everyone using the Internet is connected to another person, therefore at three degrees of separation, if the initial number of addresses was 100, the results is more than 2.8 million people. It gave a sense of what "targeted search" meant.[35] The internal security services of the FBI, MI5, and the Met in London, or the DGSI in France, were partly seduced by the possibilities opened up by this "total awareness" of data, or at least by the correlations emerging from interoperable databases to which the police had access. They pushed hard for access to other databases on criminal justice, border control, migrants, and even asylum seekers or international travellers. While some countries of the global North have narrowed the scope of the search to terrorist suspects only, others have opened it up to foreigners, migrants, minorities, or social services, but this has provoked a lot of resistance from NGOs, from some trade unions of the services obliged to adapt to these policies, and from privacy obligations defended by lawyers. Most elements of this diffraction have depended on data protection legislation in different countries, with the European Union imposing greater restrictions on data protection than other regions, but nevertheless accepting the principle of interoperability and access for law enforcement agencies (including some intelligence services) to these data highways, linking law enforcement and border agencies at the global North level, and allowing the identification of individuals seeking to travel.[36]

More recently, the "data avalanche" and its consequences on overriding disturbing effects have often backfired due to court rulings and internal resistance, with too many people on the lists for the wrong reasons, and the bureaucratic obligation to check them anyway, forcing "less" work on the "real" suspects confirmed by traditional methods.[37] For the internal security services, it was very bad publicity to have people on watch lists who could continue to operate and act, and some of the counter-terrorist units are now reluctant to use these "predictive" methods. The same trajectory of overconfidence and reluctance happened with the Border Force and Customs and Immigration. While they were very happy with the introduction of computer management and e-gates, they became increasingly unhappy with the multiplication of watch lists to be checked. In both police and border guard organisations, specific e-services were created by their personnel to use digital tools, but without applying the preventive–predictive logic of security.

In police organisations, whether in North America or Europe, this logic is considered counterproductive, multiplying too much false information and destroying the police's evidence-based, administrative, and penal logic, which implies that suspects will eventually be transferred to the criminal justice system. For the border guards, the complaint is even more acute, and they refuse to be turned into verifiers of the data of the watch lists of suspects at the borders, losing their own initiatives as well as the confidence of the public. They claim that their daily work is being undermined by this will to prevent by digital means and that the internal struggles between the services that

specialise in intelligence and predicting the movements of so-called migrant flows (including refugees) and those that want to control on a case-by-case basis are being intensified. The difficult relations between the European agencies of Frontex and EU-LISA, as well as the tensions within Frontex between different services, epitomise these deep disagreements about the penetration of a different logic of work into their social universe and explain how much oversight in now on the agenda.[38] It divides those who see it as an opportunity to join the formal intelligence community, while the others resist such a move.[39] The fight against money laundering and corruption, which is closely linked to banking and digital technologies, has also been affected by this attraction towards preventive, predictive analysis and imitation of the practices of the secret services, but in this field the new services have been more successful in their way of framing the links between themselves and the traditional secret services, nevertheless the banks are uncomfortable with this evolution that transforms their clients into permanent potential suspects.[40]

The consequences of this "spiral", which implies a widening of the field of practices interconnected by the preventive–predictive logic, the digitisation, and the use of secrecy by actors beyond the public services, are numerous. It begins with the breaking down of the traditional rules of the game of espionage and counter-espionage and their dilution in cybersecurity (war and crime) and continues with the multiplication of actors who do not have a traditional public character and are called "contractors", finishing off the dominance of the secret services inherited from the Cold War. The global scale of coalition interventions (extraordinary rendition, international NSA network for mass surveillance …) has definitely changed the existing relations between the international field of politics, the use of secret violence around the world, the relations between the secret services and their own politicians and, more fundamentally, the relations between these politicians and the large segment of the population in democracies who feel that they are nevertheless living in a surveillance society based on unfounded suspicions.

The centrifugal development of new technologies and services linked to the digital cyberspace used for security rather than freedom has profoundly affected the intimacy of many people, while complexifying who is responsible. It is this effect of the violence done to the intimacy of people's lives, their sense that everything is going wrong and that democracies are no longer democracies, that we want to focus on, because it creates this legitimacy gap that we consider crucial to understand the current situation of world politics.

The intrusion of the question of legitimacy at the transnational scale: unease, denial, and hidden transcripts

A sense of unease and a crisis of systemic legitimacy?

A diffuse but constant sense of having entered a downward spiral that fuels illiberal regimes, in which the executive emancipates itself from parliamentary and judicial control through the routinisation of emergency measures, has led

to the belief that a surveillance society is emerging in which freedom and the presumption of innocence are no longer respected.[41] The role of the coalitions of secret services and their actions is central. The discomfort of using the Internet, once a joy of discovery and new freedom, is linked to the perception that large corporations and secret services are watching and spying for profit or to know our more intimate thoughts. Privacy and data protection are no longer the preserve of lawyers, they are the subject of every discussion in a café. This influence of the "big others" and the belief that privacy is being manipulated can, in turn, lead to the destabilisation of existing governments and democratic mechanisms. This has led to a sense of betrayal by elites (both public and private) in some circles, fuelled by fears of losing privacy and a belief in conspiracy theories. It has sparked a search for alternative truths and a rejection of elections. Other circles, however, have expressed resignation and have declared that they are not interested in politics at all, except for a smaller part that has mobilised in an increasingly radical way in defence of the rights in question, which paradoxically has led to a systematic questioning of governments, regardless of their reform efforts. Whatever the three conflicting tendencies it can create in politics, they all converge on a questioning of democratic politics, because of the attitude of politicians and their professionals of secret violence and surveillance.

These major implications for the everyday citizens of these democracies, who consider themselves to be affected by these activities, cast doubt on the relevance of a system of legitimacy that is centrally based on the acceptance of suspicion and surveillance by governments that claim to be democratic. The need to use secret violence in the name of protecting people is seen as not only unnecessary, but counterproductive, since it is itself a cause of anxiety. Security does not reassure, it increases insecurity.

This current legitimacy deficit could have been accepted, and the discussion of some legal solutions could have been used to limit the problem, but as the chapters of Arnaud Kurze, as well as the chapter of Elspeth Guild and Sophia Soares will show in this book, the obsession of the main actors to defend their old arrangements, such as the third-party rule, which are not adapted to change, leads in addition to a second major issue, which is that the role of privacy as the key element for allowing other rights and freedom of individuals to reconstruct a limit against secret violence and surveillance, has been under attack, instead of being seen as the solution. As the last chapter shows very convincingly, the best option is to upgrade privacy to a non-derogatory right in order to avoid some of the current justifications for surveillance and violence, too quickly accepted by some too deferent national courts. The question of the existence of transnational mechanisms to control the boundaries of a field in which the difference between liberal representative and authoritarian regimes is clear will continue to be with us until the legitimacy gap is closed or at least reduced.[42] However, far from working to show these differences in objectives and practices, the actors in the coalition or at the national level have sought to maintain and strengthen their

discretionary powers and their will to have no controllers or supervisors independent of the executive of their own country.

Denying the problem of transnational surveillance and the role of the third-party rule

Instead of recognising the problem, it seems that the main coalition governments (notably the United States, United Kingdom, and France) have adopted a strategy of denial and have used the third-party rule as a form of deadlock to block the development of transnational supervision. It seems that the US policy for all its lead agencies has been clearly to reject a "fin de non recevoir" to inquiries by supervisory bodies and courts. More precisely, any information transmitted to judicial or political authorities without the prior consent and knowledge of the service at the source of the information had to be sanctioned as a transgression. Any faulty or deviating service would thus be excluded from any future information exchange.

In order to justify such an interpretation, which places the supervisors (even if they have the highest level of confidentiality) as outsiders, the actors generally consider that it is an "absolute necessity" to respect the rule of non-transmission of information to a third party without the prior authorisation of the original sender of the information, since cooperation between Member States is voluntary and each national sovereignty is at risk if a country does not respect this rule. It would therefore be inconceivable for the supervisory authorities of other countries to have access to the information, even if they were involved in its co-production. Any attempt to divulge the information without consent, or to ask how another segment of the information was obtained, would be seen as a betrayal of the "trust" between members of the full intelligence community in this context. FVEY member services that have contributed to a global scope will have to obey, and any breach by themselves or their superiors will jeopardise their honour and overall standing within the community.

Of course, the third-party rule may appear to be reciprocal in theory, but in practice it depends on the capacity of the different services and their access (or not) to the tools that allow them to search the data themselves or by asking others to send them the results. At the heart of this asymmetry, the US intelligence services continue to have disproportionate power in relation to others. The intelligence services of France and, with minor modifications, the United Kingdom and Australia are also becoming increasingly aggressive in their desire to maintain their position. They continue to believe, wrongly, that democratic oversight prevents them from pursuing global or regional policies, thus hampering their influence in the areas where they feel they have a responsibility (and interest) to act. On the contrary, some countries have embarked on reforms to modify the traditional means of control over secret violence of public and private actors, including when they are coalescing and/or masking their collaboration. NGOs have welcomed this different mood but

this trend in favour of tighter control seems nevertheless until now to be limited to small states in Europe, and to New Zealand.[43] This difference regarding oversight may depend less on sovereignty argument than on a better appreciation of the necessity of democratic limits, even if it touches foreign affairs. The proponents of this trend towards transnational oversight, or at least greater cooperation between supervisors and national authorities, do not all consider that it is a way of overcoming the legitimacy gap, but in their view it may be a first step towards a solution. In addition, cooperation between different supervisors will contribute to a better autonomy of the whole system, at a better cost, by sharing tasks in financial situations that are always disproportionate to the detriment of the supervisors. It could also increase their efficiency by giving them a real overview of the whole of the operations, a position which is now partly shared by the supervision of the services belonging to Canada and Germany. More importantly, the distinction between the different organisations in terms of their specific craft shows that the idea of much-needed oversight is shared by many within the operational services, especially those of internal security and the military, which are more reluctant to continue with the preventive–predictive model favoured by the SIGINT Internet services. On the contrary, the latter, especially when they have their specific agency, favour the justification of surveillance and refuse as much as possible a control of their activities based on the storage of data and privacy rights. They propose not to remain silent, but to actively fight the legitimacy gap by using advertising campaigns to "rebrand" the legitimacy of their services in a different way. After an attempt of the CIA to do so in 2015, GCHQ was the first to use with some success and the support of private advertisement firms, this "new policy" in the United Kingdom. This "strategic communication" about regaining "trust" in order to convince the national "public" of the citizen is now also being adopted in the United States and France, playing with historical documentaries, films, and series that are less exotic than James Bond, and theoretically more attractive to recruit new personnel by the realism of the occupation they film.[44] Praised by some as an attempt to increase transparency or seducing some postmodern critics with their enterprise, their campaign is nevertheless seen by most insiders as breaking the traditional rules of silence, confusing politics with marketing, and reinforcing the unaccountability of politicians. They fear that, far from relegitimising the services, this policy of soft lobbying of their own citizens will, on the contrary, provoke an even stronger backlash against the services themselves. They are willing to support the small states' movement for better control of international coalitions and for the creation of a mechanism that is sufficiently autonomous to question the politicians in charge of the executive, including the head of state.

As a result, the current stalemate in opening up the question of legitimacy at the international level and accepting the idea that there must be serious mechanisms of control at this level revolves, on the one hand, around the positions that the actors occupy within the broader national

struggles and, on the other, around the solidarity they can receive from their foreign counterparts.

Hidden transcripts*[45]*; regaining a sense of limits with regard to the centrifugal dynamics to be taken into account

The evidence of recent decades shows that the so-called predictive capacity of a logic of preventive suspicion, based on technologies that promise much but produce very few results in the social world of human behaviour (unlike some results in the physical or biological sciences), is almost nil compared to chance. The operational added value of some undercover operations ends up being lost in a universe of bureaucratic statistics and profiles that do not match the objectives and take a long time to resolve. The problem of ignorance is transformed into the even greater problem of a constant and time-consuming search for mistakes and mix-ups. Professionals often complain about this "dispossession" of the political meaning of intelligence issues and a kind of obedience to the machine, which prearranged as a form of knowledge of its own, successive sorting out logics that conflate. Some actors speak of Kafkaesque logics in which unrealistic objectives leads are followed on the basis of dubious correlations derived from data that are so shared and so co-constructed, that nobody claims to be the original source, and these results are often seldom supported by concrete elements of identification. So, in the end, there is a recourse by these operational actors to their "common sense", to their "intuition", as the ultimate criterion of choice when it comes to concentrating on a few potential perpetrators of serious crimes. Many are therefore calling for less data and more analysis in order to contain the four centrifugal dynamics that we have analysed and which divide the various professions that contribute to what they call themselves "operational intelligence", namely: firstly, to avoid becoming accomplices to acts that are deeply illegitimate and unworthy of the profession; secondly, to limit the co-production of data and drastically reduce the number of cases arriving on their desks in favour of more qualitative approaches, i.e. thirdly, to re-establish precise frameworks and information pipelines reserved for certain specialists, against the idea of "fusion centres" and "global data"; and fourthly, to use private companies only for delegated tasks and to better control their field of intervention and their logic of influence, or even of decision, by imposing much stricter rules on the sale of technologies; in short, to set concrete and coherent limits to what has become unlimited and incoherent.

These observations, which come from many professionals in different intelligence services and from SIGINT, HUMINT, and OSINT activities, are all linked to the idea of "excess", which may have something to do with technology, but which is mainly due to a change in the allocation or lack of political responsibility. These difficulties, which are already acute at national level, are exacerbated in multinational coalitions for the exchange of secret

information, especially when the "heart" or "core" of the network, in most cases the agencies of the United States of America, does not assume its leading role, nor do the allied countries assume their structural dependence in the collection and asymmetric co-construction of intelligence.

The actors we met therefore want to have a say, but they explain that their narrative is like a hidden transcript, well known among insiders, but unable to easily break out of the official discourse and the strategic communication used by the heads of the services and the politicians.

To be clear, none of these actors is nostalgic for a distant past. They accept that traditional intelligence techniques are changing significantly because of the overwhelming volume of data and the ease of access to commercially available data, in the absence of sufficient legal and political safeguards to prevent disproportionate access or misuse. What they want is to regain a "sense of play" and many are prepared, against the advice of their superiors, to accept rigorous surveillance that gives them a renewed sense of the boundaries between what is wrong, punishable, and what is not.

In conclusion, the fragility of this thin dynamic of interstitial spaces of state violence, surveillance and suspicion in democracies, is at risk of disappearing through its own simultaneous expansion and diffraction, destabilising the core actors. Doing nothing will generate internal populist revolts against the "elites" and the "deep state", when all the actors are tainted by illegitimacy and covered only by a ritual of secrecy. Moreover, in the context of the war in Ukraine and the behaviour of the Russian secret services, all the actors of the democracies have to prove that they are different and have not abused their prerogatives in the struggle. They must accept that their leaders and secret services will in future be seriously controlled by the supervisory and judicial authorities. This is in their own interest. This is also the way monitoring democracies, multiplying counter powers and avoiding the tyranny of the majority, may survive and reinvent themselves through a transnational Montesquieu logic, despite the attempt of concentration of power at the world scale.

Notes

1 This chapter resumes the first part of the French Guardint final report. Due to the limited amount of space in the book, the chapter highlights only the main hypothesis and arguments developed in the report, without detailing the different examples coming from the situations of US, EU, UK, France and Germany. Other chapters in this book enter into more details and specific examples. The final report is available on demands at TOCES@proton.me.
2 See the chapter of Félix Treguer in this book.
3 The 5 eyes network and the third-party tule are presented on p78 of this chapter, see also the chapters of Arnaud Kurze, and Ronja Kniep in this book.
4 The journal Cultures & Conflits has published different issues on the topic- See Emmanuel-Pierre Guittet et al., 'Cultures & conflits, N 58, Eté 2005: Suspicion et exception' (Editions L'Harmattan, 2005).Laurent Bonelli, Hervé Rayner, and Bernard Voutat, 'Contestations et (re)légitimations du renseignement en démocratie:

Introduction', *Cultures & conflits*, no. 114–115 (20 December 2019): 7–28. See also in English Anastassia Tsoukala Didier Bigo, *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes After 9/11*, 1st ed. (Routledge, 2008).

5 We have benefited for this research of specific access allowing to have interviews with members of the different services and supervisory authorities. ANR UTIC 2015-2018- ORA- GUARDINT 2018-2023. References in the acknowledgement pages. From previous research contracts we had also many contacts beginning in the 1990s, sometimes retired and who have also accepted to discuss with us. This longitudinal approach of almost 20 years changes the relations with the interviewees that we met every year or two years. We do not here quote the persons or give evidence of their functions. They have asked for strict confidentiality.

6 Hager Ben Jaffel and Sebastian Larsson, 'Conclusion: Towards New Intelligence Studies', in *Problematising Intelligence Studies* (Routledge, 2022), 243–53.

7 See the chapter of Claudia Aradau and Emma Mc Cluskey in this book.

8 Claudia Aradau, 'Assembling (Non)Knowledge: Security, Law, and Surveillance in a Digital World', *International Political Sociology* 11, no. 4 (1 December 2017): 327–42, https://doi.org/10.1093/ips/olx019

9 Bigo, Didier. 'International Political Sociology: Rethinking the International through Field(s) of Power.' In *Transversal Lines*, edited by Basaran Tugba, Didier Bigo, Emmanuel-Pierre Guittet, and R. B. J. Walker. Routledge, 2016. Bigo, Didier, 'Sociology of Transnational Guilds', *International Political Sociology* 10, no. 4 (2016): 398–416.

10 See Walker, Rob BJ. *After the Globe, before the World*. Routledge, 2010. For a more applied approach see Bigo, Didier, 'Shared Secrecy in a Digital Age and a Transnational World', *Intelligence and National Security* 34, no. 3 (16 April 2019): 379–94, https://doi.org/10.1080/02684527.2019.1553703.

11 Richard Aldrich has been a pioneer inside intelligence studies to introduce alternatives from classical realism and behaviouralism. He has introduced transnationalism and used the approach of transgovernmentalism, but he has firmly defended the idea of necessity of violence. His work has inspired a large number of authors. Richard J. Aldrich, 'Beyond the Vigilant State: Globalisation and Intelligence', *Review of International Studies* 35, no. 4 (2009): 889–902. Richard J. Aldrich, 'Transatlantic Intelligence and Security Cooperation', *International Affairs* 80, no. 4 (1 July 2004): 731–53, https://doi.org/10.1111/j.1468-2346.2004.00413.x. Richard J. Aldrich, 'Global Intelligence Co-Operation versus Accountability: New Facets to an Old Problem', *Intelligence and National Security* 24, no. 1 (2009): 26–56.Sophia Hoffmann, 'Circulation, Not Cooperation: Towards a New Understanding of Intelligence Agencies as Transnationally Constituted Knowledge Providers', *Intelligence and National Security* 36, no. 6 (2021): 807–26.

12 Ben Jaffel, Hager; Larsson, Sebastian (ed) Hager Ben Jaffel and Sebastian Larsson, 'Conclusion: Towards New Intelligence Studies', in *Problematising Intelligence Studies* (Routledge, 2022) op.cit.

13 Norbert Elias, Michael Schröter, and E. F. N. Jephcott, *The Society of Individuals* (New York, New York: Continuum, 1991), https://ebookcentral.proquest.com/lib/kcl/detail.action?docID=5309872. For a use of a relational and processual sociological approach inspired by Norbert Elias, on the study of intelligence Hager Ben Jaffel et al., 'Collective Discussion: Toward Critical Approaches to Intelligence as a Social Phenomenon', *International Political Sociology* 14, no. 3 (2020): 323–44.

14 John C Yoo, became known for his legal opinions in the early 2000s concerning executive power, warrantless wiretapping, and the Geneva Conventions while serving in the Office of Legal Counsel (OLC) of the Department of Justice during the George W. Bush administration. Yoo was the author of the controversial

"Torture Memos". He is today Emanuel S. Heller Professor of Law at the University of California, Berkeley.

15 Alan M. Dershowitz, *Preemption: A Knife that Cuts Both Ways*, Reprint (WW Norton & Co, 2007). Michael Ignatieff, *The Lesser Evil: Political Ethics in an Age of Terror* (Princeton University Press, 2013).

16 Margaret Satthewwaite, 'Extraordinary Rendition on Disappearances in the War on Terror', *Gonz. J. Int'l L.* 10 (2006): 70, Elspeth Guild, Didier Bigo, and Mark Gibney, eds., *Extraordinary Rendition: Addressing the Challenges of Accountability*, 1 edition (New York: Routledge, 2018) Malika Danoy, 'Des Etats-Unis à La Corne d'Afrique. Le" Programme de Restitutions Extraordinaires": L'extension Du Pouvoir Chasseur Dans La Lutte Antiterroriste.', 2021. PhD (forthcoming book).

17 See the chapter of Bernardino de las Reyes in this book. Sea also Laura Poitras and Glenn Greenwald, 'NSA Whistleblower Edward Snowden: "I Don't Want to Live in a Society That Does These Sort of Things" – Video', *The Guardian*, 9 June 2013, sec. US news, Zyngmunt. Bauman, Didier Bigo et als, 'After Snowden: Rethinking the Impact of Surveillance', *International Political Sociology* 8, no. 2 (2014): 121–44; Michael Kowalski, 'Oversight in the Era of "Snowden" and Big Data: Challenges and Opportunities', *Security and Human Rights* 24, no. 3–4 (2014): 225–26, 4; David Lyon, *Surveillance after Snowden* (Cambridge; Malden, MA: Polity Press, 2015); Patrick F. Walsh and Seumas Miller, 'Rethinking "Five Eyes" Security Intelligence Collection Policies and Practice Post Snowden', *Intelligence and National Security* 31, no. 3 (15 April 2016): 345–68, Didier Bigo 'The Paradox at the Heart of the Snowden Revelations', Open Democracy, 10 February 2016,. Treguer, felix, 'L'utopie Déchue Une Contre-Histoire d'Internet (XVème-XXIème Siècle) 2019,

18 Kaster, Sean D., and Prescott C. Ensign. "Privatized espionage: NSO Group Technologies and its Pegasus spyware." *Thunderbird International Business Review* (2022). Korzak, Elaine. "Export controls: The Wassenaar experience and its lessons for international regulation of cyber tools." In *Routledge Handbook of International Cybersecurity*, pp. 297–311. Routledge, 2020.

19 *Amesys: Egyptian trials and tribulations of a French digital arms dealer*, accessed 30 March 2018, '"Projet Pegasus": Abdellatif Hammouchi, homme le mieux informé du Maroc et grand ami de la France', *Le Monde.fr*, 30 July 2021, Stephanie Kirchgaessner and Sam Jones, 'Phone of Top Catalan Politician "Targeted by Government-Grade Spyware"', *The Guardian*, 13 July 2020, sec.

20 Duncan Campbell, 'Inside Echelon: The History, Structure, and Function of the Global Surveillance System Known as Echelon', *Telepolis*, 2000; David Murakami Wood et al., 'A Report on the Surveillance Society', *Surveillance Studies Network, UK*, 2006, 1–98.

21 Walsh, Patrick F., and Seumas Miller. "Rethinking 'Five Eyes' security intelligence collection policies and practice post Snowden." *Intelligence and National Security* 31, no. 3 (2016): 345-368. Didier Bigo, Laurent Bonelli. 2019. "Digital data and the transnational intelligence space". In *Data politics op.cit.* in particular see the multi-correspondence analysis of the different personnel, budget, type of missions … of the different agencies of the five eyes plus. Didier Bigo, 'Adjusting a Bourdieusian Approach to the Study of Transnational Fields: Transversal Practices and Today State (Trans)Formations Related to Intelligence and Surveillance', in Christian Schmidt-Wellenburg and Stefan Bernhard, *Charting Transnational Fields* (Taylor & Francis Group, 2020).

22 Rogers, Damien. "Transversal Practices of Everyday Intelligence Work in New Zealand: Transnationalism, Commercialism, Diplomacy". In *Problematising Intelligence Studies*, 132–55. Routledge, 2022. See also the chapter of Damien Rogers in this book.

23 For a critique of this post 9/11 attitude see Jones, Calvert. "Intelligence reform: The logic of information sharing". *Intelligence and National Security* 22, no. 3 (1 June 2007): 384–401.
24 Didier Bigo, 'Sécurité Maximale et Prévention? La Matrice Du Futur Antérieur et Ses Grilles', in *Derrière Les Grilles: Sortir Du Tout Évaluation*, ed. Barbara Cassin (Fayard: Mille et une nuits, 2013). Daniel Solove The predictive society Available at SSRN 2023.
25 See the interview with François Thuillier on this book
26 Evelyn Ruppert, Engin Isin, and Didier Bigo, 'Data Politics', *Big Data & Society* 4, no. 2 (1 December 2017), Didier Bigo, Engin F Isin, and Evelyn Ruppert, *Data Politics: Worlds, Subjects, Rights*, 2019.Routledge-open access; Davide Beraldo and Stefania Milan, 'From Data Politics to the Contentious Politics of Data', *Big Data & Society* 6, no. 2 (1 July 2019).
27 Beyond the case of Pegasus as such, see the analysis of the marketisation and de-oligopolization of state power by spyware. Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. Hide and seek: Tracking NSO group's Pegasus spyware to operations in 45 countries. 2018 Ronald J. Deibert, 'The Autocrat in Your IPhone: How Mercenary Spyware Threatens Democracy', *Foreign Aff.* 102 (2023): 72. Surowiec-Capell, Paweł, and Philip Long. 'hybridity, soft power, and statecraft'. *The Routledge Handbook of Soft Power*, 2023.Olivier Tesquet, *Etat d'urgence Technologique* (Premier Parallèle, 2021).
28 See the interview with Thorsten Wetzling in this book.
29 Susan Strange, 'States, Firms and Diplomacy', *International Affairs* 68, no. 1 (1 January 1992): 1–15; James Der Derian, 'Anti-diplomacy, Intelligence Theory and Surveillance Practice', *Intelligence and National Security* 8, no. 3 (1993): 29–51; James Der Derian, *Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network* (Diane Pub Co, 2001).
30 Philip K. Dick, 'Minority Report (New York', *Pantheon*, 1956.'Is Predictive Policing Making Minority Report a Reality?', n.d., 3; Meredith Broussard, *Artificial Unintelligence: How Computers Misunderstand the World*, n.d.,; European Union Agency for Fundamental Rights., *Getting the Future Right: Artificial Intelligence and Fundamental Rights. Annex I, Research Methodology.* (LU: Publications Office, 2020); N. Elkin-Koren, 'Contesting Algorithms: Restoring the Public Interest in Content Filtering by Artificial Intelligence', *Big Data and Society* 7, no. 2 (2020), https://doi.org/10.1177/2053951720932296. Didier Bigo, 'Sécurité maximale et prévention? La matrice du futur antérieur et ses grilles', n.d., 16.in Barbara Cassin « Derrière les grilles: sortons du tout évaluation. Paris. Mille et une nuit (2015).
31 See the key book of Huysmans, Jef. Security Unbound: Enacting Democratic Limits. Routledge, 2014.
32 Jaffel, Hager Ben, et Sebastian Larsson. « Conclusion: Towards New Intelligence Studies ». In *Problematising Intelligence Studies*, 243–53. Routledge, 2022
33 Bigo, D: sociology of transnational guilds op.cit. The notion of interstitial spaces means that when previous autonomous fields are intertwined and that each field is affected by the rules of the games of the other, it is not a colonisation of one field by the other one but an entanglement destabilising the authorities on both fields and generating for the multi-positioned actors of both peripheries a chance to access from this place to important forms of symbolic power.
34 Paul Taylor, 'Beyond False Positives: A Typology of Police Shooting Errors', *Criminology & Public Policy* 18 (24 October 2019).
35 James Ball, 'NSA's Prism Surveillance Program: How It Works and What It Can Do', the Guardian, 8 June 2013, Try also the website of the guardian https://www.theguardian.com/world/interactive/2013/oct/28/nsa-files-decoded-

hops. President Obama asked the NSA to get back to a lesser ratio, preferably 2, which means already 18,000 people.

36 For recent developments on the entanglements of preventive predictive logics and criminal justice see Mitsilegas, V., Bergström, M., (eds.) *EU Law in the Digital Age*, Hart Publishing Ltd,(2023)

37 Tobias M. Scholz, *Big Data in Organizations and the Role of Human Resource Management* (Peter Lang D, 2017), 7.Claudia Aradau and Tobias Blanke, *Algorithmic Reason: The New Government of Self and Other* (Oxford University Press, 2022).

38 Elspeth Guild, Monitoring Border Violence in the EU: Frontex in Focus, Routledge, 2023

39 Valsamis Mitsilegas et al., 'Data Retention and the Future of Large-scale Surveillance: The Evolution and Contestation of Judicial Benchmarks', *European Law Journal*, 2022; Niovi Vavoula, 'Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?', *European Public Law* 26, no. 1 (1 March 2020): 131–56; Didier Bigo, 'Interoperability: A Political Technology for the Datafication of the Field of EU Internal Security?', in *The Routledge Handbook of Critical European Studies* (Routledge, 2020), 400–417; Anastassia Tsoukala, 'Legitimizing the Shrinking of Democratic Space in Western Liberal Democracies', *Political Anthropological Research on International Social Sciences (PARISS)* 2, no. 2 (1 December 2021): 185–204.

40 Anthony Amicelle, 'Right of Entry: The Struggle over Recognition in the World of Intelligence', *Political Anthropological Research on International Social Sciences (PARISS)* 1, no. 2 (18 December 2020): 243–72; Anthony Amicelle, 'Naissance d'une agence de renseignement: droits d'entrée dans les univers de la finance et de la sécurité', *Cultures & Conflits*, no. 114–115 (20 December 2019): 171–97.

41 Eric Van Rythoven, 'A Feeling of Unease: Distance, Emotion, and Securitizing Indigenous Protest in Canada', *International Political Sociology* 15, no. 2 (1 June 2021): 251–71; Didier Bigo, *Global (in)Security: The Field of the Professionals of Unease Management and the Ban-Opticon*, vol. 4, Traces: A Multilingual Series of Cultural Theory: Translation, Philosophy and Colonial Difference (University of Hong Kong Press, 2006); Jef Huysmans and Alessandra Buonfino, 'Politics of Exception and Unease: Immigration, Asylum and Terrorism in Parliamentary Debates in the UK', *Political Studies* 56, no. 4 (2008): 766–88, Didier Bigo, 'Security and Immigration: Toward a Critique of the Governmentality of Unease', *Alternatives: Global, Local, Political* 27, no. 1_suppl (February 2002): 63–92.

42 See the chapters of Arnaud Kurze, and Elspeth Guild and Sophia Soares in this book.

43 For a more detailed analysis consult the final French report of GUARDINT. See acknowledgement.

44 See Emma Mc Cluskey on the strat-com policy of GCHQ- forthcoming. Michelsen, Nicholas, and Thomas Colley. 'The Field of Strategic Communications Professionals: A New Research Agenda for International Security'. *European Journal of International Security* 4, no. 1 (2019): 61–78. See also Stan A. Taylor, 'Introduction: Spying in Film and Fiction', *Intelligence and National Security* 23, no. 1 (1 February 2008): 1–4,

45 James C. Scott, *Domination and the Arts of Resistance: Hidden Transcripts* (Yale University Press, 1990).

References

Aldrich, Richard J. "Beyond the Vigilant State: Globalisation and Intelligence." *Review of International Studies* 35, no. 4 (2009): 889–902

Aldrich, Richard J. "Global Intelligence Co-Operation versus Accountability: New Facets to an Old Problem." *Intelligence and National Security* 24, no. 1 (2009): 26–56

Aldrich, Richard J. "Transatlantic Intelligence and Security Cooperation." *International Affairs* 80, no. 4 (July 1, 2004): 731–753.

Amesys: Egyptian trials and tribulations of a French digital arms dealer, accessed 30 March 2018, "'Projet Pegasus': Abdellatif Hammouchi, homme le mieux informé du Maroc et grand ami de la France." *Le Monde.fr* (July 30, 2021).

Amicelle, Anthony. "Naissance d'une agence de renseignement: droits d'entrée dans les univers de la finance et de la sécurité." *Cultures & Conflits* no. 114–115 (December 20, 2019): 171–197.

Amicelle, Anthony. "Right of Entry: The Struggle over Recognition in the World of Intelligence." *Political Anthropological Research on International Social Sciences (PARISS)* 1, no. 2 (December 18, 2020): 243–272,

Aradau, Claudia, and Tobias Blanke. *Algorithmic Reason: The New Government of Self and Other*. Oxford University Press, 2022.

Aradau, Claudia. "Assembling (Non)Knowledge: Security, Law, and Surveillance in a Digital World." *International Political Sociology* 11, no. 4 (December 1, 2017): 327–342,

Ball, James. "NSA's Prism Surveillance Program: How It Works and What It Can Do." The Guardian, June 8, 2013.

Bauman, Zyngmunt, Didier Bigo et al. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8, no. 2 (2014): 121–144,

Ben Jaffel, Hager, and Sebastian Larsson. "Conclusion: Towards New Intelligence Studies." In *Problematising Intelligence Studies*, 243–253. Routledge, 2022.

Ben Jaffel, Hager et al. "Collective Discussion: Toward Critical Approaches to Intelligence as a Social Phenomenon." *International Political Sociology* 14, no. 3 (2020): 323–344.

Ben Jaffel, Hager, and Sebastian Larsson. "Conclusion: Towards New Intelligence Studies." In *Problematising Intelligence Studies*, edited by Hager Ben Jaffel and Sebastian Larsson. Routledge, 2022.

Bigo, Didier. "Sécurité maximale et prévention? La matrice du futur antérieur et ses grilles." n.d., 16.in Barbara Cassin "Derrière les grilles: sortons du tout évaluation". Paris: Mille et une nuit, 2015.

Bigo, Didier. "The Paradox at the Heart of the Snowden Revelations." Open Democracy, February 10, 2016.

Bigo, Didier. "Adjusting a Bourdieusian Approach to the Study of Transnational Fields: Transversal Practices and Today State (Trans)Formations Related to Intelligence and Surveillance." In *Charting Transnational Fields*, Christian Schmidt-Wellenburg and Stefan Bernhard. Taylor & Francis Group, 2020.

Bigo, Didier. "Interoperability: A Political Technology for the Datafication of the Field of EU Internal Security?" In *The Routledge Handbook of Critical European Studies*, 400–417. Routledge, 2020.

Bigo, Didier. "Sécurité Maximale et Prévention? La Matrice Du Futur Antérieur et Ses Grilles." In *Derrière Les Grilles: Sortir Du Tout Évaluation*, edited by Barbara Cassin Fayard. Mille et une nuits, 2013.

Bigo, Didier. "Security and Immigration: Toward a Critique of the Governmentality of Unease." *Alternatives: Global, Local, Political* 27, no. 1_suppl (February 2002): 63–92.

Bigo, Didier, Engin F Isin, and Evelyn Ruppert. *Data Politics: Worlds, Subjects, Rights*. Routledge-open access, 2019.

Bigo, Didier. *Global (in)Security: The Field of the Professionals of Unease Management and the Ban-Opticon*, vol. 4. Traces: A Multilingual Series of Cultural Theory: Translation, Philosophy and Colonial Difference. University of Hong Kong Press, 2006.

Bigo, Didier, and Laurent Bonelli. "Digital data and the transnational intelligence space." In *Data politics op.cit.* (2019).

Bigo, Didier. "Shared Secrecy in a Digital Age and a Transnational World." *Intelligence and National Security* 34, no. 3 (April 16, 2019): 379–394.

Bigo, Didier. "Sociology of Transnational Guilds." *International Political Sociology* 10, no. 4 (2016): 398–416.

Bigo, Didier. "International Political Sociology: Rethinking the International through Field(s) of Power." In *Transversal Lines*, edited by Basaran Tugba, Didier Bigo, Emmanuel-Pierre Guittet, and R. B. J. Walker. Routledge, 2016.

Bonelli, Laurent, Hervé Rayner, and Bernard Voutat. "Contestations et (re) légitimations du renseignement en démocratie: Introduction." *Cultures & conflits* no. 114–115 (December 20, 2019): 7–28.

Broussard, Meredith. *Artificial Unintelligence: How Computers Misunderstand the World*, n.d.; European Union Agency for Fundamental Rights., *Getting the Future Right: Artificial Intelligence and Fundamental Rights. Annex I, Research Methodology*. LU: Publications Office, 2020.

Campbell, Duncan. "Inside Echelon: The History, Structure, and Function of the Global Surveillance System Known as Echelon." *Telepolis* (2000).

Danoy, Malika. "Des Etats-Unis à La Corne d'Afrique. Le" Programme de Restitutions Extraordinaires": L'extension Du Pouvoir Chasseur Dans La Lutte Antiterroriste." 2021.PHD (forthcoming book).

Deibert, Ronald J. "The Autocrat in Your IPhone: How Mercenary Spyware Threatens Democracy." *Foreign Aff.* 102 (2023): 72.

Der Derian, James. "Anti-diplomacy, Intelligence Theory and Surveillance Practice." *Intelligence and National Security* 8, no. 3 (1993): 29–51.

Der Derian, James. *Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network*. Diane Pub Co, 2001.

Dershowitz, Alan M. *Preemption: A Knife that Cuts Both Ways*. Reprint WW Norton & Co, 2007.

Dick, Philip K. "Minority Report New York." *Pantheon* (1956).

Elias, Norbert, Michael Schröter, and E. F. N. Jephcott. *The Society of Individuals*. New York, NY: Continuum, 1991.

Elkin-Koren, N. "Contesting Algorithms: Restoring the Public Interest in Content Filtering by Artificial Intelligence." *Big Data and Society* 7, no. 2 (2020).

Guild, Elspeth, Didier Bigo, and Mark Gibney, eds. *Extraordinary Rendition: Addressing the Challenges of Accountability*, 1 edition. New York: Routledge, 2018.

Guild, Elspeth. *Monitoring Border Violence in the EU: Frontex in Focus*. Routledge, 2023.

Guittet, Emmanuel-Pierre et al. "Cultures & conflits, N 58, Eté 2005: Suspicion et exception." Editions L'Harmattan, 2005.

Hoffmann, Sophia. "Circulation, Not Cooperation: Towards a New Understanding of Intelligence Agencies as Transnationally Constituted Knowledge Providers." *Intelligence and National Security* 36, no. 6 (2021): 807–826.

Huysmans, Jef, and Alessandra Buonfino. "Politics of Exception and Unease: Immigration, Asylum and Terrorism in Parliamentary Debates in the UK." *Political Studies* 56, no. 4 (2008): 766–788.

Huysmans, Jef. *Security Unbound: Enacting Democratic Limits*. Routledge, 2014.

Ignatieff, Michael. *The Lesser Evil: Political Ethics in an Age of Terror*. Princeton University Press, 2013.

Jones, Calvert. "Intelligence reform: The logic of information sharing." *Intelligence and National Security* 22, no 3 (June 1, 2007): 384–401

Kaster, Sean D., and Prescott C. Ensign. "Privatized espionage: NSO Group Technologies and its Pegasus spyware." *Thunderbird International Business Review* (2022).

Kirchgaessner, Stephanie, and Sam Jones. "Phone of Top Catalan Politician "Targeted by Government-Grade Spyware"." *The Guardian* (July 13, 2020).

Korzak, Elaine. "Export controls: The Wassenaar experience and its lessons for international regulation of cyber tools." In *Routledge Handbook of International Cybersecurity*, pp. 297–311. Routledge, 2020.

Kowalski, Michael. "Oversight in the Era of "Snowden" and Big Data: Challenges and Opportunities." *Security and Human Rights* 24, no. 3–4 (2014): 225–226. 4.

Lyon, David. *Surveillance after Snowden*. Cambridge; Malden, MA: Polity Press, 2015.

Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. "Hide and seek: Tracking NSO group's Pegasus spyware to operations in 45 countries." (2018).

Michelsen, Nicholas, and Thomas Colley. "The Field of Strategic Communications Professionals: A New Research Agenda for International Security." *European Journal of International Security* 4, no. 1 (2019): 61–78.

Mitsilegas, Valsamis et al. "Data Retention and the Future of Large-scale Surveillance: The Evolution and Contestation of Judicial Benchmarks." *European Law Journal* (2022). https://doi.org/10.1111/eulj.12417

Mitsilegas, V., and M. Bergström (eds.). *EU Law in the Digital Age*. Hart Publishing Ltd, 2023.

Murakami Wood, David et al. "A Report on the Surveillance Society." *Surveillance Studies Network, UK* (2006): 1–98.

Poitras, Laura, and Glenn Greenwald. "NSA Whistleblower Edward Snowden: "I Don't Want to Live in a Society That Does These Sort of Things" – Video." *The Guardian* (June 9, 2013): sec. US news.

Rogers, Damien. "Transversal Practices of Everyday Intelligence Work in New Zealand: Transnationalism, Commercialism, Diplomacy." In *Problematising Intelligence Studies*, 132–155. Routledge, 2022.

Ruppert, Evelyn, Engin Isin, and Didier Bigo. "Data Politics." *Big Data & Society* 4, no. 2 (December 1, 2017).

Satthewwaite, Margaret. "Extraordinary Rendition on Disappearances in the War on Terror." *Gonz. J. Int'l L.* 10 (2006): 70.

Scholz, Tobias M. *Big Data in Organizations and the Role of Human Resource Management*, 7. Peter Lang D, 2017.

Scott, James C. *Domination and the Arts of Resistance: Hidden Transcripts*. Yale University Press, 1990.

Solove, Daniel. *The predictive society*. Available at SSRN, 2023.

Strange, Susan. "States, Firms and Diplomacy." *International Affairs* 68, no. 1 (January 1, 1992): 1–15.

Surowiec-Capell, Paweł, and Philip Long. "Hybridity, soft power, and statecraft." *The Routledge Handbook of Soft Power* (2023).

Taylor, Paul. "Beyond False Positives: A Typology of Police Shooting Errors." *Criminology & Public Policy* 18 (October 24, 2019).

Taylor, Stan A. "Introduction: Spying in Film and Fiction." *Intelligence and National Security* 23, no. 1 (February 1, 2008): 1–4.

Tesquet, Olivier. *Etat d'urgence Technologique*. Premier Parallèle, 2021.

Treguer, Félix. "L'utopie Déchue Une Contre-Histoire d'Internet XVème-XXIème Siècle." (2019).

Tsoukala, Anastassia, and Didier Bigo. *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes After 9/11*, 1st ed. Routledge, 2008.

Tsoukala, Anastassia. "Legitimizing the Shrinking of Democratic Space in Western Liberal Democracies." *Political Anthropological Research on International Social Sciences (PARISS)* 2, no. 2 (December 1, 2021): 185–204.

Van Rythoven, Eric. "A Feeling of Unease: Distance, Emotion, and Securitizing Indigenous Protest in Canada." *International Political Sociology* 15, no. 2 (June 1, 2021): 251–271.

Vavoula, Niovi. "Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?" *European Public Law* 26, no. 1 (March 1, 2020): 131–156.

Walker, Rob BJ. *After the Globe, before the World*. Routledge, 2010.

Walsh, Patrick F., and Seumas Miller. "Rethinking "Five Eyes" Security Intelligence Collection Policies and Practice Post Snowden." *Intelligence and National Security* 31, no. 3 (April 15, 2016): 345–368.

Walsh, Patrick F., and Seumas Miller. "Rethinking 'Five Eyes' security intelligence collection policies and practice post Snowden." *Intelligence and National Security* 31, no. 3 (2016): 345–368.

3 The code of silence

Transnational autonomy and oversight of signals intelligence[1]

Ronja Kniep

Introduction

Rarely have German intelligence agencies addressed the public as offensively as they did at the beginning of 2020. The Constitutional Court was hearing a case on the legality of surveillance conducted by the Bundesnachrichtendienst (BND), Germany's foreign intelligence agency. In the media, intelligence officers discredited the claimants – a group of NGOs and journalists – as "litigation fools"[2] ("Prozesshansel"; my translation) and feared the trial had become a "mockery of fellow agents"[3] in other countries. They framed the lawsuit as absurd, a security risk, and a possible threat to the lives of soldiers.[4] The public warning of a former head of intelligence to the Constitutional Court was also novel.[5] From the perspective of intelligence officers, their ability to work was at stake if, in accordance with the complaint, the communication of foreigners abroad was also to be protected by the German constitution.

These harsh words should be read as an attempt to defend the transnational autonomy of digital surveillance by intelligence agencies. The lawsuit challenged an established principle of division and domination of the field, which is based on the distinction between domestic and foreign communications and is constitutive of established forms of mass data collection and sharing by intelligence agencies. Eventually, the ruling of the court tackled another rule of the transnational intelligence game: the *Third Party Rule*, according to which data can be shared with a third party only under the caveat of the originator. This article outlines how the practices of the *Third Party Rule* and the *domestic–foreign–distinction* work through and produce different forms of silence that were partly and temporarily broken by the negotiations: silence created by *doxic*, unquestioned forms of symbolic power, and silence as a social code among the players of a field that internally binds its members and secures their power from external interference. Thus, in addition to secrecy – what should not be spoken about – the notion of silence draws attention to the spaces of power that are based on habitualised practices that need not or cannot be spoken about.

The negotiations of the rules of digital surveillance in Berlin and Karlsruhe cannot be understood as a purely national reform process. It was intertwined

DOI: 10.4324/9781003354130-4

with the transnational forms of symbolic power in the field of signals intelligence (SIGINT) and its oversight. The advantages of a Bourdieusian approach to studying phenomena that transcend the nation state have been described in detail and applied to research by several scholars in sociology, IR, and beyond.[6] For a better understanding of intelligence and its oversight, field analysis provides a useful tool for avoiding the naturalistic and functionalist view of intelligence and the state that has been particularly dominant in intelligence studies.[7] Similarly, the field approach allows for an analysis of intelligence oversight that focuses on the struggles and practices involved, breaking with the prominent yet incomplete understanding of oversight as a venue for compromise and balance.[8]

Along three elements of field analysis – genesis, autonomy, and heteronomy – this article examines the extent to which the structural conditions, practices, and power relations of SIGINT have destabilised or circumvented democratic oversight and democratic self-determination, using the cooperation of the German BND with the US National Security Agency (NSA) and its oversight as an example. What we can observe in this concrete cooperation and the corresponding oversight practices is partly an effect of the genesis of a transnational SIGINT field. Examining the power dynamics of this field and its interplay with established oversight structures, including the production of orthodoxy by courts, explains why digital surveillance of transnationally operating intelligence agencies continues to work so well despite (and partly due) to its contestation post-Snowden. The aforementioned negotiations in Germany and the subsequent legal and oversight reforms represent not only a challenge to the symbolic power of intelligence, but also a new form of its legalisation, normalisation, and legitimation.

Genesis: The transnational field of Signals Intelligence

Fields – such as academia, journalism, or art – are distinct social spaces of society that are characterised by four main features: asymmetric power relations structured by unequally distributed capital, common objects of struggle, largely internalised rules, and relative autonomy from other fields.[9] These social spaces or "social games"[10] can be more or less confined to national borders, or distinctly extend transnationally. However, one of the most important features of field analysis is that it breaks with such repeatedly replicated divisions as *state* vs. *international* or *individual* vs. *society* and provides analytical access to the interstices that *transnationally* or *transversally* emerge between and across them.[11] Additionally, in order to avoid thinking "the state with a state thought",[12] it is necessary to disengage from the fiction of the state as an acting agent or central power entity. In fact, it is composed of a multiplicity of actors of different fields and sub-fields that confront each other in complex, hierarchical relations in a web of interdependence of the powerful.[13]

Following this perspective, instead of conceiving intelligence agencies as neutral collectors of information working as the "right hand of the state",

intelligence can be considered a subfield of the bureaucratic field in which actors compete for interpretive and informational sovereignty over security threats. SIGINT, in turn, is a distinct cosmos within the intelligence world that has emerged in distinction to the military and other disciplines such as human intelligence (HUMINT). The shifting and shared images of the enemy among the agencies have contributed to the collective *illusio* – "the idea that the game is worth the candle, that it is worth playing".[14] This illusio has been reinforced by the cooperative adoption of surveillance practices in view of new communication technologies, ranging from the surveillance of wireless telegraphy in World War I and World War II, to satellite surveillance during the Cold War and Internet surveillance in the context of terrorist threats.

Capital and symbolic power

As a practice, SIGINT can be described as the secretive production of "exclusive information" through the mathematical and technical analysis of any traces ("data") left by human actors or machines in the electromagnetic spectrum or digital networks. As the practice of SIGINT became increasingly systematic during World War II, another type of producing "informational capital"[15] was introduced into intelligence which re-shaped existing power relations. At least by the 1950s and 1960s, SIGINT had come to be regarded as a separate entity in the military field and an elite in intelligence, a phenomenon that has been described as "SIGINT snobbery" or "alienation" from the military on the ground.[16] While reports from HUMINT or other sources were often labelled as "unconfirmed information",[17] SIGINT seemed to promise its customers the technical, quasi-magical extraction of truth from seemingly "raw data"[18] at a distance. SIGINT gained symbolic power – "a power of constituting the given (…) that can be exercised only if it is *recognized*, that is, misrecognized as arbitrary"[19] – vis-à-vis other forms and actors of intelligence.

Power relations arise within the SIGINT field from technical and legal competencies for data access and analysis. These are also mediated by economic and social capital – budget and access to transnational SIGINT networks – which constitute the informational capital that can be effective as symbolic power inside and outside the field. There are two features of the symbolic power of SIGINT. First, the interpretations and meanings coproduced and enforced in the field, such as enemy images or the classification of risk and non-risk, are commonly difficult to contest due to their secret and technically complex conditions of production; these may increase their symbolic power. Second, in addition to the exercise of "symbolic violence"[20] via these interpretations, informational power can certainly be linked to the exercise of physical violence. The infamous quote of former NSA chief Michael Hayden – "We kill people based on meta-data"[21] – does not point to a new type of practice but describes the contemporary form of the "marriage between SIGINT information and operational procedures to effect a kill"[22] that had already emerged in World War II.

Centralisation of power through transnational dynamics

The emergence of SIGINT was accompanied by a process of autonomisation and centralisation of informational and symbolic power. The centralised SIGINT agencies or departments found in many countries today are the product of struggles involving both agencies on a national level (such as the army, navy, and domestic and foreign intelligence agencies) and intelligence practitioners of other countries. For instance, the latter promoted certain persons or agencies who were regarded as more akin to their own interests,[23] and eventually, centralisation itself was advocated by foreign partner agencies. Foreign agencies preferred to have "single points of contact", which made secret interaction easier. In the 1950s, GCHQ still found parts of US American SIGINT "to be frustratingly decentralised".[24]

In many cases, transnational dynamics did not follow the formation of national SIGINT entities, but preceded or even helped to bring them about – this is sometimes ignored in functionalist narratives of how intelligence "globalised" as a natural response to global threats. In some countries, transnational exchange of military and intelligence personnel drove the institutionalisation of SIGINT more than deliberate decisions of elected governments, which were informed and convinced after surveillance practices had already been established. This was the case in the founding of the Australian[25] and German[26] SIGINT organisations, decisively driven by the exchange with US-American and (in the case of Australia) British intelligence professionals. In turn, the creation of the NSA itself was influenced by American Siginters' contacts with the British GCHQ, which was a model for the centralisation of SIGINT in the US.[27] Before the NSA was founded in 1957 as the first centralised SIGINT organisation in the US, the UKUSA alliance formed in the 1940s,[28] from which the Five Eyes eventually emerged. Transnational agreements preceded centralisation in the US, as an NSA historian describes:

> Even in such a sensitive area as foreign relationships, each COMINT service demonstrated a predisposition to act completely independently. For example, the Army and Navy persisted in establishing their own technical agreements with their British counterparts, but without coordination or dialogue with the other U.S. service. These agreements frequently conflicted, usually with respect to the amount and kinds of intelligence information to be exchanged. Because of these diverse agreements, a potential for serious damage to American intelligence interests always existed.[29]

SIGINT was thus never confined to the national bureaucratic field, constituting itself as a transnational field as early as the first half of the 20th century. SIGINT provides an example of how entangled national and transnational fields are despite their relative autonomy, and how they

encompass forms of state and non-state power that may counteract, stabilise, or exponentiate each other.

Actors and modes of cooperation

While having always been "transnational", the development of the SIGINT field since the end of World War II confirms the observation of an increase and deepening of transnational order formation in the security field.[30] This is evidenced by the growth in importance of multilateral modes of cooperation through the expansion of existing networks, the formation of new multilateral SIGINT networks, and the deepening of common practices within these networks. The UKUSA agreement, formalised in 1946, became the Five Eyes (1948). The SIGINT Seniors Europe (SSEUR, 1982) were formalised during the Cold War and the European Maximator network (1976) was formed in parallel, and later the SIGINT Seniors Pacific (SSPAC, 2005) came into being, structurally mimicking the SSEUR for the Asian pacific region (Table 3.1). The expansion of such formalised, multilateral forms of cooperation is noteworthy because informal bilateralism is often considered the preferred mode of cooperation in the field.

The Five Eyes form the NSA's closest circle as so-called Second Party Partners, which include the SIGINT organisations of the United Kingdom (Government Communications Headquarters, GCHQ), Canada (CSE, The Communications Security Establishment), Australia (Defence Signals Directorate, DSD) and New Zealand (The Government Communications Security Bureau, GCSB). Over the years, other domestic and HUMINT-focused agencies have also gathered under the Five Eyes and cooperation has also encompassed covert actions and assassinations.[31] However, even within the larger Five Eyes network, the SIGINT group remains a distinct entity with a particularly tightly knit mode of cooperation. This consists of jointly operated interception stations, a division of labour with regard to the surveillance of different geographic regions of the world, and a largely automated data exchange. In an internal document, the NSA notes that in some cases it is impossible "to tell where one partner's work ends, and another's begins".[32]

Nevertheless, even among the Five Eyes, there is no absolute no-spy agreement[34] and there is always information that is not shared, or not automatically shared. The NSA labels such exclusive material as "NOFORN" (no foreign nationals).[35] Acting together in a field does not mean unanimity. The simultaneity of cooperation and competition – which in the case of intelligence includes mutual spying and deception – is part of the modus operandi of the field. The new awareness of how closely intelligence agencies work together since the Snowden revelations, especially in the case of the Five Eyes, has sometimes led to an overemphasis on unity and alliance – even an alliance constituted by liberal, democratic, or Western values. However, Bourdieu reminds us that players of a field are particularly "united by the struggles that divide them, and even the alliances that may unite them always have something

Table 3.1 NSA's formal SIGINT Relationships (Bilateral and Multilateral)[33]

Five Eyes (1946)	*SSEUR (1982)*	*SSPAC (2005)*	*NATO*	*Bilateral Third Parties*	*Maximator (1976)*
USA (1946)	USA	USA	USA	Algeria	Denmark (1976)
Australia (1956)	Australia	Australia		Austria	France (1985)
Canada (1948)	Canada	Canada	Canada	Belgium	Germany (1976)
NZ (1956)	NZ	NZ		Croatia	Netherlands (1978)
UK (1946)	UK	UK	UK	Czech Rp. (2005)	Sweden (1976)
	Belgium	France	Albania	Denmark	
	Denmark	India (2008)	Belgium	Ethiopia	
	France	Korea (2005)	Bulgaria	Finland	
	Germany	Singapore (2005)	Croatia	France	
	Italy	Thailand (2005)	Czech Republic	Germany (1962)	
	Netherlands		Denmark	Greece	
	Norway		Estonia	Hungary	
	Spain		France	India	
	Sweden		Germany	Israel	
			Greece	Italy	
			Hungary	Japan	
			Iceland	Jordan	
			Italy	Korea	
			Latvia	Macedonia	
			Lithuania	Netherlands	
			Luxembourg	Norway (1954)	
			Montenegro	Pakistan	
			Netherlands	Poland	
			North Macedonia	Romania	
			Norway	Saudi Arabia	
			Poland	Singapore	
			Portugal	Spain	
			Romania	Sweden (1954)	
			Slovakia	Taiwan	
			Slovenia	Thailand	
			Spain	Tunisia	
			Turkey	Turkey	
			ETI	UAE	

to do with the positions they occupy within these struggles".[36] Therefore, to speak of a *field* is to break with the idea of an intelligence *community*.[37]

In addition to "Second Party Partners", the NSA has bi- and multilateral relationships with "Third Party Partners" (Table 3.1). These relationships are also relatively stable but vary in how close collaborations are structured. The closeness of the relationships is not only determined by historical and geo-political factors, but also by infrastructural, geographic constellations and available information capital; SIGINT-specific circumstances. The NSA itself describes Third Parties as providers of "unique accesses, regional analytical expertise" and "foreign language capabilities".[38] For Third Parties, on the other hand, the NSA often provides technologies and is in demand due to its "global reach".[39] Providing surveillance technologies goes hand in hand with developing shared expertise and knowledge transfer, such as in joint training. Relationships with recognised third parties are usually formalised in Memorandum of Agreements (MOAs), in which agencies agree not to spy on each other. The validity of this agreement may be selective, such as for specific joint programmes. But as the NSA writes in an internal presentation, "[we] can, and often do, target the signals of most 3rd party foreign partners".[40]

SIGINT cooperation between the BND and the NSA was formalised in 1962,[41] after the Central Intelligence Agency (CIA) had played a major role in the formation of the German agency.[42] More precisely, the SIGINT relationship was established between the NSA and the SIGINT department BND-TA, which stands for *Technische Aufklärung* (TA). Thus, in Germany, the autonomisation of SIGINT took place within its foreign intelligence agency, the BND. The fact that the SIGINT department has been referred to by BND personnel as having developed a life of its own, as a "a department *sui generis*"[43] that differs from the rest of the agency due to its military and technical mindset, can be regarded as a field effect.

Presumably, there are a number of other SIGINT agreements around the world which add to a transnational space of partly overlapping SIGINT networks. In addition, there are certainly multiple collaborations of SIGINT agencies with domestic and HUMINT agencies and private companies. However, cooperation among SIGINT agencies has a distinguishable quality which becomes visible through exclusive multilateral SIGINT networks or the high level of institutionalisation. The transnational orientation of different intelligence agencies varies[44] and is particularly strong in SIGINT. This is precisely the effect, the force of a field: the attraction of a particular, shared game.

Autonomy: The foreign neverland and the code of silence

The degree of autonomy of a field – the degree to which a field follows its own rules, logics, and practices at the expense of external domination – is a central feature of a field that distinguishes one field from another, varies from field to field, and historically fluctuates. While Vauchez[45] describes

transnational fields as weakly autonomous constellations, the analysis of relative autonomy remains an empirical exercise and is central to understanding the power relations of actors inside and outside of a field. Eventually, the emergence of a relative autonomy is one of the conditions for existence of fields in the first place.

There are a number of concrete criteria for assessing the degree of autonomy of a field.[46] These include the entry conditions and the sanctioning of rule breaking. Generally, intelligence has a relatively high degree of autonomy. Security checks set high barriers to entry to the field, classification schemes prevent exchange with outsiders, and breaking internal secrecy rules is relentlessly sanctioned with exclusion, not only from agencies themselves but also in some cases from taking part in society. This is demonstrated by the way whistle-blowers are treated, even in democracies. Traditionally, particularly high levels of secrecy have been applied in SIGINT. Historians found that the reluctance of SIGINT agencies to share information with national authorities has cost numerous lives.[47] This secrecy is exacerbated when it comes to collaborations with transnational peers that are negotiated and implemented – at least in detail – not between governments but between organisations and individual departments. Joint operations usually take place as carefully shielded *compartmented operations*, as the field language puts it. Beyond these particularly high levels of secrecy, there are two rules in SIGINT that enable and promote the transnational autonomy and ultimately secure the power of actors in the field: the *domestic–foreign distinction* applied to data and the *Third Party Rule*.

The domestic–foreign distinction as a doxa *of mass surveillance*

The exercise of symbolic power and domination does not begin with immediately tangible infringements on individual freedom of choice (as action theory and liberal ideas of freedom suggest) but with the construction of legitimate perceived classifications. In the intelligence field, these include the production of distinctions between security and insecurity, risk and non-risk, or suspicious and unsuspicious behaviour. While these classifications in SIGINT are traditionally produced based on data and algorithmically mediated, they are reconfigured by using new technologies such as machine learning.[48] This is also true for the distinction between domestic and foreign communication.

The domestic–foreign distinction describes the common practice in the SIGINT field that foreign communication, nota bene, has no protection or a significantly lower level of protection from surveillance than communication involving national citizens or persons on national territory. (Para)*doxically*, this is not a distinction that separates the SIGINT agencies of different countries from each other, but a field-relevant division principle that connects the agencies. Large scale and largely uncontrolled foreign data collection is a central currency of the field's transnational surveillance economy. Many of

the closer collaborations are based on the ability to arbitrarily collect and automatically forward foreign data. One of these collaborations was the BND-NSA Operation codenamed *Eikonal*.[49] By the end of the 1990s, the agencies had begun to discuss the new challenge of intercepting Internet cables. In *Eikonal*, ultimately operational from 2004 until 2008, the BND learned from the NSA how to "early on master and surveil mass data from the internet [my translation]"[50] while the BND let the NSA participate in the results. The German agency autonomously and automatically shared intercepted (with few exceptions) foreign data with the NSA based on millions of search terms, i.e. technical identifiers such as emails or IP addresses, called selectors. Even the BND did not have complete knowledge to whom or what the NSA's selectors referred to. It mattered, however, that the selectors do not aim at domestic communication.

It is not a coincidence that it is mostly the foreign rather than the domestic intelligence agencies which have exclusive competencies for mass surveillance. This provides SIGINT agencies with a special position in the national security field. The claim that "we are not monitoring our own citizens" has also served as an argument to establish and legitimise mass surveillance as a practice in democracies. Thus, the domestic–foreign distinction was part of the *doxa* of the field on the basis of which the rationalities and transnational economy of mass surveillance emerged. The *doxa* refers to the unquestioned common sense of a given field; a point of view that, through its naturalisation and silent acceptance, is also an effect of symbolic power and domination.[51]

In practice, the *doxic* foreign–domestic distinction does not mean that SIGINT agencies never put their own citizens under surveillance. In contrast to the surveillance of foreigners, however, these practices are either defined as transgressions that are sanctioned when they become public, or they are subject to stricter authorisation and oversight rules and are internally defined as comparatively unusual business. The BND, for instance, declares the collection of foreign communication as "Routineverkehre" ("routine traffic"), in contrast to "G10 collection" which targets domestic communication protected by the basic law (Article 10) and requires ex-ante authorisation. The foreign domain, however, is an intelligence neverland, as for a long time, neither legal rules nor democratic oversight set limits on surveillance practices.[52] It is convenient, therefore, for intelligence agencies to conduct or even outsource joint operations abroad. Despite its self-declared "homefield advantage as the primary hub for worldwide telecommunications",[53] it became attractive for the NSA to set up cable tapping operations with their third party partners in Europe. Not only could these accesses fill small gaps in its global reach, but there were also no restrictions imposed by law or oversight. The ability of SIGINT agencies to jointly operate in the unregulated foreign domain might also have contributed to the extraordinary close ties in SIGINT.

The high degree of internalisation of a *doxa* and its integration into the practice of the field is also visible in the defensive reactions of the intelligence

agencies cited in the introduction. They experience the claim to extend basic rights protection to foreigners abroad as something that completely escapes the *common sense* of their world and embarrasses them in front of their colleagues abroad. These are precisely the characteristics of a *doxa*: forms of rule and domination are based on it, but it does not come in a diabolical guise or as a coercive measure. "The dominant are generally silent".[54] Their philosophy becomes visible as such only "when they are rankled, when people say to them: 'Why are you like you' are?".[55] Only in retrospect do *doxic* realities become identifiable – sometimes even to rulers themselves. Former NSA director Michael Hayden states:

> we [the NSA] have historically been Manichean about the rest of the world. Are you, or are you not protected by the Fourth Amendment to the US Constitution? Are you? Oh my God, we can't touch you. Are you not? Game on![56]

In similarly sloppy terms, a BND Siginter said that "as long as no basic rights holder is affected, they [data] are cleared for firing [my translation]".[57]

The *doxa* – as part of the *practical sense* of the field – was based on the distinction between domestic and foreign, which was challenged but not abolished by the *object sense,*[58] the transnationality of the Internet. The Internet's methods for transmitting data in packages, in which an e-mail, for example, is fragmented as it is sent and routed over unpredictable geographic routes, make it difficult to distinguish between domestic and foreign communications. In the case of telephone surveillance, area codes made it clear where the communicating party was located. The architecture of the Internet undermines a clean separation of domestic and foreign. However, it is insufficient to simply state that infrastructural conditions have dissolved the distinction. We must also look at the technological practices that have been developed to maintain the distinction. While the BND initially combined algorithmic filters with manual review, the agencies increasingly rely on more automated techniques, including machine learning. Here, communicative relationships determine whether surveillance subjects receive fundamental rights protection or are "fair game". Traditional state rationalities of *jus loci* (territoriality) or *jus sanguinis* (ancestry) as legitimate constitutional principles of citizenship are being replaced in the intelligence field by *jus algoritimi* (communicative behaviour).[59] This shows how state power is simultaneously reproduced and transformed in the transnational SIGINT field.

Contrary to the common narrative of the extraterritoriality of the Internet, the shift of communications from satellites to Internet cables was also accompanied by a re-territorialisation of surveillance. To capture certain foreign communications, agencies required access to cables within their countries, over which communications were routed in ways that made the separation of domestic from foreign communications nearly impossible. The transnationality of the Internet irritated the *doxic* distinctions of domestic and foreign, which

agencies sought to restore with new techniques and new interpretations of law; at least to those outside the field, the arbitrariness of these interpretations was obvious. The BND defined communications routed over German cables as a "virtual foreign country"[60] and the British GCHQ monitored Facebook messages per se as "external" because it was a virtual platform.[61]

Third Party Rule – The code of silence

Another significant and autonomy-enhancing rule in the transnational intelligence game is the *Third Party Rule*. The *Third Party Rule* is not a legal norm,[62] but rather a flexibly interpreted practice by intelligence agencies in which information is shared with third parties only with the consent of the transmitting agency. A flexible interpretation means "that the originator of the information controls to whom it is released",[63] but also that agencies can inquire and negotiate among themselves whether and which parts of information may be passed on and to whom. Both the type of information and the power relations in the field are likely to play a role in these negotiations. Silence, here, is not absolute but works on a continuum. Little is known about the exact procedures in multilateral collaborations within which data from multiple agencies can be aggregated into information. However, it may be even easier to refuse to release information to third parties if all the participants in the network have to agree to disclosure, in accordance with a consensus principle.[64] Despite the flexibility and differences in who is defined as a third party, the rule amounts to a structural exclusion of outsiders from the exchange of information.

In the language of German authorities, the *Third Party Rule* has been described as an "Informationbeherrschungsrecht"[65] – which literally translates as an "information mastery right" – of the sharing agency. In the wording of the Federal Ministry of the Interior, "the issuing state or states remain 'masters of information' and retain the power of disposal over the information they release [own translation]".[66] The masters of information, however, are not primarily sovereign states but the agencies themselves: the globally connected "SIGINT Seniors" whose sharing options are co-determined by their positions in the transnational field, such as the social capital (networks) and symbolic capital (recognition) available to them.

The exclusion of actors external to the field creates an unequal but "shared secrecy"[67] among agencies, which does not precisely display national sovereignty but, on the contrary, can lead to tensions between transnational solidarities and the interests of other national security agencies. In Germany, this was illustrated by discussions surrounding the video footage of the attacker Anis Amri, which the BND received from a foreign intelligence agency after Amri's attack in Berlin in 2016 but did not initially forward to German investigative authorities.[68] Such public cases are both occasions for problematising and legitimising the field practices. The agencies can claim: Without the *Third Party Rule*, we will no longer obtain such information. In practice, however, the rule

is about much more than the "decisive tip" in case of imminent danger, i.e. selective information exchange for terrorist threat prevention. It is the joint practices of the agencies as a whole, which regularly escape external interference and control by referring to a partner's need for secrecy.

The *Third Party Rule* has functional similarities with the unwritten law of the *omertà*, the Mafia's code of silence.[69] Both codes of silence, the *Third Party Rule* and the *omertà* promote internal solidarity and external shielding of their respective fields, becoming a "structural component of the sphere of power [my translation]".[70] As Georg Simmel has noted about secret societies, there is a "protective character" of these societies as an external quality, while their inner quality consists of "a specific type of confidence between the members" built on the mutually expected "ability to preserve silence".[71] The *Third Party Rule* codifies the transnational secrecy of SIGINT beyond state secrecy, being framed as a professional codex in the name of cooperation and the loyal promise to keep the secrets of others. Non-compliance with the *Third Party Rule* in the SIGINT field, while not sanctioned by physical death like the omertà, is punishable in case of doubt by discrediting and isolation in the exchange of information – quasi-professional death. The threat of being cut off from transnational exchange of information can be used or misused by intelligence professionals, at times in public, to hold back information or fend off control. Addressing the parliamentary inquiry into the BND's involvement in Five Eyes cooperation, the former head of the BND, Gerhard Schindler, warned about the consequences of "too much oversight":

> This international cooperation is in danger of lasting damage … the first partner agencies worldwide, not only in Europe, are reviewing their cooperation with the BND, and the signals we are hearing are anything but positive. I am very concerned about this development because ultimately the future of the service is at stake [own translation].[72]

The argument of the agencies is then: if you control us too much, you put your own security at risk.[73] As a consequence, oversight bodies, especially parliamentary bodies, are more or less explicitly defined as third parties in many countries.[74] The *Third Party Rule* institutionalises existing control gaps that arise from the weak regulation of intelligence cooperation and the monitoring of foreigners abroad. If an active inquiry is made, a reference to the *Third Party Rule* often follows. As a legal scholar has noted, considering "the high degree of international networking of intelligence, the *Third Party Rule* leads to a considerable immunisation of the security agencies against domestic investigations [own translation]".[75]

Heteronomy: Oversight and the production of orthodoxy

All fields and the positions within the field are embedded in various relations to other fields. These relations constitute the point of entry for external

(heteronomous) influence on the players and their practices. On the one hand, structural influence is exerted on SIGINT by those fields occupied by its "customers" from the political and bureaucratic field, the military, and the larger intelligence field in which SIGINT agencies work as central distributors of informational capital. As such, SIGINT agencies have to respond to different customer demands and their field logics. This includes quickly delivering "actionable information"[76] for covert action and (para)military operations. SIGINT then becomes intertwined with the life-or-death logic of war, becoming both a potential resource for protecting the lives of soldiers, as often publicly emphasised by intelligence officers, or for the killing of declared enemies. When innocents are targeted as a result of incomplete, inaccurate, or inaccurately interpreted data, the *illusio* of data magic becomes fatal.[77] Another newly pronounced heteronomous force in the past two decades has been the influence of commercial markets for digital data and private intelligence products and personnel on SIGINT.[78] The relationships between SIGINT and commercial (or other) fields require analysis in their own right. However, it is important to note that heteronomy is not a one-way street in these relationships. SIGINT has successfully exported its logics to the private tech world as well.[79]

Despite heteronomous dynamics in both directions, the SIGINT field generally has a high degree of transnational autonomy that consolidates its symbolic power. However, this degree has changed. SIGINT had a very high degree of autonomy in the period from the mid-1960s until the end of the 1980s. The establishment of centralised and often remotely located SIGINT organisations and high budgets in the Cold War context contributed to this autonomy, as did the infrastructures of global, already automated and wireless surveillance of satellite communication – a surveillance practice referred to as using a "vacuum cleaner in the ether"[80] or surveillance of the "open sky"[81] which required neither authorisation nor structural cooperation with hosts of communication carriers. The emergence of the Internet and the dominance of new private actors whose rationalities differed from the traditional telecommunication world, alongside the end of the Cold War, made the field more prone to heteronomous influence.

Intelligence oversight – a heteronomous force?

In intelligence studies, it is often claimed that during the same period – the late 1960s and especially the 1970s – intelligence was put under the rule of law and democratic oversight, which would amount to a loss of autonomy. This narrative is particularly strong in the context of the *Church Committee* in the US[82] and the *Hope Commission* in Australia[83] which, following scandals exposed by whistle-blowers and journalists, led to semi-public investigations into intelligence in these countries for the first time. However, as Félix Tréguer has shown,[84] the institutionalisation of oversight structures in the reforms following the *Church Committee* and the habitus of oversight

professionals actually went along with them being included in the realm of secrecy and following field logics, rather than them acting as a heteronomous force. The "overseers" of intelligence are simultaneously recipients of silence (e.g. when defined as "third parties") and producers of silence, though to a differing degree depending on how close oversight institutions are to the intelligence field and the executive. Generally, the closer an oversight institution and its actors are positioned to the intelligence field, the more information is shared with them, and the more susceptible these actors become to the logics of the field they are supposed to oversee.

Using the information from the Snowden revelations and subsequent inquiries, (again) a wider set of actors (who have been and continue to be formally excluded from intelligence oversight) have started to hold intelligence agencies to account more systematically from the outside, for instance through litigation or campaigning.[85] The following examples show the interplay between external claims challenging the autonomy of SIGINT and its defence, and how courts particularly act as intermediaries in their capacity of normalisation, legitimation, and production of orthodoxy.

Breaking the silence of the doxa

The *doxic* symmetry of cognitive and objective structures – the basis for how the foreign–domestic distinction formerly worked in the field – was broken not only by the *object sense* of the Internet, but also equally by diplomatic and legal discourses that developed on a transnational scale in the wake of the Snowden revelations. In 2013 and 2014, all eyes initially turned to the NSA and its Five Eyes partners. Here, the mass surveillance of foreign communications did not yet appear as what it was, namely, the *doxa* of a transnational field, but as American imperialism. Prompted by a German-Brazilian initiative involving a number of other governments and civil society organisations, a first official heterodox discourse formed that turned the *doxa* into an *orthodoxy*: a UN resolution on the "Right of Privacy in the Digital Age" was launched that challenged the domestic–foreign distinction through the language of human rights and universality.[86] In doing so, data subjects formerly cleared for unregulated surveillance were reconfigured as data citizens, enshrined in international law.[87] This language of human or universal rights was taken up by the Obama Administration in the Presidential Policy Directive 28; on this basis, SIGINT rules were formulated to be valid regardless of nationality.[88]

A decisive moment in the German debate on the *domestic–foreign distinction* was the confrontation of two field discourses in the first public hearing of the Bundestag Inquiry into BND and NSA in May 2014. The interpretations shared by the BND and the German government were challenged by the interpretation of the German basic law of highly respected legal experts, including a former constitutional judge. The basic law's privacy rights, they claimed, are neither tied to citizenship nor territory: "Article 10 [privacy of correspondence] protects as a human right".[89] Despite being

publicly contested by high-profile representatives of the juridical field, the 2016 BND reform upheld the domestic–foreign distinction, though it was further differentiated. European communications were to receive more protection than before, which seemed to be a political move following the revelations of the BND's surveillance of European country representations and EU institutions.

The persisting inconsistency between the intelligence and juridical views and the discursive space it opened became the basis of a constitutional complaint in Germany. The litigation was launched by two civil society organisations which joined forces with international journalists to establish "legal standing"; to make sure that there were claimants who were affected by extraterritorial surveillance[90]. The Federal Constitutional Court's subsequent ruling on BND's SIGINT practices established for the first time with legal force that the surveillance of foreigners abroad also constitutes an encroachment on fundamental rights. The fundamental right to privacy, it declared, has a binding effect on German authorities which is not restricted to German territory.[91] This decision made explicit what a ruling by the constitutional court from 1999 had left open.[92] From a purely juridical point of view, the judges found nothing surprising about the argument of the extraterritorial binding effect of the basic law.[93, 94] Instead, they saw the opposing view held by the BND and the government as a curiosity.[95] The punch of the ruling resulted from the clash of the extraterritoriality argument with the BND's foreign surveillance practices – which seemed to have been almost immune for a long time – and from the fact that the judges made such detailed specifications on the rules of SIGINT and its oversight. However, three examples show how the domestic–foreign distinction was nevertheless not abolished with the ruling and the subsequent BND reform, but became a newly legalised and legitimised orthodoxy.

First, the court ruling does not only declare a different level of protection at home and abroad to be permissible, but also justifies it in terms of legal theory so that, in the end, the logic of the law fits the practical logic of the field. For example, a duty to notify about surveillance, which is provided for German citizens and ultimately enables the claiming of rights, would not be necessary abroad as this would not enable democratic discourse in the same way as the notification requirement does for national citizens.[96] Above all, however, a notification seemed impracticable, even unthinkable for intelligence professionals who used to polemically argue for the territorial logic of privacy protections: "Shall we, then, inform the Chinese or Afghans about our surveillance"? This easy-to-follow argument not only ignores the very broad exceptions for notifications in practice, but also ignores the fact that notifications are not the only mechanism of redress that could be established for non-nationals (for instance, there are institutional channels for complaints). The importance of individual remedies has recently been stressed by international case law on surveillance by intelligence agencies and its oversight. This may enact more far-reaching and more heteronomous demands than national courts.[97]

Second, the maintenance of the distinction is supported by the fact that a special body, the Independent Control Council, was created for the oversight of extraterritorial surveillance instead of either integrating this task into existing oversight structures or bundling it into a new structure.[98] As a result, there is a dual oversight structure that mimics the *foreign–domestic distinction*. Third, the principle of an automated exchange of foreign data is legally legitimised, provided that there is a certain degree of control of the mass of exchanged data.[99]

The juridical field has a special role to play in transforming *doxa* ("what is done") into *orthodoxy* ("what must be done").[100] Equipped with appropriate material and symbolic resources, legal work performatively co-produces the *right view* and can simultaneously reject the definitions of other social worlds as *wrong*. With litigation collectives,[101] new modes of intelligence oversight have emerged that can mobilise the symbolic power of law for contestation, co-producing new *orthodoxies* as a result. However, the expectation that judges could be the "last institutional resort against large-scale surveillance"[102] did not seem to materialise, as the ruling enshrines the legitimacy of mass surveillance as a principle of orthodoxy. The domestic–foreign distinction is not rejected by the court ruling or the reform but is modified in such a way that mass collection and exchange continue to work well.

Contesting and normalising the code of silence

In a quite straightforward way, the 2020 ruling also takes up the obstacles to oversight from the *Third Party Rule.*[103] Citing three different organs of the Council of Europe – the Venice Commission, the Parliamentary Assembly and the Commissioner for Human Rights – it states: "for conducting effective oversight … it must also be ensured that oversight is not obstructed by the third party rule" and "that the bodies conducting legal oversight are no longer considered 'third parties'".[104] By taking a position on the definition of who cannot count as a third party, the ruling clearly intervenes further in the field practices than in its previous ruling dealing with the *Third Party Rule*. In its 2016 decision on the *NSA selectors* (further discussed below), the judges refrained from determining whether or not the rule applies to oversight bodies because "it is upon this agency [sharing intelligence] to determine who it considers to be a 'third party'".[105]

In the subsequent reform, the government designed organisational oversight structures that protect the functioning of the *Third Party Rule* and only slightly displaced its boundaries. Existing oversight bodies, such as the Federal Commissioner for Data Protection and Freedom of Information (BfDI) and the Parliamentary Control Committee (PKGr), remain third parties while the newly created Independent Control Council, formally bound to the executive sphere, is set up as a "control body acting independently of the Third Party Rule".[106] The Control Council is formally inaugurated into the code of silence and must keep this silence when reporting to parliamentary oversight.[107] The

alternative of entrusting already competent data protection authorities with control was rejected; "This, they argued, would be detrimental to international intelligence sharing because of significant reservations and concerns voiced by Germany's main intelligence partners".[108]

Despite having unique competencies for ex-post and ex-ante oversight, it remains questionable to what extent the Independent Control Council will act as an independent and heteronomous player. First, it lacks a form of adversarial council, as required by the ECtHR as a safeguard "against arbitrariness".[109] Second, if the Council finds irregularities and wants to file a complaint, this has to be discussed with the BND first. Third, it is formally integrated into the executive branch, removing intelligence oversight further away from the parliamentary sphere and away from more independent data protection institutions.

Furthermore, while the court found that a narrow definition of the *Third Party Rule* that only includes the agencies and the government and excludes legal oversight would be unlawful, in principle the rule was further legitimised and normalised. Drawing on the 2016 *NSA selectors*' case law, the judges made clear that not only the agencies but also governments may refuse to hand over information to oversight bodies or committees.[110] In the case it referred to, the court legitimised the refusal of the BND and the German government to allow oversight bodies[111] to inspect the search terms shared by the NSA with the BND – the "selectors list".[112] Among these selectors, such as telephone numbers, IP addresses, and e-mail addresses, were technical identifiers of several institutions of the EU and EU countries, including the French ministry for foreign affairs, Le Palais de L'Élysée and the EU-Commission. [113] Additionally, there were identifiers belonging to Germans or individuals within German territory, which had been shared by the NSA with the BND, in violation of the Basic Law and the MOA formalized by the two agencies.[114] Some of the latter were at least temporarily part of the BND's data collection.[115] Instead of the parliamentary committee, a so-called "expert in a position of trust" (sachverständige Vertrauensperson) was appointed to inspect and report[116] on the selectors. While the court acknowledged that this inspection did not satisfy the parliamentary committee's right to collect evidence, it ultimately acted as a protector of the code of silence, undermining independent inquiries into basic rights violations. In deciding that "secrecy interest outweighs the parliamentary interest in information",[117] the court followed the Government's argument that a disclosure of the selectors to the parliamentary committee would be a violation of the mutually promised confidentiality under the *Third Party Rule,* harming the ability of the German intelligence agencies to cooperate.[118]

A legal scholar commenting on the *NSA selectors* ruling noted that, surprisingly, there has never been any documentation of the US-American side's wish to keep the selectors secret, which according to him makes the whole legal decision questionable: "it is not sufficient to use a non-legal norm such as the Third-Party Rule to give constitutional standing to the silence of a foreign

power [my translation]".[119] The code of silence works through silence; when it works perfectly, it completely escapes the public eye and academic research. The case of the *NSA selectors*, in principle cemented by the 2020 ruling, however, provides one example of how the *Third Party Rule* can destabilise democratic oversight of the transnationally constituted field of intelligence.

Conclusion

This paper approaches intelligence and its oversight through the characterisation of the social space of SIGINT, which can be described as a transnational field in Bourdieu's sense. This field perspective allows us to observe dynamics that can be connected to current debates on transnational power and domination and their contestation in digital societies, as well as to understand the dynamics of transnationally connected intelligence agencies and their oversight.

The SIGINT field is an example of transnational domination that is not particularly precarious or weakly autonomous, but relatively stable. This stability, however, does not point to democratic legitimacy. The rule-making and autonomy of the transnational field are accompanied by deficits in parliamentary control that resemble the problem of an inter-ministerial "executive multilateralism".[120] Unlike executive multilateralism, however, the transnational multilateralism of intelligence agencies does not involve democratically elected representatives. The field perspective also draws attention to the fact that the multilateralism of SIGINT is not to be equated with a cooperative and procedural control mechanism, but rather with the emergence of a field with a specialised rationality. However, what is negotiated in the context of field rationalities does not remain in the field. As IR scholar Itamar Mann points out, the rules of global mass surveillance created by SIGINT agencies resemble the "dark side"[121] of Anne-Marie Slaughter's notion of disaggregated sovereignty – not only because the rules defy democratic self-determination, but because they influence how governments interpret their laws and constitutions.[122] There is a problem of democracy in the field of intelligence not because of anomie[123] (i.e. weak or absent orders), but because of autonomy (i.e. self-legislated orders that have an impact on democratic institutions). Fields are not closed spaces, they are intertwined.

The field approach allows for the analysis of the rule-making power of intelligence agencies which are relatively independent of governments – and their potentially anti-democratic tendencies – without having to resort to the idea of a 'deep state'. Considering that the concept of a deep state has been successfully hijacked by conspiracy theorists and right-wing populists, it seems more useful to use the autonomy of fields and the symbolic power attached to them as analytical categories to analyse the (transnational) power of intelligence. The conception of fields in which there are struggles and resistance – "and thus historicity!"[124] – as opposed to apparatuses (as Althusser proposes[125]) or systems (like those of Luhmann[126]), is quite explicitly directed

against the "fantasy of the conspiracy, the idea that an evil will is responsible for everything that happens in the social world".[127] Moving away from a functionalist view of surveillance and intelligence has consequences for thinking about domination. Not only being ruled, but also the exercise of rule involves internal struggles and resistance and is underpinned by unintended and sometimes pre-reflexive dynamics. Transnationally connected intelligence agencies are neither an Orwellian instance of power nor a heroic alliance in defence of our security – neither *deus* nor *diabolus* in machina.[128]

Contemporary forms of digital surveillance do not emerge solely from the logic of digital communication or from the nature of a particular threat.[129] Digital surveillance is rather the product of disputes, struggles, and processes of differentiation of social fields in which sociotechnical interpretations are negotiated, declared as legitimate, and thus become effective as symbolic power. Symbolic domination can be read in terms of its temporality and historicity, which can take *doxic* (uncontested) and *orthodox* (contested) forms. *Doxic* rule describes symbolic relations in which politicisation is initially impossible. Dynamics of politicisation and de-politicisation only set in when the silence of pre-reflexive *doxa* is broken. However, precisely these pre-political states are relevant to domination. They are the product of a misrecognised power that acts gently, though not as the result of a "soft power"[130] that persuades through appeal and attraction, but through the exercise of symbolic violence that categorises and excludes. The exercise of symbolic domination also operates through unquestioned principles of division and habitualised practice and must be included in an analysis of the phenomena of transnational domination.

In the context of other debates on the power of data and surveillance in digital societies, in which much thought is given to the power of social networks, disinformation, and the manipulability of opinions, this reference to the silence of domination is initially irritating. The fact that domination functions not only through discourse, but also through the absence of discourse, does not only apply to intelligence. The surveillance capitalism of Google and Facebook was also able to emerge primarily on the basis of long-term silent acceptance and habitualised forms of data production. In particular, algorithmic order formation[131] and communication infrastructures as a whole[132] are also accompanied by misrecognition effects linked to symbolic power. We can learn from Bourdieu: the misrecognition, and often, the silence of domination and its contingency are the very best conditions for it to work.

This raises the question of how and under what circumstances silent, internalised forms of domination can be broken. These are primarily crises, but also the confrontation of the discourses of different fields, which particularly unmask the field-specific forms of *doxa*. Lastly, a reflexive break with the *doxa* is demanding, but possible. For Bourdieu, however, the break with the *doxa* is primarily performed by sociologists who break with the common sense of their objects of study and thus "destroy a doxa".[133] On this point, this chapter resolutely opposes Bourdieu's "underestimation of actors and …

overestimation of critical social science [own translation]".[134] Next to social sciences and crises, practices oriented towards heteronomous confrontation and irritation can counter *doxic* forms of domination. Breaking the silence of *doxa* is thus not to be understood as a purely intellectual or accidental act, but also as a political act of contestation, and a potentially emancipatory practice. The extent to which oversight can act as a heteronomous force – be it through civic practices, courts, or specific bodies – becomes crucial.

Notes

1 This is a revised and updated version of Ronja Kniep, "'Herren der Information'. Die Transnationale Autonomie Digitaler Überwachung." *Z Politikwissenschaft* 32 (2022): 457–480.
2 Josef Hufelschulte, "Lauscher Ohne Ohren," *Focus*, January 11, 2020, https://www.focus.de/magazin/archiv/politik-lauscher-ohne-ohren_id_11572881.html.
3 Ibid.
4 August Hanning, "BND-Debatte: Gastbeitrag – Absurdistan in Karlsruhe!," *bild.de*, January 14, 2020, https://www.bild.de/politik/inland/politik-inland/bnd-debatte-gastbeitrag-absurdistan-in-karlsruhe-67318416.bild.html.
5 dpa, "Ex-BND-Chef Schindler Warnt Karlsruhe: Sicherheit Nicht Gefährden," *Zeit Online*, December 14, 2019, https://www.zeit.de/news/2019-12/14/ex-bnd-chef-warnt-karlsruhe-sicherheit-nicht-gefaehrden.
6 Rebecca Adler-Nissen, ed., *Bourdieu in International Relations*: *Rethinking Key Concepts in IR,* The new international relations (Abingdon, Oxon: Routledge, 2012); Christian Schmidt-Wellenburg and Stefan Bernhard, eds., *Charting Transnational Fields* (Routledge, 2020).
7 Hager Ben Jaffel et al., "Collective Discussion: Toward Critical Approaches to Intelligence as a Social Phenomenon" *International Political Sociology* 14, no. 3 (2020): 323–44, https://doi.org/10.1093/ips/olaa015.
8 Bernadino Leon-Reyes, "Towards a Reflexive Study of Intelligence Accountability," in *Problematising Intelligence Studies: Towards a New Research Agenda*, ed. Hager Ben Jaffel and Sebastian Larsson, Routledge new intelligence studies (Abingdon, Oxon, New York, NY: Routledge, 2022), 37.
9 Vincent Pouliot, "The Logic of Practicality: A Theory of Practice of Security Communities" *International Organization* 62, no. 2 (2008): 274, https://doi.org/10.1017/S0020818308080090.
10 Pierre Bourdieu and Loïc J. D. Wacquant, *An Invitation to Reflexive Sociology*, Reprinted (Cambridge, Malden, Mass.: Polity Press, 2013), 25.
11 Tugba Basaran et al., eds., *International Political Sociology*: *Transversal Lines,* Routledge studies in international political sociology (Abingdon, Oxon, New York, NY: Routledge, 2017).
12 Reference to Norbert Elias in Pierre Bourdieu, *On the State*: *Lectures at the Collège De France, 1989 – 1992*, ed. Patrick Champagne et al. (Cambridge: Polity, 2014), 123.
13 Ibid., 131.
14 Pierre Bourdieu, *Science of Science and Reflexivity*: *Translated by Richard Nice* (Chicago, IL: University of Chicago Press, 2004), 50.
15 Bourdieu, *On the state*, 213.
16 Matthew M. Aid and Cees Wiebes, *Secrets of Signals Intelligence During the Cold War and Beyond,* Cass series--studies in intelligence (London, Portland, OR: Frank Cass, 2001), 16.
17 Ibid.

18 For a critical discussion see Didier Bigo and Laurent Bonelli, "Digital Data and the Transnational Intelligence Space," in *Data Politics*, eds. Didier Bigo, Engin Isin and Evelyn Ruppert (Abingdon, Oxon; New York, NY: 2019), 105.
19 John B. Thompson and Pierre Bourdieu, eds., *Language and Symbolic Power*: *Edited and Introduced by John B. Thompson. Translated by Gino Raymond and Matthew Adamson*, (Cambridge, Mass.: Polity, 1991), 170.
20 Ibid., 23.
21 Lee Ferran, "Ex-NSA Chief: 'We Kill People Based on Metadata'" *ABC News*, May 12, 2014, https://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata.
22 Thomas R. Johnson, *American Cryptology During the Cold War, 1945–1989*: *Book I: The Struggle for Centralization, 1945–1960,* United States Cryptologic History. Series VI, The NSA Period 1952 – Present Volume 5 (Center For Cryptologic History, National Security Agency, 1995), 2.
23 Wolfgang Krieger, *Partnerdienste*: *Die Beziehungen des BND zu den westlichen Geheimdiensten 1946–1968*. first edition, Veröffentlichungen der Unabhängigen Historikerkommission zur Erforschung der Geschichte des Bundesnachrichtendienstes 1945-1968 Band 12 (Berlin: Ch. Links Verlag, 2021).
24 Johnson, *American Cryptology during the Cold War, 1945–1989*, 108.
25 Andrew O'Neil, "Australia and the 'Five Eyes' intelligence network: the perils of an asymmetric alliance" *Australian Journal of International Affairs* 51, no. 5 (2017); Jean Bou, *MacArthur's Secret Bureau*: *The Story of the Central Bureau, General MacArthur's Signals Intelligence Organisation* (Loftus, N.S.W.: Australian Military History Publications, 2012).
26 Armin Müller, *Wellenkrieg*: *Agentenfunk Und Funkaufklärung Des Bundesnachrichtendienstes 1945–1968*. first edition, Veröffentlichungen der Unabhängigen Historikerkommission zur Erforschung der Geschichte des Bundesnachrichtendienstes 1945-1968 Band 5 (Berlin: Ch. Links Verlag, 2017).
27 Johnson, *American Cryptology during the Cold War, 1945–1989*.
28 Jeffrey T. Richelson and Desmond Ball, *The Ties That Bind*: *Intelligence Cooperation Between the UKUSA Countries - the United Kingdom, the United States of America, Canada, Australia and New Zealand* (Boston: Allen & Unwin, 1990); John Ferris, *Behing the Enigma*: *The Authorised History of GCHQ, Britain's Secret Cyber-Intelligence Agency* (London: Bloomsbury Publishing, 2020), 324f.
29 Thomas L. Burns, *The Quest for Cryptologic Centralization and the Establishment of NSA: 1940-1952,* Series V: The Early Postwar Period VI (Center For Cryptologic History, National Security Agency, 2005), https://www.nsa.gov/portals/75/documents/about/cryptologic-heritage/historical-figures-publications/publications/misc/quest_for_centralization.pdf, 16.
30 Michael Zürn, *A Theory of Global Governance*: *Authority, Legitimacy, and Contestation*, first edition (Oxford, United Kingdom: Oxford University Press, 2018).
31 Richelson and Ball, *The ties that bind*, 228–38.
32 NSA, *Classification Guide for SIGINT Material Dating from 16 August 1945 – 31 December 1967*, March 18, 2023, https://www.aclu.org/foia-document/classification-guide-sigint-material-dating-16-august-1945-31-december-1967
33 Own representation based on NSA, *Approved SIGINT Partners*, March 18, 2023, https://www.aclu.org/foia-document/approved-sigint-partners-and-fad-fy-12-ccp-funding-partners; Bart Jacobs, "Maximator: European Signals Intelligence Cooperation, from a Dutch Perspective" *Intelligence and National Security*, 2020, https://doi.org/10.1080/02684527.2020.1743538.

34 NSA, *Classification Guide for SIGINT Material Dating from 16 August 1945 – 31 December 1967*.
35 NSA, *Coming Soon: A SID Classification Guide*, March 18, 2023, https://theintercept.com/snowden-sidtoday/3991126-coming-soon-a-sid-classification-guide/
36 Bourdieu, *Science of science and reflexivity*, 46.
37 Ibid., 45
38 NSA, *NSA third parties*, March 18, 2023, https://www.aclu.org/foia-document/third-party-relationships
39 Ibid.
40 Laura Poitras et al., "Cover Story: How the NSA Targets Germany and Europe," *SPIEGEL ONLINE*, 2013, http://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html.
41 NSA, *Information Paper NSA Relationship with Germany*, March 18, 2023, https://www.aclu.org/foia-document/information-paper-nsa-relationship-germany
42 Krieger, *Partnerdienste*.
43 Deutscher Bundestag, *Stenografisches Protokoll 118 I*, 2016, 16, https://dserver.bundestag.de/btd/18/CD12850/D_I_Stenografische_Protokolle/Protokoll%20118%20I.pdf
44 Bigo and Bonelli, "Digital Data and the Transnational Intelligence Space."
45 Antoine Vauchez, "Transnationale Expertenfelder Als Schwache Felder. Der Entwurf Des Ersten Weltgerichtshofs Und Die Entstehung Eines Internationalen Expertentums" *Berliner Journal für Soziologie* 24, no. 2 (2014), https://doi.org/10.1007/s11609-014-0249-4.
46 Pierre Bourdieu, *Die Regeln Der Kunst*: *Genese Und Struktur des Literarischen Feldes*, first edition (Frankfurt am Main: Suhrkamp, 2001), 349.
47 Aid and Wiebes, *Secrets of signals intelligence during the Cold War and beyond*, 12–14.
48 For instance, Claudia Aradau and Tobias Blanke, "Governing Others: Anomaly and the Algorithmic Subject of Security" *European Journal of International Security* 3, no. 1 (2018), https://doi.org/10.1017/eis.2017.14.
49 Deutscher Bundestag, *Beschlussfassung Und Bericht Des 1. Untersuchungsausschusses Nach Artikel 44 Des Grundgesetzes*: *Beschlussempfehlung*, 2017, Drucksache 18/12850, 887ff.
50 Deutscher Bundestag, *Beschlussfassung und Bericht des 1. Untersuchungsausschusses nach Artikel 44 des Grundgesetzes*, 1475.
51 Bourdieu, *On the state*, 115.
52 Mark M. Jaycox, "No Oversight, No Limits, No Worries: A Primer on Presidential Spying and Executive Order 12,333" *SSRN Electronic Journal*, 2019, https://doi.org/10.2139/ssrn.3486701.
53 NSA, *IG Report Working Draft*, March 18, 2023, https://www.aclu.org/foia-document/draft-nsa-ig-report, 29
54 Bourdieu, *On the state*, 184.
55 Ibid.
56 Micheal Hayden quoted in Christopher Smith Ochoa, Frank Gadinger, and Taylan Yildiz, "Surveillance Under Dispute: Conceptualising Narrative Legitimation Politics" *European Journal of International Security*, 2020, 13, https://doi.org/10.1017/eis.2020.23.
57 Deutscher Bundestag, *Beschlussfassung und Bericht des 1. Untersuchungsausschusses nach Artikel 44 des Grundgesetzes*, 707.
58 Regula V. Burri, "Soziotechnische Rationalität: Praxistheorie Und Der 'Objektsinn' Von Artefakten" *Soziale Welt* 59, no. 3 (2008), http://www.jstor.org/stable/40878603.

59 John Cheney-Lippold, "Jus Algoritmi: How the National Security Agency Remade Citizenship" *International Journal of Communication* 10, no. 0 (2016), http://ijoc.org/index.php/ijoc/article/download/4480/1618.
60 Stefan Krempl, "Geheimakte BND & NSA: Operation Eikonal – Das Inland Als "Virtuelles Ausland"," *heise online*, April 9, 2017, https://www.heise.de/newsticker/meldung/Geheimakte-BND-NSA-Operation-Eikonal-das-Inland-als-virtuelles-Ausland-3677151.html.
61 Eric King, "Witness Statement of Eric King", 2016, https://privacyinternational.org/sites/default/files/2018-03/2014.06.08%20Eric%20King%20witness%20statement.pdf, 22.
62 Bettina Schöndorf-Haubold, "Auf Dem Weg Zum Sicherheitskooperationsrecht?" in *Nachrichtendienste in Vernetzter Sicherheitsarchitektur*, ed. Jan-Hendrik Dietrich, Klaus F. Gärditz and Kurt Graulich, first edition, Beiträge zum Sicherheitsrecht und zur Sicherheitspolitik (2020), 25.
63 James Clapper, DNI, *Classified State Secrets declaration of DNI Clapper disclosing information regarding the government*, March 18, 2023, https://www.aclu.org/foia-document/dni-clapper-2013-jewelshubert-state-secrets-declaration, 10.
64 Wissenschaftlicher Dienst des Bundestages, *Kontrolle der Tätigkeit der Nachrichtendienste ausgewählter Staaten in der Counter Terrorism Group. Auslegung der sog. Third Party Rule*, 2020, 9, https://www.bundestag.de/resource/blob/711216/545abe8b8e6f5e470b7cc968681685cc/WD-3-046-20-pdf-data.pdf
65 BVerfG, *Order of the Second Senate of 13 October 2016 - 2 BvE 2/15 -,* para. 164., 2016, http://www.bverfg.de/e/es20161013_2bve000215en.html
66 Deutscher Bundestag, BT-Drs. 19/15583, 2019, 21, https://dserver.bundestag.de/btd/19/155/1915583.pdf
67 Didier Bigo, "Shared Secrecy in a Digital Age and a Transnational World" *Intelligence and National Security* 34, no. 3 (2019), https://doi.org/10.1080/02684527.2019.1553703.
68 Ronen Steinke and Florian Flade, "BND Besitzt Bislang Unbekanntes Amri-Video" *Süddeutsche Zeitung*, October 2, 2019, https://www.sueddeutsche.de/politik/breitscheidplatz-amri-bnd-1.4625186.
69 Anton Blok, *Die Mafia in einem sizilianischen Dorf*: *1860–1960; eine Studie über gewalttägige bäuerliche Unternehmer*, first edition, (Frankfurt am Main: Suhrkamp, 1981), 82.
70 Ibid., 260.
71 Georg Simmel, "The Sociology of Secrecy and of Secret Societies," *American Journal of Sociology* 11, no. 4 (1906): 472, https://doi.org/10.1086/211418.
72 Deutscher Bundestag, *Stenografisches Protokoll 50 I*, 2015, 73, https://dserver.bundestag.de/btd/18/CD12850/D_I_Stenografische_Protokolle/Protokoll%2050%20I.pdf
73 Bruno Kahl, "Rahmenbedingungen Und Notwendigkeiten Internationaler Kooperation Von Nachrichtendienten" in *Nachrichtendienste in Vernetzter Sicherheitsarchitektur*, ed. Jan-Hendrik Dietrich, Klaus F. Gärditz and Kurt Graulich, first edition, Beiträge zum Sicherheitsrecht und zur Sicherheitspolitik (2020), 158.
74 Thorsten Wetzling and Kilian Vieth, *Upping the Ante on Bulk Surveillance. An International Compendium of Good Legal Safeguards and Oversight Innovations,* Publication Series on Democracy 50 (Heinrich Böll Stiftung, 2019), https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex5_CompendiumBulkSurveillance.pdf#page=65, 63.
75 Klaus F. Gärditz, "Verweigerung Der Vorlage Von Geheimdienstakten" *DVBl* 14 (2015): 8.

76 NSA, *Generally Speaking: Supporting the Tactical Units*, March 18, 2023, https://www.aclu.org/node/59605
77 Murtaza Hussain, "No Accountability in Military Probe of Kabul Drone Strike — But Intelligence Failures Laid Bare" *The Intercept*, November 5, 2021, https://theintercept.com/2021/11/04/kabul-drone-strike-military-investigation-intelligence/; Spiegel Staff, "Obama's Lists: A Dubious History of Targeted Killings in Afghanistan" *Der Spiegel*, December 28, 2014, https://www.spiegel.de/international/world/secret-docs-reveal-dubious-details-of-targeted-killings-in-afghanistan-a-1010358.html.; Jeremy Scahill and Glenn Greenwald, "The NSA's Secret Role in the U.S. Assassination Program," *The Intercept*, February 10, 2014, https://theintercept.com/2014/02/10/the-nsas-secret-role/.
78 Ronald J. Deibert, "Subversion Inc: The Age of Private Espionage," *Journal of Democracy*, no. 33 (2022), https://www.journalofdemocracy.org/articles/subversion-inc-the-age-of-private-espionage/.
79 Ibid.
80 "»Staubsauger Im Äther«. Interview with Gerhard Güllich" *Der Spiegel*, April 11, 1993, https://www.spiegel.de/politik/staubsauger-im-aether-a-14db5db0-0002-0001-0000-000013679935.
81 Bertold Huber, "Das Neue G 10-Gesetz, 2001" *NJW*, 2001, 3302.
82 Loch K. Johnson, "The Church Committee Investigation of 1975 and the Evolution of Modern Intelligence Accountability" *Intelligence and National Security* 23, no. 2 (2008), 198–225.
83 John Charles Blaxland and Rhys Crawley, *The Secret Cold War*: *The Official History of ASIO, 1976–1989* (Crows Nest: Allen & Unwin, 2018).
84 See his chapter in this volume: Félix Tréguer. 'From Radical Contention to Deference: A Sociogenesis of Intelligence Oversight in the United States (1967–1981)'.
85 Claudia Aradau and Emma Mc Cluskey, "Making Digital Surveillance Unacceptable? Security, Democracy, and the Political Sociology of Disputes" *International Political Sociology* 16, no. 1 (2022), https://doi.org/10.1093/ips/olab024.
86 Elspeth Guild, "Data Rights: Claiming Privacy Rights Through International Institutions," in eds. Didier Bigo, Engin Isin and Evelyn Ruppert (Abingdon, Oxon; New York, NY: 2019)
87 Ibid., 281.
88 President of the United States, *Presidential Policy Directive. Signals Intelligence Activities*, 2014, https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.
89 Deutscher Bundestag, *Stenografisches Protokoll 5 I*, 2014, 6f.
90 Gesellschaft für Freiheitsrechte, "BND Law on worldwide mass surveillance", 2018, https://freiheitsrechte.org/en/themen/digitale-grundrechte/bnd-gesetz-2
91 BVerfG, *Judgment of the First Senate of 19 May 2020 - 1 BvR 2835/17* -, Ls 1-2, 2020, http://www.bverfg.de/e/rs20200519_1bvr283517en.html
92 BVerfG, *Order of the First Senate of 14 July 1999 - 1 BvR 2226/94* -, paras. 1–308, 1999, http://www.bverfg.de/e/rs19990714_1bvr222694en.html, para. 173.
93 Robert Uerpmann-Wittzack, "Der Offene Rechtsstaat Und Seine Freunde" *JURA - Juristische Ausbildung* 42, no. 9 (2020), https://doi.org/10.1515/jura-2020-2536.
94 Björn Schiffbauer, "Die Würde des Rechtsstaats ist unantastbar" *JuWissBlog* no. 75, 2020, https://www.juwiss.de/75-2020/
95 Ibid.
96 BVerfG 2020, para. 269
97 With reference to *Big Brother Watch v. UK*, *Centrum för Rättvisa v. Sweden*, and *Schrems II* in Kilian Vieth-Ditlmann and Thorsten Wetzling, "Caught in the Act?

An analysis of Germany's new SIGINT reform" (2021), https://www.stiftung-nv.de/sites/default/files/caught-in-the-act_analysis-of-germanys-new-sigint-reform_0.pdf, 63f.

98 Thorsten Wetzling and Daniel Moßbrucker, "BND-Reform, die Zweite: Vorschläge zur Neustrukturierung der Nachrichtendienst-Kontrolle" (2020), https://www.stiftung-nv.de/de/publikation/bnd-reform-die-zweite, 2.

99 BVerfG 2020, Ls. 7, paras. 262, 323

100 Bourdieu, *On the state*, 256.

101 Lisa Hahn and Myriam von Fromberg, "Klagekollektive Als „Watchdogs",*Z Politikwissenschaft*, 2020, https://doi.org/10.1007/s41358-020-00241-4.

102 Félix Tréguer, "Intelligence Reform and the Snowden Paradox: The Case of France," in "Post-Snowden Internet Policy," ed. Julia Pohle and Leo van Audenhove, special issue, *Media and Communication* 5, no. 1 (2017): 17–28, http://www.cogitatiopress.com/mediaandcommunication/article/download/821/821, 25–26.

103 BVerG 2020, paras. 32, 51

104 BVerG 2020, para 292; 294

105 BVerf 2016, para. 163

106 Deutscher Bundestag, BT-Drs. 19/26103, 2021, 50.

107 Ibid., p. 100

108 Elspeth Guild and Thorsten Wetzling, "Germany's BND Act & Recent CJEU Case Law – About:Intel," *about:intel*, February 17, 2021, https://aboutintel.eu/bnd-reform-cjeu/.

109 European Court of Human Rights, *Centrum för Rättvisa v. Sweden*, 25.05.2021, para. 297, https://data.guardint.org/en/entity/wdwrxl9tv6f?page=79

110 BVerG 2020, para. 293

111 The parliamentary 'NSA inquiry committee' – a committee created to investigate the BND's involvement in the Five Eyes – and the G10 commission who back then was the only quasi-judicial oversight body in Germany.

112 BVerfG 2016

113 Georg Mascolo, "Geheimdienst-Affäre - BND Half NSA Beim Ausspähen Von Frankreich Und EU-Kommission - Politik - SZ," *sueddeutsch.de*, April 29, 2015, accessed November 13, 2022, https://www.sueddeutsche.de/politik/geheimdienst-affaere-bnd-half-nsa-beim-ausspaehen-von-frankreich-und-eu-kommission-1.2458574.

114 Kurt Graulich, *Nachrichtendienstliche Fernmeldeaufklärung mit Selektoren in einer transnationalen Kooperation: Prüfung und Bewertung von NSA-Selektoren nach Maßgabe des Beweisschlusses BND-26*, 2015, https://www.bundestag.de/resource/blob/393598/b5d50731152a09ae36b42be50f283898/mat_a_sv-11-2-data.pdf., 158 f., 142 ff., 174 ff., 182, 216 f.

115 Ibid., 176.

116 Ibid.

117 BVerG 2016, Ls 5.

118 Ibid., para. 2; See Bigo in this volume, p.X

119 Christoph Möllers, "Von Der Kernbereichsgarantie Zur Exekutiven Notstandsprärogative: Zum BND-Selektoren-Beschluss Des BVerfG" *JuristenZeitung* 72, no. 6 (2017): 278, https://doi.org/10.1628/002268817×X14870706821192.

120 Michael Zürn, "Global Governance and Legitimacy Problems" *Government and Opposition* 39, no. 2 (2004): 264, https://doi.org/10.1111/j.1477-7053.2004.00123.x.

121 Itamar Mann, "The Disaggregated Law of Global Mass Surveillance" in *The Changing Practices of International Law*, ed. Tanja E. Aalberts and Thomas Gammeltoft-Hansen (New York: Cambridge University Press, 2018), 155.

122 Mann, "The Disaggregated Law of Global Mass Surveillance," 130.

123 Andreas Friedel, "Anomie Durch Kontrollverlust? Handlungsspielräume Und Lenkungsprobleme Deutscher Geheimdienste" in *Demokratie und Anomie: Eine Fundamentale Herausforderung Moderner Volksherrschaft in Theorie Und Praxis*, ed. Martin Sebaldt et al. (Wiesbaden: Springer Fachmedien Wiesbaden, 2020).
124 Bourdieu and Wacquant, *An invitation to reflexive sociology*, 102.
125 Louis Althusser, *On the reproduction of capitalism. Ideology and ideological state apparatuses*. (London: Verso, 2014).
126 Dirk Baecker and Niklas Luhmann, *Introduction to systems theory*. (Cambridge, UK: Polity, 2013).
127 Ibid.
128 Bourdieu, *On the state*, 6.
129 Bigo, "Shared secrecy in a digital age and a transnational world," 391.
130 Joseph Nye, "Soft power: the evolution of a concept" *Journal of Political Power* 14, no. 1 (2021), 196-208.
131 Christian Katzenbach and Lena Ulbricht, "Algorithmic Governance," *Internet Policy Review* 8, no. 4 (2019), https://doi.org/10.14763/2019.4.1424.
132 Jeanette Hofmann, "Digitale Kommunikationsinfrastrukturen," in *Handbuch Digitalisierung in Staat Und Verwaltung*, ed. Tanja Klenk, Frank Nullmeier and Göttrik Wewer (Wiesbaden: Springer Fachmedien Wiesbaden, 2020).
133 Bourdieu, *On the state*, 117.
134 Robin Celikates, *Kritik als soziale Praxis*: *Gesellschaftliche Selbstverständigung und kritische Theorie,* Frankfurter Beiträge zur Soziologie und Sozialphilosophie 13 (Frankfurt/Main: Campus-Verl., 2009), 95.

References

Adler-Nissen, Rebecca, ed. *Bourdieu in International Relations: Rethinking Key Concepts in IR*. The new international relations. Abingdon, Oxon: Routledge, 2012.

Aid, Matthew M., and Cees Wiebes. *Secrets of Signals Intelligence During the Cold War and Beyond*. Cass series—studies in intelligence. London, Portland, OR: Frank Cass, 2001.

Althusser, Louis. *On the reproduction of capitalism. Ideology and ideological state apparatuses*. London: Verso, 2014.

Aradau, Claudia. "Assembling (Non)Knowledge: Security, Law, and Surveillance in a Digital World." *International Political Sociology* 11, no. 4 (2017): 327–342.

Aradau, Claudia, and Tobias Blanke. "Governing Others: Anomaly and the Algorithmic Subject of Security." *European Journal of International Security* 3, no. 1 (2018): 1–21. 10.1017/eis.2017.14.

Aradau, Claudia, and Emma Mc Cluskey. "Making Digital Surveillance Unacceptable? Security, Democracy, and the Political Sociology of Disputes." *International Political Sociology* 16, no. 1 (2022). 10.1093/ips/olab024.

Baecker, Dirk, and Niklas Luhmann. *Introduction to systems theory*. Cambridge, UK: Polity, 2013.

Basaran, Tugba, Didier Bigo, Emmanuel-Pierre Guittet, and R.B.J. Walker, eds. *International Political Sociology: Transversal Lines*. Routledge studies in international political sociology. Abingdon, Oxon, New York, NY: Routledge, 2017.

Ben Jaffel, Hager, Alvina Hoffmann, Oliver Kearns, and Sebastian Larsson. "Collective Discussion: Toward Critical Approaches to Intelligence as a Social Phenomenon." *International Political Sociology* (2020). 10.1093/ips/olaa015.

Bigo, Didier. "Shared Secrecy in a Digital Age and a Transnational World." *Intelligence and National Security* 34, no. 3 (2019): 379–394. 10.1080/02684527.2019.1553703.

Bigo, Didier, and Laurent Bonelli. "Digital Data and the Transnational Intelligence Space." In *Data Politics*, edited by Didier Bigo, Engin Isin, and Evelyn Ruppert, 100–122. Abingdon, Oxon; New York, NY, 2019.

Bigo, Didier, Engin F. Isin, and Evelyn Sharon Ruppert, eds. *Data Politics: Worlds, Subjects, Rights*. Routledge studies in international political sociology. Abingdon, Oxon, New York, NY: Routledge, 2019.

Blaxland, John Charles, and Rhys Crawley. *The Secret Cold War: The Official History of ASIO, 1976–1989*. Crows Nest: Allen & Unwin, 2018.

Blok, Anton. *Die Mafia in einem sizilianischen Dorf: 1860–1960; eine Studie über gewalttägige bäuerliche Unternehmer*, First edition. Frankfurt am Main: Suhrkamp, 1981.

Bou, Jean. *MacArthur's Secret Bureau: The Story of the Central Bureau, General MacArthur's Signals Intelligence Organisation*. Loftus, N.S.W.: Australian Military History Publications, 2012.

Bourdieu, Pierre. *Die Regeln Der Kunst: Genese Und Struktur des Literarischen Feldes*, First edition. Frankfurt am Main: Suhrkamp, 2001.

Bourdieu, Pierre. *Science of Science and Reflexivity*, translated by Richard Nice. Chicago, IL: University of Chicago Press, 2004.

Bourdieu, Pierre. *On the State: Lectures at the Collège De France, 1989–1992*, edited by Patrick Champagne et al.. Cambridge: Polity, 2014.

Bourdieu, Pierre, and Loïc J. D. Wacquant. *An Invitation to Reflexive Sociology*. Reprinted. Cambridge, Malden, Mass.: Polity Press, 2013.

Burns, Thomas L. *The Quest for Cryptologic Centralization and the Establishment of NSA: 1940-1952*. Series V: The Early Postwar Period VI, Center For Cryptologic History. National Security Agency, 2005. https://www.nsa.gov/portals/75/documents/about/cryptologic-heritage/historical-figures-publications/publications/misc/quest_for_centralization.pdf.

Burri, Regula Valérie. "Soziotechnische Rationalität: Praxistheorie Und Der 'Objektsinn' Von Artefakten." *Soziale Welt* 59, no. 3 (2008): 269–286. http://www.jstor.org/stable/40878603.

BverfG. *Order of the First Senate of 14 July 1999 - 1 BvR 2226/94* -, paras. 1-308, 1999. http://www.bverfg.de/e/rs19990714_1bvr222694en.html.

BverfG. *Order of the Second Senate of 13 October 2016 - 2 BvE 2/15* -, paras. 1-190, 2016, http://www.bverfg.de/e/es20161013_2bve000215en.html.

BverfG. *Judgment of the First Senate of 19 May 2020 - 1 BvR 2835/17* -, paras. 1-332, 2020, http://www.bverfg.de/e/rs20200519_1bvr283517en.html.

Celikates, Robin. *Kritik als soziale Praxis: Gesellschaftliche Selbstverständigung und kritische Theorie*. Frankfurter Beiträge zur Soziologie und Sozialphilosophie 13. Frankfurt/Main: Campus-Verl., 2009.

Cheney-Lippold, John. "Jus Algoritmi: How the National Security Agency Remade Citizenship." *International Journal of Communication* 10, no. 0 (2016): 1721–1742. http://ijoc.org/index.php/ijoc/article/download/4480/1618.

Clapper, James. *Classified State Secrets declaration of DNI Clapper disclosing information regarding the government*. March 18, 2023. https://www.aclu.org/foia-document/dni-clapper-2013-jewelshubert-state-secrets-declaration.

Deibert, Ronald J. "Subversion Inc: The Age of Private Espionage." *Journal of Democracy* no. 33 (2022): 28–44. https://www.journalofdemocracy.org/articles/subversion-inc-the-age-of-private-espionage/.

Deutscher Bundestag. *Stenografisches Protokoll 118 I*. 2016. https://dserver.bundestag.de/btd/18/CD12850/D_I_Stenografische_Protokolle/Protokoll%20118%20I.pdf.

Deutscher Bundestag. *Stenografisches Protokoll 50 I*. 2015. https://dserver.bundestag.de/btd/18/CD12850/D_I_Stenografische_Protokolle/Protokoll%2050%20I.pdf.

Deutscher Bundestag. *Stenografisches Protokoll 5 I*. 2014. http://dipbt.bundestag.de/dip21/btd/18/CD12850/D_I_Stenografische_Protokolle/Protokoll%2005%20I.pdf.

Deutscher Bundestag. *Beschlussfassung Und Bericht Des 1. Untersuchungsausschusses Nach Artikel 44 Des Grundgesetzes: Beschlussempfehlung*. Drucksache 18/12850, 2017.

Deutscher Bundestag. *BT-Drs. 19/15583*. 2019. https://dserver.bundestag.de/btd/19/155/1915583.pdf.

Deutscher Bundestag. *BT-Drs. 19/26103*. 2021. https://dserver.bundestag.de/btd/19/261/1926103.pdf.

dpa. "Ex-BND-Chef Schindler Warnt Karlsruhe: Sicherheit Nicht Gefährden." *Zeit Online*, December 14, 2019. https://www.zeit.de/news/2019-12/14/ex-bnd-chef-warnt-karlsruhe-sicherheit-nicht-gefaehrden.

European Court of Human Rights. *Centrum för Rättvisa v. Sweden*, para. 297, 25.05.2021. https://data.guardint.org/en/entity/wdwrxl9tv6f?page=79.

Ferran, Lee. "Ex-NSA Chief: 'We Kill People Based on Metadata'." *ABC News*, May 12, 2014. https://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata.

Ferris, John. *Behing the Enigma: The Authorised History of GCHQ, Britain's Secret Cyber-Intelligence Agency*. London: Bloomsbury Publishing, 2020.

Friedel, Andreas. "Anomie Durch Kontrollverlust? Handlungsspielräume Und Lenkungsprobleme Deutscher Geheimdienste." In *Demokratie Und Anomie: Eine Fundamentale Herausforderung Moderner Volksherrschaft in Theorie Und Praxis*, edited byMartin Sebaldt et al., 41–73. Wiesbaden: Springer Fachmedien Wiesbaden, 2020.

Gärditz, Klaus F. "Verweigerung Der Vorlage Von Geheimdienstakten." *DVBl* 14 (2015).

Gesellschaft für Freiheitsrechte. "BND Law on worldwide mass surveillance." 2018. https://freiheitsrechte.org/en/themen/digitale-grundrechte/bnd-gesetz-2.

Graulich, Kurt. *Nachrichtendienstliche Fernmeldeaufklärung Mit Selektoren in Einer Transnationalen Kooperation: Prüfung Und Bewertung Von NSA-Selektoren Nach Maßgabe Des Beweisschlusses BND-26*. October 23, 2015. https://www.bundestag.de/resource/blob/393598/b5d50731152a09ae36b42be50f283898/mat_a_sv-11-2-data.pdf.

Guild, Elspeth. "Data Rights: Claiming Privacy Rights Through International Institutions." In *Data Politics*, edited by Didier Bigo, Engin Isin and Evelyn Ruppert, 267–284. Abingdon, Oxon; New York, NY, 2019.

Guild, Elspeth, and Thorsten Wetzling. "Germany's BND Act & Recent CJEU Case Law – About:Intel." *about:intel* (February 21, 2021). https://aboutintel.eu/bnd-reform-cjeu/.

Hahn, Lisa, and Myriam von Fromberg. "Klagekollektive Als „Watchdogs"." *Z Politikwissenschaft* (2020). 10.1007/s41358-020-00241-4.

Hanning, August. "BND-Debatte: Gastbeitrag – Absurdistan in Karlsruhe!" *bild.de* (January 14, 2020). https://www.bild.de/politik/inland/politik-inland/bnd-debatte-gastbeitrag-absurdistan-in-karlsruhe-67318416.bild.html.

Hofmann, Jeanette. "Digitale Kommunikationsinfrastrukturen." In *Handbuch Digitalisierung in Staat Und Verwaltung*, edited by Tanja Klenk, Frank Nullmeier and Göttrik Wewer, 1–11. Wiesbaden: Springer Fachmedien Wiesbaden, 2020.

Huber, Bertold. "Das Neue G 10-Gesetz, 2001." *NJW* (2001): 3296–3302.

Hufelschulte, Josef. "Lauscher Ohne Ohren." *Focus* (January 11, 2020). https://www.focus.de/magazin/archiv/politik-lauscher-ohne-ohren_id_11572881.html.

Hussain, Murtaza. "No Accountability in Military Probe of Kabul Drone Strike — But Intelligence Failures Laid Bare." *The Intercept* (November 5, 2021). https://theintercept.com/2021/11/04/kabul-drone-strike-military-investigation-intelligence/.

Jacobs, Bart. "Maximator: European Signals Intelligence Cooperation, from a Dutch Perspective." *Intelligence and National Security* (2020): 1–10. 10.1080/02684527.2020.1743538.

Jaycox, Mark M. "No Oversight, No Limits, No Worries: A Primer on Presidential Spying and Executive Order 12,333." *SSRN Electronic Journal* (2019): 10.2139/ssrn.3486701.

Johnson, Thomas R. *American Cryptology During the Cold War, 1945-1989: Book I: The Struggle for Centralization, 1945-1960*. United States Cryptologic History. Series VI, The NSA Period 1952 – Present Volume 5. Center For Cryptologic History, National Security Agency, 1995.

Johnson, Loch K. "The Church Committee Investigation of 1975 and the Evolution of Modern Intelligence Accountability." *Intelligence and National Security* 23, no 2 (2008): 198–225.

Kahl, Bruno. "Rahmenbedingungen Und Notwendigkeiten Internationaler Kooperation Von Nachrichtendienten." In *Nachrichtendienste in Vernetzter Sicherheitsarchitektur*, edited by Jan-Hendrik Dietrich, Klaus F. Gärditz and Kurt Graulich, First edition, 153–162. Beiträge zum Sicherheitsrecht und zur Sicherheitspolitik, 2020.

Katzenbach, Christian, and Lena Ulbricht. "Algorithmic Governance." *Internet Policy Review* 8, no. 4 (2019). 10.14763/2019.4.1424.

King, Eric. "Witness Statement of Eric King." 2016. https://privacyinternational.org/sites/default/files/2018-03/2014.06.08%20Eric%20King%20witness%20statement.pdf.

Kniep, Ronja. "'Herren Der Information'. Die Transnationale Autonomie Digitaler Überwachung." *Z Politikwissenschaft* 32 (2022): 457–480.

Krempl, Stefan. "Geheimakte BND & NSA: Operation Eikonal – Das Inland Als "Virtuelles Ausland". *heise online* (April 9, 2017). https://www.heise.de/newsticker/meldung/Geheimakte-BND-NSA-Operation-Eikonal-das-Inland-als-virtuelles-Ausland-3677151.html.

Krieger, Wolfgang. *Partnerdienste: Die Beziehungen des BND zu den westlichen Geheimdiensten 1946-1968*, First edition, Veröffentlichungen der Unabhängigen Historikerkommission zur Erforschung der Geschichte des Bundesnachrichtendienstes 1945-1968 Band 12. Berlin: Ch. Links Verlag, 2021.

Leon-Reyes, Bernadino. "Towards a Reflexive Study of Intelligence Accountability." In *Problematising Intelligence Studies: Towards a New Research Agenda*, edited by Hager Ben Jaffel and Sebastian Larsson, 30–47. Routledge new intelligence studies. Abingdon, Oxon, New York, NY: Routledge, 2022.

Mann, Itamar. "The Disaggregated Law of Global Mass Surveillance." In *The Changing Practices of International Law*, edited by Tanja E. Aalberts and Thomas Gammeltoft-Hansen, 129–157. New York: Cambridge University Press, 2018.

Mascolo, Georg. "Geheimdienst-Affäre - BND Half NSA Beim Ausspähen Von Frankreich Und EU-Kommission - Politik - SZ." *sueddeutsch.de*, April 29, 2015. https://www.sueddeutsche.de/politik/geheimdienst-affaere-bnd-half-nsa-beim-ausspaehen-von-frankreich-und-eu-kommission-1.2458574.

Möllers, Christoph. "Von Der Kernbereichsgarantie Zur Exekutiven Notstandsprärogative: Zum BND-Selektoren-Beschluss Des BVerfG." *JuristenZeitung* 72, no. 6 (2017): 271. 10.1628/002268817X14870706821192.

Müller, Armin. *Wellenkrieg: Agentenfunk Und Funkaufklärung Des Bundesnachrichtendienstes 1945–1968*, First edition. Veröffentlichungen der Unabhängigen Historikerkommission zur Erforschung der Geschichte des Bundesnachrichtendienstes 1945-1968 Band 5. Berlin: Ch. Links Verlag, 2017.

NSA. *Approved SIGINT Partners*. March 18, 2023. https://www.aclu.org/foia-document/approved-sigint-partners-and-fad-fy-12-ccp-funding-partners.

NSA. *Classification Guide for SIGINT Material Dating from 16 August 1945 – 31 December 1967*. March 18, 2023. https://www.aclu.org/foia-document/classification-guide-sigint-material-dating-16-august-1945-31-december-1967.

NSA. *Coming Soon: A SID Classification Guide*. March 18, 2023. https://theintercept.com/snowden-sidtoday/3991126-coming-soon-a-sid-classification-guide/.

NSA. *NSA third parties*. March 18, 2023. https://www.aclu.org/foia-document/third-party-relationships.

NSA. *Information Paper NSA Relationship with Germany*. March 18, 2023. https://www.aclu.org/foia-document/information-paper-nsa-relationship-germany.

NSA. *IG Report Working Draft*. March 18, 2023. https://www.aclu.org/foia-document/draft-nsa-ig-report.

NSA. *Generally Speaking: Supporting the Tactical Units*. March 18, 2023. https://www.aclu.org/node/59605.

Nye, Joseph. "Soft power: the evolution of a concept." *Journal of Political Power* 14, no. 1 (2021): 196–208.

O'Neil, Andrew. "Australia and the 'Five Eyes' intelligence network: the perils of an asymmetric alliance." *Australian Journal of International Affairs* 51, no. 5 (2017): 529–543.

Poitras, Laura, Marcel Rosenbach, Fidelius Schmid, Holger Stark, and Jonathan Stock. "Cover Story: How the NSA Targets Germany and Europe." *SPIEGEL ONLINE*, June 1, 2013. http://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html.

Pouliot, Vincent. "The Logic of Practicality: A Theory of Practice of Security Communities." *International Organization* 62, no. 2 (2008): 257–288. 10.1017/S0020818308080090.

President of the United States. "Presidential Policy Directive. Signals Intelligence Activities." 2014. https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

Richelson, Jeffrey T., and Desmond Ball. *The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries - the United Kingdom, the United States of America, Canada, Australia and New Zealand*. Boston: Allen & Unwin, 1990.

Scahill, Jeremy, and Glenn Greenwald. "The NSA's Secret Role in the U.S. Assassination Program." *The Intercept*, February 10, 2014. https://theintercept.com/2014/02/10/the-nsas-secret-role/.

Schiffbauer, Björn. "Die Würde des Rechtsstaats ist unantastbar." *JuWissBlog* no. 75 (2020): accessed November 2, 2022. https://www.juwiss.de/75-2020/.

Schmidt-Wellenburg, Christian, and Stefan Bernhard, eds. *Charting Transnational Fields*. Routledge, 2020.

Schöndorf-Haubold, Bettina. "Auf Dem Weg Zum Sicherheitskooperationsrecht?" In *Nachrichtendienste in Vernetzter Sicherheitsarchitektur*, edited byJan-Hendrik Dietrich, Klaus F. Gärditz and Kurt Graulich, First edition, 3–34. Beiträge zum Sicherheitsrecht und zur Sicherheitspolitik, 2020.

Simmel, Georg. "The Sociology of Secrecy and of Secret Societies." *American Journal of Sociology* 11, no. 4 (1906): 441–498. 10.1086/211418.

Smith Ochoa, Christopher, Frank Gadinger, and Taylan Yildiz. "Surveillance Under Dispute: Conceptualising Narrative Legitimation Politics." *European Journal of International Security* (2020): 1–23. 10.1017/eis.2020.23.

Staff, Spiegel. "Obama's Lists: A Dubious History of Targeted Killings in Afghanistan." *Der Spiegel*, December 28, 2014. https://www.spiegel.de/international/world/secret-docs-reveal-dubious-details-of-targeted-killings-in-afghanistan-a-1010358.html.

"»Staubsauger Im Äther«. Interview with Gerhard Güllich." *Der Spiegel*, April 11, 1993. https://www.spiegel.de/politik/staubsauger-im-aether-a-14db5db0-0002-0001-0000-000013679935.

Steinke, Ronen, and Florian Flade. "BND Besitzt Bislang Unbekanntes Amri-Video." *Süddeutsche Zeitung*, October 2, 2019. https://www.sueddeutsche.de/politik/breitscheidplatz-amri-bnd-1.4625186.

Thompson, John B., and Pierre Bourdieu, eds. *Language and Symbolic Power: Edited and Introduced by John B. Thompson. Translated by Gino Raymond and Matthew Adamson*. 1. publ. in paperb., repr. Cambridge, Mass.: Polity, 1991.

Tréguer, Félix. "Intelligence Reform and the Snowden Paradox: The Case of France." In *Post-Snowden Internet Policy*, edited by Julia Pohle and Leo van Audenhove. Special issue, *Media and Communication* 5, no. 1 (2017): 17–28. http://www.cogitatiopress.com/mediaandcommunication/article/download/821/821.

Tréguer, Félix. "From Radical Contention to Deference: A Sociogenesis of Intelligence Oversight in the United States (1967–1981)", edited by Didier Bigo, Emma Mc Cluskey, and Félix Tréguer. New Intelligence Studies. Routledge, 2023.

Uerpmann-Wittzack, Robert. "Der Offene Rechtsstaat Und Seine Freunde." *JURA – Juristische Ausbildung* 42, no. 9 (2020): 953–961. 10.1515/jura-2020-2536.

Vauchez, Antoine. "Transnationale Expertenfelder Als Schwache Felder. Der Entwurf Des Ersten Weltgerichtshofs Und Die Entstehung Eines Internationalen Expertentums." *Berliner Journal für Soziologie* 24, no. 2 (2014): 201–226. 10.1007/s11609-014-0249-4.

Vieth-Ditlmann, Kilian, and Thorsten Wetzling. "Caught in the Act? An Analysis of Germany's New SIGINT Reform." November 25, 2021. https://www.stiftung-nv.de/sites/default/files/caught-in-the-act_analysis-of-germanys-new-sigint-reform_0.pdf.

Wetzling, Thorsten, and Daniel Moßbrucker. "BND-Reform, Die Zweite: Vorschläge Zur Neustrukturierung Der Nachrichtendienst-Kontrolle." 2020. https://www.stiftung-nv.de/de/publikation/bnd-reform-die-zweite.

Wetzling, Thorsten, and Kilian Vieth. "Upping the Ante on Bulk Surveillance. An International Compendium of Good Legal Safeguards and Oversight Innovations".

Publication Series on Democracy 50. Heinrich Böll Stiftung, 2019. https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex5_CompendiumBulkSurveillance.pdf#page=65.

Wissenschaftlicher Dienst des Bundestages. *Kontrolle Der Tätigkeit Der Nachrichtendienste Ausgewählter Staaten in Der Counter Terrorism Group. Auslegung Der Sog. Third Party Rule*. 2020. https://www.bundestag.de/resource/blob/711216/545abe8b8e6f5e470b7cc968681685cc/WD-3-046-20-pdf-data.pdf.

Zürn, Michael. "Global Governance and Legitimacy Problems." *Government and Opposition* 39, no. 2 (2004): 260–287. 10.1111/j.1477-7053.2004.00123.x.

Zürn, Michael. *A Theory of Global Governance: Authority, Legitimacy, and Contestation*, First edition. Oxford, United Kingdom: Oxford University Press, 2018. https://ebookcentral.proquest.com/lib/gbv/detail.action?docID=5313274.

4 From abuse to trust and back again

Intelligence scandals and the quest for oversight

Emma Mc Cluskey and Claudia Aradau

Introduction

In the wake of the Snowden disclosures, the Independent Reviewer of Terrorism Legislation in the United Kingdom (UK), Sir David Anderson, was called upon by the government to evaluate the practices of the intelligence agencies. "This Commission", recalls Anderson, "had its genesis in political dispute".[1] The report was published under the title "A Question of Trust". In his recollection, Anderson describes the political context in which the report was produced as one of heightened mistrust:

> The post-Snowden environment was characterised by mutual mistrust between the privacy and security lobbies, often expressed in emotional accusations: of deceit, snooping and scorn for democracy on one side, lack of appreciation for the security forces on the other.
>
> Those well-worn epithets, Orwellian and Kafkaesque, are still wheeled out from time to time, but serious commentators have moved on to serious questions.[2]

Anderson's diagnosis is one of many which see a post-Snowden context of mistrust and proceed to restore the lost trust. His diagnosis also resonates with wider anxieties about the "decline of trust" in democracy and a problematisation of the relations between trust and democracy.[3] Should there be trust in democratic institutions, including governments, and is trust even desirable? There are many conflicting answers to these questions. On the one hand, some political scientists hold that ideas of personal or direct trust between individuals cannot and should not be extended to indirect or impersonal trust; trust which concerns formal institutions.[4] For political philosopher Pierre Rosanvallon, trust is inimical to democracy, as it is distrust that is the engine of democratic action: "Its [distrust's] purpose is to make sure that elected officials keep their promises and to find ways of maintaining pressure on the government to serve the common good".[5] On the other hand, trust has been seen as an ingredient for collective action and a

DOI: 10.4324/9781003354130-5

"power-saving" device for democracies,[6] as it reduces the costs of citizen watchfulness and monitoring.

This chapter proposes to approach the invocation of trust in intelligence agencies historically rather than through a definition of trust as legitimate or illegitimate, desirable or undesirable, or integral or antithetical to democracy. By juxtaposing two historical moments of scandal about the activities of intelligence agencies in the UK, we argue that Anderson's arguments are part of a wide-ranging reframing of abuse by intelligence agencies through narratives of trust and mistrust. "Abuse" and "trust" are two different diagnoses of the relations between citizens and government, between intelligence agencies and parliaments whereby trust obscures an analysis of power. Trust enters a binary relation with mistrust or distrust, one where state authorities and the secret services are supposed to "win" the public's trust or show themselves worthy of the citizens' trust. In this articulation, we show how trust becomes re-personalised as "being" trustworthy. State institutions are decomposed into trustworthy individuals whom parliamentarians, overseers, and publics know to be "trustworthy". Unlike personalised trust, abuse is about stabilised and systematic hierarchies of power. The power asymmetries between institutions and citizens (or non-citizens) are such a situation where "abuse" comes to reframe power relations. In that sense, abuse is a diagnosis of action, of "wrong-doing" rather than "being trustworthy". Yet, abuse can also be limited if framed only as deviance, as exceptional rather than a more systemic effect of power relations.

We show how abuse and trust underpin different modes of democratic oversight by enabling or foreclosing demands for accountability. The chapter argues that the mobilisation of "trust" as a discourse in relation to the intelligence and security services constrains the terrain of possible democratic oversight, rendering some practices of oversight actionable and others not. "Trust" discourses, somewhat counterintuitively, facilitate greater impunity for intelligence agencies, allowing them to evade accountability and scrutiny. By positing a direct relation between publics and governments, trust/mistrust homogenises them as two different spheres and thereby obfuscates the social struggles over who and what counts in these debates. In conclusion, we propose to recast abuse in relation to intelligence services and surveillance along the lines of police abuse to expand the democratic field of accountability.[7]

Through zooming in on two historical moments of crisis and tension, we trace how "abuse" and "trust" are articulated by different actors and how they shape different practices of oversight and demands for accountability. The first moment of crisis concerns the revelations about an elected Member of Parliament (MP), Harriet Harman and a civil society member, Patricia Hewitt, having been unlawfully surveilled by the Security Service (MI5) in the 1980s. The second moment of crisis is that of the 2013 Snowden disclosures, when mass surveillance by the GCHQ and other intelligence agencies in the UK and the US, amongst others, led to public mobilisation about the activities of the intelligence agencies. By juxtaposing these two moments, we can map the changing

relations between abuse and trust for oversight and accountability of intelligence agencies. To unpack the discourses of abuse and trust, we have drawn on a varied range of material, which included parliamentary debates and inquiries, litigation before the European Commission of Human Rights and subsequently the European Court of Human Rights, oral history interviews with MPs, oversight professionals and members of civil society, media coverage of these scandals, reports and memoirs by participants and observers at the time.

Intelligence oversight, abuse, and trust

A paradox exists at the heart of intelligence oversight and control. On the one hand, the history of intelligence scandals shows that legislative and democratic control of intelligence agencies has largely only resulted from public controversies or scandals, which have raised public concern over "abuse of power". As Peter Gill acknowledges in the case of the UK, the activities of the intelligence agencies have led to "allegations of abuse of power".[8] For Gill, these criticisms of abuse were not part of a wider critique of state power, but specifically focused on the effects that unlawful and improper actions by the intelligence agencies had on their effectiveness and on democratic values:

> First, there is the question of effectiveness of the security intelligence process and to the extent to which the secrecy within which it is shrouded is maintained mainly to prevent revelations of the sheer bureaucratic ineptitude to which the process is prone; and, second, the extent to which the lack of democracy control of the process has led to systematic abuse of power by the state.[9]

On the other hand, both the activities of intelligence agencies and their oversight are formulated in terms of trust rather than abuse of power. How are we to understand the relation between "abuse" and "trust"?

A fair amount has been written about the supposed relationships of "trust" necessary for effective intelligence cooperation and collaboration.[10] Personal and social relationships are said to be key in creating the conditions for trustworthiness, enabling efficient cooperation despite uncertainties and vulnerabilities of transnational relations.[11] As intelligence practitioner and scholar David Omand puts it, trustworthiness is "the most valuable attribute of any successful [intelligence] partnership".[12]

What is perhaps more surprising is that the literature on the democratic oversight of intelligence agencies also invokes this idea of trust, albeit in relation to intelligence agencies' overseers. Largely, though not always, grounded in the same state-centric, functionalist, and policy-oriented epistemologies as the literature on intelligence, this scholarship often works with the assumption that effective oversight depends on a type of deliberative politics, which is buttressed by mutual trust between all the actors involved:

intelligence agencies, overseers, and the general public.[13] This trust is, however, personalised, dependent on the individuals who make up these institutions. They need to be impartial and non-conflictual (the two often overlap in the demand for oversight to be non-political).

Therefore, one of the main points of agreement amongst oversight scholars is that the most effective form of control of intelligence is depoliticised, thus free from contestation and dispute. Peter Gill has traced the idea of the desirability of de-politicised oversight back to the era of the birth of parliamentary oversight in the 1960s and 1970s.[14] Here, an inherent fear by intelligence actors of legislatures leaking information and instrumentalising secret material for political grandstanding is said to be the crucial factor in ensuring that all oversight is free from partisanship. Even though there has never been an intelligence leak from a parliamentarian in the history of intelligence oversight, this normative bias towards confidence and consensus is reproduced throughout the oversight literature, extending to technical bodies and civil society.[15] If scrutiny by other actors is envisaged, this only comes at a later stage than more official forms of oversight such as parliamentary oversight, judicial review, and internal control acting as a "fire alarm" as opposed to a "police patrol" to intelligence practices.[16] Oversight can thus be seen as democratic through pluralising actors and interests without conflict.

For example, in their first annual report, the Intelligence and Security Committee of the UK Parliament (ISC) noted that "The key to making this oversight work lies in establishing mutual respect and confidence between ourselves and the agencies".[17] If these relations of trust work, then the Committee can also "command the confidence of Parliament and the public".[18] The memoirs of the first ISC chairperson, Tom King, reveal some of the parliamentarians' initial struggles to gain the trust of the agencies.[19] Establishing oversight was a struggle to convince the heads of agencies to trust parliamentarians, whom they considered unreliable and liable to leak secrets for political gain. For Tom King, this required selecting the correct people, often long-serving and senior parliamentarians who were deemed to be serious and responsible.[20]

Interestingly, an area in which discourses of trust were *not* mobilised in these early days was around the oversight of intelligence budgets and the involvement of the public audit office. The oversight of the agencies' spending was deemed much less contentious than oversight of the practices of the agencies. One MP involved with the establishment of the ISC was categorical in articulating the importance of making the agencies financially accountable in the (then, quite limited) remit of the committee. Commenting on the huge overspend of GCHQ in their relocation of headquarters to Cheltenham, this MP was far from invoking discourses of "trust", when they maintained that budgets of the agencies needed to be strictly controlled: "This [senior GCHQ] person should not have been put in charge of this project. He's probably very good at code breaking, but this doesn't make him an ideal man to be put in charge of a multi-million-pound project".[21]

What is interesting is that some 25 years after its establishment, members of the ISC are still aware of, and articulate this fundamental power imbalance. In more recent decades, a member of the ISC spoke about the need to create a space of "trust" between parliamentary overseers and the agency staff, so that intelligence practitioners would feel comfortable in airing any problems. In this conception of oversight, "trust" also acts as a sort of understanding on the part of overseers, acknowledging the huge responsibility that the agencies are under in protecting national security.[22] Thus, even when maladministration or another form of abuse is found, the framing of "trust" ultimately forecloses more antagonistic practices of holding to account and control. Moreover, such antagonistic practices lack institutional materialisation within existing oversight structures.

The US literature on intelligence oversight is even more forceful in this regard, with intelligence studies scholar Loch K. Johnson linking the 1990s, what he calls the "partisan era", with weaker congressional control over the agencies.[23] Jennifer Kibbe strengthens this line of argument by claiming that intelligence officials are much less likely to provide information to congressional overseers if they doubt their motivations, stating that overseers who are moderate, responsible, and dedicated to non-partisanship are the only ones who could win the trust of the agencies.[24] In the European context, Ian Leigh has also made a strong argument for non-partisan oversight as inherently more trustworthy, linking parliamentary scrutiny with the possibility of an immature approach which could pave the way for sensationalism and the airing of conspiracy theories.[25] Tracing the institutionalisation of oversight in the US throughout the 1960s and 1970s, Félix Tréguer has carefully unpacked the narrative that the agencies have been increasingly subject to greater democratic control, by showing how the inclusion of congressional and semi-juridical overseers into the "ring of secrecy" served to unsettle the boundary between the agencies and their critics, preventing them from formulating more radical critiques.[26]

In these discussions, trust is often also linked to transparency and secrecy. In a project on the decline of state secrecy, Richard Aldrich and Christopher Moran argue that these disclosures are in fact evidence of a decline of state secrecy, with intelligence operatives now operating much more carefully, keeping in mind how certain practices will appear if they are leaked on Twitter ten minutes later.[27] Unlinking greater transparency from democratic accountability, they point out how the agencies themselves are moving away from a focus on information control towards a proactive strategy of public relations, designed to inculcate trustworthiness and public approval. Yet, it remains unclear how revelations change or not the actions of intelligence agencies beyond strategies of public communications, and how these revelations can transform "doing" and not just "being".

Moreover, situating trust in relation to the opposition transparency/secrecy overlooks the ways in which trust requires both knowledge and non-knowledge. As philosopher Byung-Chul Han explains, "It [trust] makes actions possible despite one's lack of knowledge. If I know everything in

advance, there is no need for trust".[28] Thus, trust is not contradictory to secrecy and non-knowing, but it accommodates degrees of secrecy and ignorance. Oversight committees can ask intelligence agencies for some information, but only in circumscribed situations. In that sense, we can see trust not just as an economiser of power, but also an economiser of knowledge. Building oversight on relations of trust means that oversight agents are not supposed to know too much. At the same time, as Didier Bigo has explained, they acquire knowledge by entering the structural space of secrecy. To gain the right of entry into the so-called "ring of secrecy", they are obliged to "differentiat[e] themselves from other actors as the legitimate owners of secrecy".[29] Similar to data sharing between agencies, the entry into this shared social space of secrecy was "the result of the structural positions of the different services regarding each other and not just a relation of 'trust' between them".[30] "Trust", however, is used to obfuscate and obscure these relationships of power and differences in structural positions; a displacement which continues to the present day. Moreover, "trust" continues to obfuscate the limits to the knowledge that oversight committees can acquire. Becoming part of the "ring of secrecy" does not mean that they have access to the same information or that they can even request it.

Whilst the literature within intelligence studies then can be seen to have taken "trust" somewhat for granted, recent literature from within critical security studies and surveillance studies has taken a more sociological approach, problematising the role of "trust" in relation to democratic scrutiny and accountability of surveillance practices. Vis-à-vis calls for greater transparency, Fredrika Björklund points to the counterintuitive finding that sees populations who report high levels of trust in public institutions as in fact more accepting of surveillance, contrary to the much of the surveillance studies scholarship that argues that surveillance erodes trust within societies.[31] For these authors, the supposed virtues of trust and transparency as policy goals have in fact obscured more multifaceted and sometimes conflicting dynamics at play in contesting surveillance, running the risk of promoting not only simplistic but perhaps also counterproductive proposals for remedying the human rights implications of surveillance.[32]

Unlike trust, "abuse of power" has received much less attention in political science and international relations, even if the term circulates widely. It has been used in relation to unlawful actions by governments and intelligence agencies, corruption, or otherwise improper use of power. A common thread around abuse is that it emerges within hierarchical power relations. As feminist sociologist Vikki Bell has pointed out, it is how "the perpetual asymmetry of power is upheld" that makes abuse possible.[33] In that sense, abuse has come to name forms of violence where such hierarchical relations are at play: domestic abuse, child abuse, and sexual abuse. Yet, abuse of power with reference to governments and institutions has dwindled from public imaginaries and even civil society activism and litigation. A recent contribution on police abuse and democracy reformulates abuse beyond the

correlation with lawfulness: "we define police abuse as police actions that may or may not be 'illegal' but severely limit selective citizens' rights, receive minimal punishment (limited accountability), and may play a role in maintaining (or promoting) particular political and economic objectives".[34] While this broader understanding of abuse is not at work in the surveillance scandals we explore, it helps us trace the analytical significance of "abuse" in relation to "trust". As Charlotte Heath-Kelly has remarked in the different context of psychiatric scandals, abuse was associated with systematicity rather than individualised malpractice or misconduct.[35] As we will see in the cases of surveillance scandals, abuse continues to be connected to systematicity rather than individualised mistakes or errors to be corrected.

Coming back to this paradox which discursively links abuse by intelligence agencies with (mis)trust of these agencies, we take up these authors' call to see trust and abuse in a more political-sociological light. We propose to situate both trust and abuse sociologically and historically by juxtaposing two moments of crisis and scandal within intelligence oversight, one which led to problematisations of abuse, improper action, and destruction of democratic values in the 1980s and the other, in the wake of the Snowden disclosures, which was articulated in terms of trust and mistrust. Through the methodological device of juxtaposition, we aim to flesh out not only how trust as a discourse and practice has structured the possibilities of scrutiny and accountability, but also how it has obfuscated debates about abuse of power by the intelligence agencies. The first moment of crisis is not an isolated one, but it is one that has led to most parliamentary and public debate and subsequent litigation given that evidence about unlawful surveillance of two former members of the National Council for Civil Liberties (NCCL, now Liberty) by MI5 was revealed by a whistleblower. The second moment of crisis comes in the wake of the disclosures by National Security Agency (NSA) whistleblower Edward Snowden of routine collection and transnational sharing of citizens' data, which coincided with the overhauling of surveillance legislation in the UK context.

Problematising abuse: Hewitt and Harman v the UK

In 1985, Harriet Harman and Patricia Hewitt filed a case before the European Commission of Human Rights (now European Court of Human Rights), accusing the UK of having subjected them to secret surveillance by the Security Service. At the time of the application, Hewitt was General Secretary of the NCCL and Harman was a Labour Member of Parliament. Previously, Harman had been legal officer of the NCCL. A former MI5 intelligence officer, Cathy Massiter, revealed in a TV broadcast that both Hewitt and Harman had been placed under surveillance by MI5 as "communist sympathisers" and "subversives".[36]

The Commission found that the interference with the applicants' right to private life was not "in accordance to the law",[37] as there was no legislation

that would have ensured the foreseeability of surveillance and guarded against arbitrariness. By extension, given the finding of a breach of Article 8 on the right to privacy and lack of effective remedy, the Commission Report did not examine the violation of the right to freedom of expression (Article 10) and the right to freedom of association (Article 11). The Commission report was formulated in the language of violations of rights and breach of the European Convention on Human Rights. The government's arguments rely on secrecy and the stance of "neither confirm nor deny". The government also continued to argue that the applicants "have not substantiated their complaints".[38]

Although the case ushered in many of the oversight changes in the UK, it is often bypassed in the intelligence studies literature. The *Historical Dictionary of British Intelligence* has only an entry on Cathy Massiter, but none on the victims of abuse across history. Massiter's role is described in dismissive terms as a "controversial and unprecedented "intervention" which derailed the government's lawyers, "who otherwise would have prevailed".[39] This is exactly the opposite of how the case was covered in the media at the time and the debates it led to. As a media article explained Cathy Massiter's actions at the time, "An intelligence officer for 13 years, she spoke out recently because she could no longer be part of the phone-tapping abuses of MI5 which were in contravention of its own charter".[40] Mark Hollingsworth and Richard Norton-Taylor argued that the targeting of trade union and NCCL leaders was made possible by the ambiguity of subversion and who therefore was deemed to count as a subversive: "The current definition of a subversive is now so vague that it is dangerously open to abuse".[41] Scholars who have assessed the lawfulness of MI5 in terms of establishment and function have highlighted the problems arising from "the secrecy of its mandate, the secrecy and arbitrariness of its powers, and the open violation of the law".[42] Moreover, the history of MI5 actions, which had come to the public eye during the Cold War, was one of abuse and unlawful surveillance of trade unionists, striking miners, civil society actors, or left-wing writers.[43]

The report by the European Commission on Human Rights on the Hewitt's and Harman's application also highlights the arbitrariness of surveillance:

> In order to open a file on Harriet Harman the Security Service would have to find a category in which to place her. She was clearly not a member of the Communist Party of Great Britain. However, she was legal officer for NCCL which had been assessed as a subversive organisation. The only category open in which to record her was "Communist sympathiser". Although she was not a member of the Communist Party and there was not evidence that she was sympathetic to the Communist Party, bureaucratically this was the only appropriate category in which she could be placed.[44]

The Commission also noted that the allegations and Massiter's revelations were "neither confirmed nor denied" by the UK government.

Media coverage of the Channel 4 20/20 Vision programme in which Massiter made the revelations of unlawful surveillance by MI5 formulated public concerns in terms of abuse by the intelligence agencies.[45] The programme was initially banned by the Independent Broadcasting Authority (IBA). In 1993, *The Guardian* reported the start of a campaign to "shine light on state abuses" and "encourage 'ordinary people' to challenge secrecy, surveillance and vetting".[46]

In the House of Commons, debates about the Harman and Hewitt case also raised questions about abuses of power by the security and intelligence agencies. Similar concerns about the ambiguity and expansiveness of national security were voiced. While the Security Services Act states the political neutrality of the security services, the definition of national security is so broad as to include "actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means".[47] MP Stuart Randall pointed out the abuse of powers by MI5:

> What Cathy Massiter had to say showed unequivocally that there was an abuse of civil liberties. Such abuse has resulted in a loss of confidence in the service, and that is not good for our nation, our national security or our democracy.[48]

Randall continues his scathing critique of the Bill on grounds of vagueness and imprecision:

> The Bill is a great disappointment. It is vague, it is imprecise, and it will have little effect on the way in which the Security Service operates. The Bill fails to provide adequate safeguards against abuse and illegal activity by MI5. It contains no measures to improve the service's efficiency and effectiveness. Of special importance is the fact that the Bill includes little to enhance the civil liberties and genuine freedoms of the people of Britain.[49]

Avoiding abuse would require more precise language and safeguards alongside civil liberties and freedom. Thus, oversight cannot be the only measure to prevent or respond to abuse, but it needs to be supplemented by strong civil liberties. In 1993, in debating the Security Service and the need for oversight, Labour MP David Winnick pointed out that

> Parliamentary scrutiny in itself will not prevent abuses. No one has suggested anything of the sort. If MI5 was subject to some accountability other than simply to the Home Secretary, the tribunal and the commissioner, there would at least be the feeling that their activities would need to be justified.[50]

Interestingly, at the time of statutory legislation for the intelligence and security services, there were voices among MPs that did not believe that abuse

could be prevented, but that forms of justification through oversight might reduce it. By contrast, the Under-Secretary of State for the Home Department sees the Security Service Act of 1989 as having "provided for safeguards against any abuse, whether by members of the service or by Ministers".[51]

In a Memorandum to the Select Committee on Home Affairs Committee, David Bickford, former legal director of MI5 and MI6, explains the tensions between the Security Service and the government concerning secrecy:

> On the one hand the Security Service saw the benefits of more opennes [sic] and of using intelligence for the first time to convict terrorists and to aid the police in the future fight against organised crime. On the other, the Home Office and Whitehall were fearful that the consequent reduction in secrecy surrounding the Service would lead to an erosion of longheld principles of secrecy surrounding government business as a whole.[52]

Bickford argues that it was the Harman and Hewitt case before the European Commission for Human Rights that spurred the government into legislative action:

> The 1989 Security Services Act oversight was secured only in the face of the certainty of losing the ECHR Hewitt and Harman case. The absolute minimum of oversight was given. It was gauged just sufficient to satisfy the European Commission, which would be unwilling to reject a state's legislation introduced to satisfy a complaint unless it was absolutely necessary to do so.[53]

The language of "abuse of power" and human rights violations exposes surveillance and other intelligence practices to the dynamics of justification and critique. It makes the targets of surveillance into subjects who can demand redress and make rights claims.[54] It opens a scene of dispute over the operations of power that are at stake. However, there are also limitations to how abuse has been understood. Firstly, abuse of power seems to indicate that there is a non-violent and lawful "use of power". Secondly, abuse of power has been formulated in relation to existing laws, what is "in accordance to the law" and what is not. Therefore, abuse emerging out of structural inequalities and stabilised hierarchies of power remains difficult to articulate.

Despite these limitations, the denunciation of "abuse of power" brings questions about the actions of intelligence service to the public. It also problematises the powers that these services hold and the secrecy that they invoke to shield their actions from accountability. Denunciations of abuse highlight the central role that whistleblowers, media, and civil society organisations played in holding intelligence services accountable. Finally, abuse makes it possible to attend to the experience of those who are targeted by surveillance. It gives them a language in which to formulate rights claims. In

the next section, we turn to a more recent controversy about mass surveillance by the intelligence agencies.

Invoking trust: The post-Snowden landscape and UK surveillance legislative struggle

The summer of 2013 famously saw the disclosures of mass surveillance of populations from NSA whistleblower Edward Snowden. The disclosures were immediately reframed as arousing a "crisis of trust" between citizens and the intelligence agencies. Deputy Prime Minister at the time, Nick Clegg, argued that the lack of accountability for these practices could "corrode trust", a sentiment echoed by the Independent Reviewer of Terrorist legislation, David Anderson, who labelled his investigation into bulk powers "A Question of Trust".[55] Around the same time, the UK was also witnessing legislative struggles around these so-called "investigatory powers". So, how can we conceptualise discourses of trust during this time? Abuse only appears in the European Court of Human Rights judgement in the case of *Big Brother Watch et al. v the UK*, which challenged the mass surveillance regime in the UK. The Court concluded that,

> while there is no evidence to suggest that the intelligence agencies are abusing their power - on the contrary, the Interception of Communications Commissioner observed that the selection procedure was carefully and conscientiously observed by analysts … , the Court is not persuaded that the safeguards governing the selection of bearers for interception and the selection of intercepted material for examination are sufficiently robust to provide adequate guarantees against abuse.[56]

In the wake of the Snowden disclosures, the House of Commons in the UK held a debate and addressed a statement by the then Foreign Secretary, William Hague. One of the Labour MPs, Paul Flynn, reminds the House of the 1980s and Cathy Massiter:

> The Cathy Massiter case proved that, 50 years after the last war, intensive surveillance of peace activists, trade unionists and left-wing parties had failed to turn up a single spy, but it was discovered that in that same period, more than 20 members of the Secret Intelligence Service were spying for the Soviet Union. Since then, we have had untruths on weapons of mass destruction and a Government cover-up to this House on the handing over of prisoners to oppressive regimes to be tortured. Is the Foreign Secretary telling us today that the only people now under surveillance are the guilty? How does he manage that?[57]

Hague responded by highlighting that the UK has developed a "strong legal framework" to govern the activities of intelligence agencies alongside oversight

mechanisms. So unlawfulness is of the past and can have no place in the present. It is therefore not surprising that "abuse" is not mentioned in this debate. At this point, neither is "trust". However, we suggest that a discourse of trust comes to occupy the terrain of dispute over abuses of power.

In the few occasions that the term "trust" was mobilised in Parliament in relation to the intelligence agencies, it was to reinforce a binary framing of either being for or against the services: "The choice is clear: do we trust our skilled professionals, or do we further disable them and let the terrorists and those who seek to destroy our society wreak havoc in this world?".[58] What is invoked here is an idea of personal trust, trust that is built based on past experience and anticipation of future action. This is the trust that emerges out of familiarity. In relation to the foreclosure and structuring of debate around the new legislation, "trust" discourse was thus seen much more in relation to the supposed trustworthiness of external experts and civil society actors, related to their perceived independence, motivation, and capacity to engage in "serious" discussions about legislating for bulk surveillance.

The first effect of this invocation of trust was to foreclose debate. As with the discussions around the formation of the Intelligence Security Committee in Parliament in the 1990s, we once again see "trust" mobilised to structure the cost of entry into the field of oversight and to demarcate what was rendered as serious debate around mass surveillance. Here, certain frames of questioning were de-legitimised by being assumed to come from actors who were not sufficiently trustworthy. Unlike in the 1990s, when many accusations of (dis)trustful premises for action or ulterior motives were levelled at MPs, this period saw a greater consensus in Parliament for the importance of the work of the intelligence agencies and fewer possibilities for political grandstanding.[59]

The implementation of a post-Snowden emergency, stop-gap legislation aimed at allowing the security services to retain the powers of data collection that they had been using – the so-called Data Retention and Investigatory Powers Act 2014 (DRIPA) – saw David Anderson QC appointed to conduct the review of investigatory powers. For some civil society actors, the appointment of Anderson was testimony to the foreclosure of some types of debate:

> The role of David Anderson was to get someone who is trusted to come up with things that are going to be accepted. And he did a good job because he had to come up with things that were going to be accepted. But that still shows the power the security services were still wielding. They were the ones that defined the parameters of what was going to be acceptable.[60]

Anderson himself acknowledges these constraints in his written reflections on his role after the Snowden disclosures, "A common feature of those

reviews is that they were commissioned as a way out of political conflict".[61] Within this report, Anderson explicitly links (hypothetical) abuse with mistrust, framing not the mass surveillance per se, but the possibility of abuse of this data as a reason for possible mistrust:

> [Bulk powers] involve potential access by the state to the data of large numbers of people whom there is not the slightest reason to suspect of threatening national security or engaging in serious crime […] any abuse of those powers could thus have particularly wide ranging effects on the innocent […] even the perception that abuse is possible, and that it could go undetected, can generate corrosive mistrust.[62]

However, the question of abuse is pre-emptively eliminated by the invocation of lawfulness and the personalisation of trust through the familiarity of trustworthy individuals who either work for the agencies or hold the role of overseers.

Parliamentarians also took care to formulate their interventions into debates around these legislative struggles in language that did not connect them to any "lobby groups", which would de-legitimise their arguments.[63] This was the case in reports of the Intelligence Security Committee, the so-called official overseers, but also the case with MPs involved in debates around the Investigatory Powers Bill. Parliamentarians across all parties trying to limit these data collection and retention powers spoke about appearing more trustworthy and reputable to fellow parliamentarians if they spoke from a position of being attuned to the needs of the security services rather than presenting arguments put forward by civil society.

While these dynamics of foreclosure were visible to the NGOs involved in these debates, the structural consensus around conceiving of the intelligence agencies as working for the "common good", which necessitated use of "bulk powers", allowed very little room for manoeuvre. One of our interlocutors explained: "I think that in that sense, by us tagging along with [the framing of the debate on investigatory powers] we all basically became part of the same dynamic; the idea that [both civil society] and the security agencies okayed this".[64]

After the passing into law of the Investigatory Powers Act, the debate on bulk data collection and retention became effectively "closed". As one external expert noted at the time, "My reading of the IP Bill is that it will result in, and perhaps intends, closing for ever the democratic debate about what constitutes acceptable state surveillance".[65] With the debate about the content of the bill effectively closed, discourses of trust became centred around structures of safeguarding and oversight of the bulk powers, rather than challenging the content of these powers in any meaningful way.

Another shift enabled by trust is that the actions of intelligence agencies are rendered in the register of "error" rather than "abuse". Dominic Grieve,

former Chair of the ISC, shifts from the problematisation of misuse to that of mistakes in the House of Commons:

> Assurances are therefore needed that the extensive powers and capabilities that they undoubtedly have are taken on trust in so far as any potential for misuse is concerned. That is why the Intelligence and Security Committee was set up and the various commissioners appointed. It is noteworthy that, apart from a few exceptions based on mistake rather than on malicious intent, all those bodies have consistently given the investigatory powers used by the agencies a clean bill of health.[66]

The very existence of overseers becomes an indicator and guarantee of trust. Therefore, any disclosures by whistleblowers become read as mistakes or errors. Errors are contingent and the result of epistemic limitations so that they can be corrected. Indeed, with the 2016 Investigatory Powers Act, and despite these declarations of defeat from within UK civil society, the UK was lauded by some observers as having adopted an exemplary approach to intelligence oversight.[67] In justifying her support for the Investigatory Powers Bill, one Conservative MP emphasises trust: "Trust is the golden thread running through the viability of the new legislation. Some things necessarily need to remain secret, but notwithstanding that need for secrecy, the public's trust, a sound legal basis and opportunity for impartial challenge are important for ensuring long-term robustness".[68]

Following this legislation, all signals intelligence is overseen by one independent national agency, the Investigatory Powers Commissioner's Office (IPCO), which was brought into being to replace a patchwork of commissioners which were set out in various piecemeal previous legislations. As IPCO oversees the use of investigatory powers, and not the practices of intelligence agencies per se, they are thus responsible for overseeing more than 600 public bodies, which in addition to the intelligence agencies, comprise also of police and law enforcement agencies, local authorities, prisons, warrant granting departments, and others.[69]

In coming back to what the language of "trust" permits and what it makes unacceptable, what is interesting in the relations between the newly minted oversight body, IPCO, and the agencies it oversees is precisely the consensual and harmonious frames that are invoked from the outset of its conception. In this vein, IPCO uses the discourse of compliance and scalability to speak about their approach to oversight. Within this framework, external oversight forms a consistent and commensurable "addition" to the internal compliance checks already being carried out within the agency. The role of independent oversight is therefore much more procedural and already aligned with the common goal of following legal standards. Compliance teams within the agencies are the first point of contact for IPCO inspectors, with the compliance team organising the logistics of the inspection.[70] As a former oversight

professional explains, trust is integral to their interactions with the intelligence agencies:

> We took the strong view and I'm sure the commissioner would say, you know, we trusted the compliance teams. You know, they didn't ever do anything to call into question their integrity and integrity as a core value for public servants.[71]

In this way, IPCO defines its oversight function in relation to the agencies as one of mutual cross-fertilisation and enrichment for a common purpose, underpinned by trust and understanding. A former commissioner described how inspections of agencies would play out in day-to-day practice:

> You wouldn't go in and say, I'm here to test stuff. You would just go and watch an operation. And you might spend a couple of days following someone around or just seeing what's going on. And that would give the idea was that would give the inspectors a bit more knowledge of how the institution works or that you wouldn't otherwise you probably wouldn't see any failings ever in practice.[72]

Inspections are said to take place in an "open" and "constructive" atmosphere, with some of the most fruitful inspections being where an intelligence officer, in narrating how a particular practice plays out, themselves exercise reflexivity, and self-assessment within this encounter. Oversight translates in this regard as inspiring a sort of awakening or epiphany amongst intelligence officers; encouraging them to come around to normalising compliance and the possibility to use less intrusive measures.

Thus, trust shapes relations between agencies and publics, oversight institutions and publics as well as oversight institutions and the agencies themselves. Yet, this expansion of trust to all relations means that inquiries into abusive practices become unthinkable. At best, oversight can produce a catalogue of errors to be corrected.

Conclusion: Abuse, trust, and democracy

This chapter has traced a shift from denunciations of abuse by intelligence agencies towards the invocation of trust – with the equivalent bemoaning of distrust – in the UK. By taking two historical moments when surveillance by intelligence agencies has come to public knowledge through the actions of whistleblowers, we have shown how abuse and trust enact different relations between publics, civil society actors, oversight institutions, and intelligence agencies.

By juxtaposing these historical moments of crisis and scandal in terms of oversight of intelligence agencies in the UK, we could see the work that "trust" discourses did in immediately foreclosing debate, rendering some forms of

oversight actionable and others not. Domains of oversight which remained outside of "trust" discourses, such as auditing of intelligence budgets, were much more amenable to meaningful scrutiny and contestation. We have also shown how "trust" displaces further contestation, immediately delimiting what counts as "serious" engagement with the intelligence agencies to "trustworthy" individuals. This shift towards the language of trust enacts intelligence agencies as personalised trustworthy individuals who interact with other personalised trustworthy individuals (MPs or other overseers). Moreover, trust as an economiser of power and knowledge means that limited questions are asked about the actions of intelligence agencies, their "doing" and limited knowledge is expected. Thus, debates about trust are formulated in terms of secrecy and transparency.

Unlike trust, abuse highlighted questions of the misuse of power given stabilised hierarchies where those affected by intelligence actions have little or any levers on these power relations. However, the discourse of abuse was also limited by the framing of "unlawfulness", so that other actions that might be experienced as abuse by citizens and non-citizens were neither thinkable nor acceptable as part of the debate. Framing "trust" and "abuse" through a political-sociological lens reveals the many ways in which "trust" framings, perhaps counterintuitively, facilitate impunity and allow the evasion of scrutiny and accountability. Far from a virtuous policy goal, "increasing trust" in intelligence agencies should be viewed with caution in terms of human rights and democratic principles.

Unlike trust, we have seen that discourses of abuse underpin a different mode of democratic oversight; one that enables a more profound mode of challenge of human rights violations. However, from parliamentary and public debates, "abuse" has been relegated to the legal sphere, while "trust" has become an increasingly discursive currency of all interactions with intelligence agencies. The reformulation of police abuse to encompass the perspectives of those affected by intelligence actions and their experience of abusive practices can offer a different sociological lens upon oversight and accountability.

Notes

1 David Anderson, "Shades of Independent Review," 2017, accessed 13 January 2020, https://www.daqc.co.uk/2017/12/06/shades-independent-review/.
2 Ibid.: 12.
3 Mark E Warren, ed., *Democracy and Trust* (Cambridge: Cambridge University Press, 2010).
4 Russell Hardin, "Do we want trust in government," in *Democracy and Trust*, ed. Mark E Warren (Cambridge: Cambridge University Press, 1999).
5 Pierre Rosanvallon, *Counter-Democracy: Politics in an Age of Distrust* (Cambridge: Cambridge University Press, 2008), 22.
6 Claus Offe, "Can we trust our fellow citizens?," in *Democracy and Trust*, ed. Mark E Warren (Cambridge: Cambridge University Press, 2010).
7 Michelle D Bonner et al., eds., *Police Abuse in Contemporary Democracies* (Basingstoke: Palgrave Macmillan, 2018).

8 Peter Gill, *Policing Politics: Security Intelligence and the Liberal Democratic State*, 1st edition ed. (London: Routledge, 1994).
9 Ibid.: 22.
10 for an overview of the literature, see Pepijn Tuinier, Thijs Brocades Zaalberg, and Sebastiaan Rietjens, "The Social Ties that Bind: Unraveling the Role of Trust in International Intelligence Cooperation," *International Journal of Intelligence and CounterIntelligence*, https://doi.org/10.1080/08850607.2022.2079161.
11 Ibid.
12 David Omand and Mark Phythian, *Principled Spying: The ethics of secret intelligence* (Oxford University Press, 2018).
13 Zachary K Goldman and Samuel James Rascoff, "Introduction. The new intelligence oversight," in *Global intelligence oversight: governing security in the twenty-first century*, ed. Zachary K Goldman and Samuel James Rascoff (Oxford: Oxford University Press, 2016). For an elaboration of this critique, see Hager Ben Jaffel et al., "Collective Discussion: Toward Critical Approaches to Intelligence as a Social Phenomenon," *International Political Sociology* 14, no. 3, https://doi.org/10.1093/ips/olaa015.
14 Peter Gill, "Evaluating intelligence oversight committees: The UK intelligence and security committee and the 'war on terror'," *Intelligence and National Security* 22, no. 1.
15 For an analysis, see Bernardino Leon-Reyes, "Towards a Reflexive Study of Intelligence Accountability," in *Problematising Intelligence Studies*, ed. Hager Ben Jaffel and Sebastian Larsson (London: Routledge, 2022).
16 Hans Born, "Parliamentary and external oversight of intelligence services," in *Democratic Control of Intelligence Services*, ed. Marina Caparini and Hans Born (London: Routledge, 2016); Mathew D McCubbins and Thomas Schwartz, "Congressional oversight overlooked: Police patrols versus fire alarms," *American Journal of Political Science*; Steven J Balla and Christopher J Deering, "Police patrols and fire alarms: An empirical examination of the legislative preference for oversight," *Congress & the Presidency* 40, no. 1.
17 IPCO, "Annual Report 1995," 1996, accessed 14 October 2022, https://isc.independent.gov.uk/wp-content/uploads/2021/01/1995_ISC_AR.pdf.
18 Ibid.: 11.
19 Tom King, *A King Among Ministers: Fifty Years in Parliament Recalled* (Lewes: Unicorn, 2020).
20 Ibid.
21 Interview with former MP, 26/05/2021.
22 Interview with former MP, 27/10/2020.
23 Loch K. Johnson, "A shock theory of congressional accountability for intelligence," in *Handbook of Intelligence studies*, ed. Loch K. Johnson (London: Routledge, 2007).
24 Jennifer Kibbe, "Congressional Oversight of Intelligence: Is the Solution Part of the Problem?," *Intelligence and National Security* 25, no. 1, https://doi.org/10.1080/02684521003588104. See also Marvin C. Ott, "Partisanship and the Decline of Intelligence Oversight," *International Journal of Intelligence and CounterIntelligence* 16, no. 1, https://doi.org/10.1080/713830378.
25 Ian Leigh, "Rebalancing Rights and National Security: Reforming UK Intelligence Oversight a Decade after 9/11," *Intelligence and National Security* 27, no. 5, https://doi.org/10.1080/02684527.2012.708525.
26 See Tréguer's chapter in this volume.
27 Richard J Aldrich and Christopher R Moran, "'Delayed Disclosure': National Security, Whistle-Blowers and the Nature of Secrecy," *Political Studies* 67, no. 2, https://doi.org/10.1177/0032321718764990.

28 Byung-Chul Han, *The Transparency Society*, trans. Erik Butler (Stanford, CA: Stanford University Press, 2015), 47.
29 Didier Bigo, "Shared secrecy in a digital age and a transnational world," *Intelligence and National Security* 34, no. 3: 391, https://doi.org/10.1080/02684527.2019.1553703.
30 Ibid.: 385.
31 Fredrika Björklund, "Trust and surveillance: An odd couple or a perfect pair?," in *Trust and Transparency in an Age of Surveillance* (London: Routledge, 2021).
32 Ibid. On the implications of surveillance, see David Lyon, ed., *Surveillance as Social Sorting: Privacy, risk, and digital discrimination* (London: Routledge, 2003).
33 Vikki Bell, *Interrogating Incest: Feminism, Foucault, and the law* (London: Routledge, 1993).
34 Michelle D Bonner et al., "Introduction," in *Police Abuse in Contemporary Democracies*, ed. Michelle D Bonner et al. (Basingstoke: Palgrave Macmillan, 2018), 3–4.
35 Charlotte Heath-Kelly, "Cold War Psychiatry, Extremism, and Expertise: The "Special Committee on the Political Abuse of Psychiatry"," *International Political Sociology* 16, no. 1, https://doi.org/10.1093/ips/olab034.
36 European Commission on Human Rights, *Application No. 12175/86. Patricia Hope Hewitt and Harriet Harman against the United Kingdom* (1989), 15.
37 Ibid.: 41.
38 Ibid.: 15.
39 Nigel West, *Historical Dictionary of British Intelligence* (Lanham, MD: Scarecrow Press, 2014), 357.
40 P. Morgan, "The MI5 spy who had a conscience," *Courier-Mail* 1985, 11 May.
41 Mark Hollingsworth and Richard Norton-Taylor, "MI5: Building empires, ruining careers / A look at the long tentacles of the security service," *The Guardian Weekly* 1988, 6 September.
42 Keith Ewing, Joan Mahoney, and Andrew Moretta, *MI5, the Cold War, and the Rule of Law* (Oxford: Oxford University Press, 2020).
43 Ibid.; James Smith, *British Writers and MI5 Surveillance, 1930-1960* (New York: Cambridge University Press, 2012).
44 European Commission on Human Rights, *Application No. 12175/86. Patricia Hope Hewitt and Harriet Harman against the United Kingdom.*
45 The search was conducted in the Nexis database on 'Harman' and 'MI5' in the UK print media. The first coverage of the scandal was in *The Guardian* in 1985 and final mention in 1997, also in *The Guardian.*
46 Alan Travis and Richard Norton-Taylor, "Campaigners shine light on state abuses. Consortium launches drive to encourage 'ordinary people' to challenge secrecy surveillance and vetting," *The Guardian* 1993, 8 June.
47 "Security Services Act," 1989, accessed 7 November, 2022, https://www.legislation.gov.uk/ukpga/1989/5/contents.
48 "Security Services Bill," Hansard, 1988, accessed 23 August 2022, https://hansard.parliament.uk/Commons/1988-12-15/debates/d883cff5-8a7b-4f69-a85d-45e6767e5ffa/SecurityServiceBill?highlight=hewitt#contribution-96ac9194-69e7-4239-b0dd-83efe7cdb285.
49 Ibid.: Column 1173.
50 "Security Service," 1993, accessed 23 August 2022, 2022, https://hansard.parliament.uk/Commons/1993-03-29/debates/f51f0921-3199-496b-8d39-036655b9e209/SecurityService?highlight=hewitt#contribution-4ca1798d-f921-4756-83a3-5b0ba9813108.

51 Ibid.: Column 135.
52 Ibid.
53 Ibid.
54 Claudia Aradau and Emma Mc Cluskey, "Making digital surveillance unacceptable? Security, Democracy and the Political Sociology of Disputes," *International Political Sociology* 16, no. 1, https://doi.org/10.1093/ips/olab024.
55 David QC Anderson, *A Question of Trust. Report of the Investigatory Power Review* (London: Stationary Office, 2015).
56 "Case of Big Brother Watch and Others v. The United Kingdom (Applications nos. 58170/13, 62322/14 and 24960/15)," 2018, accessed 3 November, 2022, https://hudoc.echr.coe.int/.
57 Paul Flynn "GCHQ. Volume 564," Hansard, 2013, accessed 3 November 2022, https://hansard.parliament.uk/Commons/2013-06-10/debates/13061011000001/GCHQ.
58 Suella Fernandes "Investigatory Powers Bill. Volume 607," Hansard, 2016, accessed 7 November 2022, https://hansard.parliament.uk/commons/2016-03-15/debates/16031546000001/InvestigatoryPowersBill.
59 Interview with former MP, 27/10/2020.
60 Interview with civil society actor, 25/03/2020.
61 Anderson, "Shades of Independent Review."
62 Ibid.
63 Interview with former MP, 27/10/2020; interview with former MP 26/05/2021.
64 Interview with civil society actor, 25/03/2020.
65 George Danezis, "IP Draft Bill," 2016, accessed 5 June, 2023, https://conspicuouschatter.wordpress.com/2015/11/05/uk-draft-ip-bill-the-last-policy-discussion-about-surveillance-before-the-mass-gagging/.
66 Dominic Grieve "Investigatory Power Bill. Volume 611," 07 June 2016, 2016, accessed 1 August 2016, https://hansard.parliament.uk/Commons/2016-06-07/debates/16060732000001/InvestigatoryPowersBill?highlight=needle%20haystack#contribution-16060733000117.
67 Joe Cannataci cited in "Annual Report of the Investigatory Powers Commissioner 2017," 2019, accessed 3 March, 2020, https://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202017%20Web%20Accessible%20Version%2020190131.pdf.
68 Suella Fernandes "Investigatory Powers Bill. Volume 616," Hansard, 2016, accessed 7 November 2022, https://hansard.parliament.uk/Commons/2016-11-01/debates/79609F80-4ECA-4C9D-93D8-98AA35992EF8/InvestigatoryPowersBill?highlight=suella%20fernandes#contribution-FB21B325-99C1-40FB-B064-698D6C4F63E9.
69 Investigatory Powers Commissioner's Office, "Organisations we oversee," 2023, accessed 5 June, 2023, https://www.ipco.org.uk/what-we-do.
70 Interviews with former oversight professionals, 13/11/2019; 05/12/2020.
71 Interview, former oversight official, 13/11/2019.
72 Interview, former oversight professional, 13/11/2019.

References

Aldrich, Richard J., and Christopher R. Moran. "'Delayed Disclosure': National Security, Whistle-Blowers and the Nature of Secrecy." *Political Studies* 67, no. 2 (2019): 291–306. 10.1177/0032321718764990. https://journals.sagepub.com/doi/abs/10.1177/0032321718764990.

Anderson, David. *A Question of Trust. Report of the Investigatory Power Review*. London: Stationary Office, 2015.

"Annual Report 1995." 1996, accessed 14 October, 2022. https://isc.independent.gov.uk/wp-content/uploads/2021/01/1995_ISC_AR.pdf.

"Annual Report of the Investigatory Powers Commissioner 2017." 2019, accessed 3 March, 2020. https://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202017%20Web%20Accessible%20Version%2020190131.pdf.

Aradau, Claudia, and Emma Mc Cluskey. "Making Digital Surveillance Unacceptable? Security, Democracy and the Political Sociology of Disputes." *International Political Sociology* 16, no. 1 (2022): 1–19.

Balla, Steven J., and Christopher J. Deering. "Police Patrols and Fire Alarms: An Empirical Examination of the Legislative Preference for Oversight." *Congress & the Presidency* 40, no. 1 (2013): 27–40.

Bell, Vikki. *Interrogating Incest: Feminism, Foucault, and the Law*. London: Routledge, 1993.

Ben Jaffel, Hager, Alvina Hoffmann, Oliver Kearns, and Sebastian Larsson. "Collective Discussion: Toward Critical Approaches to Intelligence as a Social Phenomenon." *International Political Sociology* 14, no. 3 (2020): 323–344. https://doi.org/10.1093/ips/olaa015.

Bigo, Didier. "Shared Secrecy in a Digital Age and a Transnational World." *Intelligence and National Security* 34, no. 3 (2019/04/16 2019): 379–394. https://doi.org/10.1080/02684527.2019.1553703.

Björklund, Fredrika. "Trust and Surveillance: An Odd Couple or a Perfect Pair?" In *Trust and Transparency in an Age of Surveillance*, 183–200. London: Routledge, 2021.

Bonner, Michelle D., Michael Kempa, Mary Rose Kubal, and Guillermina Seri. "Introduction." In *Police Abuse in Contemporary Democracies*, edited by Michelle D Bonner, Guillermina Seri, Mary Rose Kubal and Michael Kempa, 1–30. Basingstoke: Palgrave Macmillan, 2018.

Bonner, Michelle D., Guillermina Seri, Mary Rose Kubal, and Michael Kempa, eds. *Police Abuse in Contemporary Democracies*. Basingstoke: Palgrave Macmillan, 2018.

Born, Hans. "Parliamentary and External Oversight of Intelligence Services." In*Democratic Control of Intelligence Services*, edited by Marina Caparini and Hans Born, 185–198. London: Routledge, 2016.

"Case of Big Brother Watch and Others V. The United Kingdom (Applications Nos. 58170/13, 62322/14 and 24960/15)." 2018, accessed 3 November, 2022. https://hudoc.echr.coe.int/.

European Commission on Human Rights. *Application No. 12175/86. Patricia Hope Hewitt and Hariett Harman against the United Kingdom*. 1989.

Ewing, Keith, Joan Mahoney, and Andrew Moretta. *Mi5, the Cold War, and the Rule of Law*. Oxford: Oxford University Press, 2020.

"GCHQ. Volume 564." Hansard, 2013, accessed 3 November 2022. https://hansard.parliament.uk/Commons/2013-06-10/debates/13061011000001/GCHQ.

Gill, Peter. *Policing Politics: Security Intelligence and the Liberal Democratic State*, 1st edition ed. London: Routledge, 1994.

Gill, Peter. "Evaluating Intelligence Oversight Committees: The UK Intelligence and Security Committee and the 'War on Terror'." *Intelligence and National Security* 22, no. 1 (2007): 14–37.

Goldman, Zachary K., and Samuel James Rascoff. "Introduction. The New Intelligence Oversight." In *Global Intelligence Oversight: Governing Security in the*

Twenty-First Century, edited by Zachary K Goldman and Samuel James Rascoff, xvii–xxxi. Oxford: Oxford University Press, 2016.

Han, Byung-Chul. *The Transparency Society*, translated by Erik Butler. Stanford, CA: Stanford University Press, 2015.

Hardin, Russell. "Do We Want Trust in Government." In *Democracy and Trust*, edited byMark E Warren, 22–41. Cambridge: Cambridge University Press, 1999.

Heath-Kelly, Charlotte. "Cold War Psychiatry, Extremism, and Expertise: The "Special Committee on the Political Abuse of Psychiatry"." *International Political Sociology* 16, no. 1 (2021). 10.1093/ips/olab034. https://doi.org/10.1093/ips/olab034.

Hollingsworth, Mark, and Richard Norton-Taylor. "Mi5: Building Empires, Ruining Careers / a Look at the Long Tentacles of the Security Service." *The Guardian Weekly*. September 6, 1988.

"Investigatory Powers Bill. Volume 607." Hansard, 2016, accessed 7 November 2022. https://hansard.parliament.uk/commons/2016-03-15/debates/16031546000001/InvestigatoryPowersBill.

"Investigatory Powers Bill. Volume 611." 07 June 2016, 2016, accessed 1 August, 2016. https://hansard.parliament.uk/Commons/2016-06-07/debates/16060732000001/InvestigatoryPowersBill?highlight=needle%20haystack#contribution-16060733000117.

"Investigatory Powers Bill. Volume 616." Hansard, 2016, accessed 7 November 2022. https://hansard.parliament.uk/Commons/2016-11-01/debates/79609F80-4ECA-4C9D-93D8-98AA35992EF8/InvestigatoryPowersBill?highlight=suella%20fernandes#contribution-FB21B325-99C1-40FB-B064-698D6C4F63E9.

"Ip Draft Bill." 2016, accessed 5 June, 2023. https://conspicuouschatter.wordpress.com/2015/11/05/uk-draft-ip-bill-the-last-policy-discussion-about-surveillance-before-the-mass-gagging/.

Johnson, Loch K. "A Shock Theory of Congressional Accountability for Intelligence." In *Handbook of Intelligence Studies*, edited by Loch K. Johnson, 361–378. London: Routledge, 2007.

Kibbe, Jennifer. "Congressional Oversight of Intelligence: Is the Solution Part of the Problem?". *Intelligence and National Security* 25, no. 1 (2010/02/01 2010): 24–49. https://doi.org/10.1080/02684521003588104.

King, Tom. *A King among Ministers: Fifty Years in Parliament Recalled*. Lewes, UK: Unicorn, 2020.

Leigh, Ian. "Rebalancing Rights and National Security: Reforming UK Intelligence Oversight a Decade after 9/11." *Intelligence and National Security* 27, no. 5 (2012/10/01 2012): 722–738. https://doi.org/10.1080/02684527.2012.708525.

Leon-Reyes, Bernardino. "Towards a Reflexive Study of Intelligence Accountability." In *Problematising Intelligence Studies*, edited by Hager Ben Jaffel and Sebastian Larsson, 30–47. London: Routledge, 2022.

Lyon, David, ed. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London: Routledge, 2003.

McCubbins, Mathew D., and Thomas Schwartz. "Congressional Oversight Overlooked: Police Patrols Versus Fire Alarms." *American Journal of Political Science* (1984): 165–179.

Morgan, P. "The Mi5 Spy Who Had a Conscience." *Courier-Mail*, 1985, 11 May.

Offe, Claus. "Can We Trust Our Fellow Citizens?" In *Democracy and Trust*, edited by Mark E Warren, 42–87. Cambridge: Cambridge University Press, 2010.

Omand, David, and Mark Phythian. *Principled Spying: The Ethics of Secret Intelligence*. Oxford University Press, 2018.

"Organisations We Oversee." 2023, accessed 5 June 2023. https://www.ipco.org.uk/what-we-do.

Ott, Marvin C. "Partisanship and the Decline of Intelligence Oversight." *International Journal of Intelligence and CounterIntelligence* 16, no. 1 (2003/01/01 2003): 69–94. https://doi.org/10.1080/713830378.

Rosanvallon, Pierre. *Counter-Democracy: Politics in an Age of Distrust*. Cambridge: Cambridge University Press, 2008.

"Security Service." 1993, accessed 23 August 2022, 2022. https://hansard.parliament.uk/Commons/1993-03-29/debates/f51f0921-3199-496b-8d39-036655b9e209/SecurityService?highlight=hewitt#contribution-4ca1798d-f921-4756-83a3-5b0ba9813108.

"Security Services Act." 1989, accessed 7 November 2022. https://www.legislation.gov.uk/ukpga/1989/5/contents.

"Security Services Bill." Hansard, 1988, accessed 23 August 2022. https://hansard.parliament.uk/Commons/1988-12-15/debates/d883cff5-8a7b-4f69-a85d-45e6767e5ffa/SecurityServiceBill?highlight=hewitt#contribution-96ac9194-69e7-4239-b0dd-83efe7cdb285.

"Shades of Independent Review." 2017, accessed 13 January 2020. https://www.daqc.co.uk/2017/12/06/shades-independent-review/.

Smith, James. *British Writers and Mi5 Surveillance, 1930–1960*. New York: Cambridge University Press, 2012.

Travis, Alan, and Richard Norton-Taylor. "Campaigners Shine Light on State Abuses. Consortium Launches Drive to Encourage 'Ordinary People' to Challenge Secrecy Surveillance and Vetting." *The Guardian*, 1993, 8 June.

Tuinier, Pepijn, Thijs Brocades Zaalberg, and Sebastiaan Rietjens. "The Social Ties That Bind: Unraveling the Role of Trust in International Intelligence Cooperation." *International Journal of Intelligence and CounterIntelligence* (2022): 1–37. https://doi.org/10.1080/08850607.2022.2079161.

Warren, Mark E., ed. *Democracy and Trust*. Cambridge: Cambridge University Press, 2010.

West, Nigel. *Historical Dictionary of British Intelligence*. Lanham, MD: Scarecrow Press, 2014.

5 An analysis of post-Snowden civil society accountability

Bernardino León-Reyes

Introduction

The 2013 Snowden disclosures exposed an extensive global surveillance program by the United States' National Security Agency (NSA), which involved the collection of vast amounts of personal information from millions of individuals around the world. Despite the scale of the revelations and the outrage they sparked among civil society groups and the public, the policy changes that followed have been very limited, especially in comparison to the reforms that followed the intelligence scandals of the 1970s. A puzzle that some have labeled as "the Snowden Paradox"[1] which calls for explanation.

To that end, the purpose of this chapter is twofold: to describe the strategies of these civil society groups and to understand why they failed to achieve profound policy reforms. Drawing on in-depth ethnographic interviews (n = 48)[2] with not only journalists and activists but also policy makers, former security agents, and whistleblowers involved in the Snowden disclosures, this chapter sketches out the different groups and strategies followed within each of these two civil-society fields – journalism and activism – in the United States and the United Kingdom, tracing the historical shifts that have happened in both fields.

Furthermore, in line with the introduction to this volume, this chapter adopts an approach based on International Political Sociology (IPS) to destabilize traditional categories and classifications and to develop a more nuanced and complex understandings of the international. Therefore, this chapter questions methodological nationalism by tracing the "vernacularization" of the Snowden scandal – demonstrating how it was at the same time a transnational phenomenon but also affected by national power struggles –, as well as it concludes questioning the very category that it departs from: that of "civil society".[3]

Journalism: Controlling or normalizing intelligence scandals?

"Good journalism should challenge people". Carl Bernstein's quote is perhaps one of the best-remembered lines from the Watergate scandal. If we think about non-institutional efforts to render intelligence abuses accountable, the

DOI: 10.4324/9781003354130-6

image of the investigative journalist is perhaps the first image that comes to mind. From the scandals that triggered the Church, Pike, and Rockefeller committee, inaugurated by a 1974 investigation of the *New York Times*, to the involvement of the *Washington Post and the Guardian* in helping Edward Snowden in 2013, journalists have the capacity of pressuring public intelligence officials to investigate abuses and, occasionally, to undertake reforms.

While the relevance of the media is mentioned *en passant* in several publications, there is a surprising gap in the literature on intelligence studies on this topic. Only two publications delve in detail into the role of media in intelligence oversight: Caparini's book on the topic[4] and Hillebrand's journal article in *Intelligence and National Security*;[5] beyond this, most references to the issue are oblique,[6] reflecting the lack of interest in civil society in the discipline.[7] If we look at the discipline of International Relations more broadly, we find recent publications on the matter, such as Ochoa et al.[8] While these studies of the press are nuanced enough to avoid essentializing in a normative way (i.e., reducing it to what it *should* be), they do fall short on other ends. Particularly, they fail to grasp the differing logics within the field of journalism, which have different resources at stake and dynamics.

If we want to answer rigorously to the question of "how do media render accountable the actions of intelligence services", we must be attentive to the different sub-fields of journalism. In other words, what are the transformations, stakes, and struggles around resources in each of them. At the most basic level, we should distinguish between at least three sub-fields of the media: investigative journalism, general reporting, and opinion pieces. Even if these three forms of journalism can be found together in the most influential newspapers like the *New York Times*, the *Washington Post*, the *Guardian,* or *Le Monde*, each of them has very different origins that can be traced through sociogenesis.

Investigative journalism

The American investigative tradition spans back to the first decade of the twentieth century, when so-called "muckrakers" became celebrities exposing the crimes of magnates, politicians, and other actors of an incipient industrial society.[9] While these early investigative journalists were initially able to influence progressive reformers, their relevance declined from the 1920s. It was not until the 1970s that the Pentagon Papers, Watergate, and other scandals inaugurated a new "Golden Age" of investigative reporting. Journalists were democratic heroes, portrayed by Hollywood stars. However, with the optimism of the post-Cold War – which lowered political and economic turmoil – the public had less appetite for this type of reporting. In addition, since the expansion of internet advertisements, many local newspapers (which did much of the investigative heavy-lifting of the country) had to close down or slash their budgets, often closing their expensive investigative teams.[10] In addition, by the time Edward Snowden became concerned

with the increasing capabilities of the NSA, hacktivist Julian Assange and his team at WikiLeaks were attempting to reinvent journalism with what they called "citizen journalism": the practice of releasing thousands of documents to the public, without curating, spinning, or pacing them in the fashion that investigative reporters had done until then.

All this to say that it was not obvious, by any means, that Edward Snowden would recur to four investigative reporters to help him blow the whistle. One of the reasons he chose Glenn Greenwald was because he had participated in online forums discussing US intelligence abuses for some years,[11] where Greenwald was regarded as someone hostile to the agencies and the practice of refraining from holding back stories. Snowden trusted the autonomy of Laura Poitras, Glenn Greenwald, Barton Gellman, and Ewen MacAskill, which had broken important stories in the Guardian and the Washington Post.[12] However sclerotic investigative journalism had become, Snowden had seen the way in which every US administration had delegitimized previous whistleblowers, not only pressing charges under the Espionage Act of 1917 but also leaking personal details to make them look like a traitor. Therefore, he required the prestige of these media outlets to legitimize the authenticity and the relevance of those documents.

Unlike Julian Assange's more radical positioning, Edward Snowden's habitus did not push him toward seeking to overthrow any system, but rather to reform and protect the United States, the country to which he had pledged allegiance as a former member of the military. For this reason and because of his concerns about potentially inadvertently disclosing classified information to US enemies, Snowden chose to carefully handle all documents and only release them to journalist Glenn Greenwald. He also made a conscious decision to avoid releasing documents that could put US personnel in danger.

Not only that: he trusted the capacity of these outlets to keep a story alive for a sustained period of time. Investigative journalists tend to be experts in building the agenda: setting the topics discussed in different media forms, such as TV talks or op-eds, and pressuring policy makers to take action.[13] In comparison to citizen journalism, traditional investigative journalism such as that of Poitras, Greenwald, Gellman, and MacAskill amplified the gravity of the disclosures. An incredible amount of work is done behind the racks: spinning the story in a specific way, controlling the timeframe to keep the story alive as long as possible, and using informal networks of other journalists and politicians:

> Glenn and Greenwald had been in Hong Kong for a few days. And as you can imagine, like trying to consume U.S. News in Hong Kong, you certainly can get a sense, but you can't really get a sense of like the feel of it. And so that was a big a big part of it. And, you know, I had to tell Glenn "it's great that you're aggressively pushing to get all these stories out, but you need to slow it down a little bit because we need to be able to digest these stories and kind of figure out like, what is the strategy for!".[14]

However, what are some of the challenges that investigative journalists are facing today? Chief among them, there is what we could call a "selective crackdown on leaking": the fact that the administration does not prosecute the frequent leaks spined by government officials but do so when whistleblowers denounce wrongdoings.[15] In every single interview among the dozen I had with investigative reporters, they all described an increasing pressure from every administration – local or national – to limit their capacity to report.[16]

> I was later part of a government leak investigation into [one] story and I found it devastating because I hadn't been briefed as a reporter beforehand what the FBI could legally access. I didn't know that they could just go into my Gmail. I didn't know how they got 40 days if my phone records. It turns out, I mean, at least as far as I know, they did not disclose having taken any of my emails and they're supposed to disclose what they take. But they interviewed anyone I spoke to in a 40 day period who had access to classified information. I have one best friend who still won't speak to me. So, and it also had a very chilling effect on my future journalism because I always wondered. You know, when I came out with a scoop, is this going to end the career of the person or people that I interviewed?[17]

This experience is the most extreme expression of the efforts by administrations to limit reporting on these issues. A 2014 PEN American Center report on the chilling effects of these practices found that 28% of US journalists "had curtailed or avoided social media activities" on the topic of national security, and 16% had "avoided writing or speaking about a particular topic". In other words, the crackdown on whistleblowers is also an attack of free press.

General news

The ways in which these investigations are covered in general reporting are essential, as we do know that the wider public and policy makers are extremely influenced by them. As a former US Senate staffer recalled,

> The first thing members of Congress do and of course I've worked for a number of them is that they get the New York Times, they get The Washington Post. Some of them were conservative ones, read The Wall Street Journal. They read a couple of newspapers from their home state, and that's how they begin their day over a cup of coffee. And if there's something in the New York Times that said the CIA is kidnaping young girls and taking into Afghanistan, well, that would get your attention.[18]

For that reason, it is essential to understand how the wider media landscape translates these investigations into their daily coverage. In a personal interview, Barton Gellman, Washington Post journalist and Pulitzer award-winning for

his role in the Snowden disclosures, shared his recollection of the media climate after the story broke:

> You had the problem of our competitors. And the competitors of The Washington Post couldn't match the story because you really needed to have the documents and there was no path for that so that a limited number of choices for how they could advance the story. One way to advance the story is to find sources who will tell you very skeptical things about the story and who will leak information about Snowden personally or will claim that internal investigations are not finding evidence for this […] There are lots of ways that you can undermine this story because you have cooperative sources in the government whose job is to dampen the impact.[19]

Therefore, here we see two realities coming together to shape the way in which the media covered the Snowden revelations. On the one hand, an aggressive administration that, as we have seen, will not hesitate to heavily persuade journalists to the point of intimidating them. On the other hand, and perhaps more important, we start recognizing in this testimony the fact that oftentimes media controversies are more shaped by previous cleavages and enmities. As a former investigative reporter, turned scholar of journalism, Paul Lashmar explains in relation to the United Kingdom, where this controversy was vernacularized:

> So, when it comes to The Guardian, why did The Mail and other newspapers attack it? Well, one of the one of the suppositions that can be made, if you might read the editors of those newspapers minds, was that they were getting their own back of the phone hacking because The Guardian had led the attack on phone hacking by Nick Davis and had caused huge, huge problems for News International, resulted in closure in custody, probably millions, if not a billion pounds of damages through the Murdoch empire. […] And when The Guardian did that, it made some very, very bad enemies. And I think that was part of the motivation on the attacks on The Guardian.[20]

This maps really well with the recollections of a British senior activist, who explained in these terms the struggles, the reaction of the media that did not have the documents ranged from ignoring the topic to attacking the Guardian for running it:

> Who had the documents? The Guardian. No one else had documents. And so he ran the story. The Guardian. Who else ran stories? Nobody. So, the first huge dynamic in all of it was the this was the Guardian's story. And basically, nobody else touched it. So, stuff that was Earth shattering barely got a mention everywhere else. And, in lots of ways, the press turned on

> The Guardian and said "you're risking national security". That was the Daily Mail, the Sun, you know, really attacking.[21]

A different senior activist involved in the same campaign recalled that

> Prior to the Snowden incident in 2013, the media, including The Sun, were fascinated by and wrote extensively about our work. However, when Snowden happened, the media, including those who had previously supported us, turned against us because The Guardian had the exclusive story, and it was seen as an "American outing our our boys".[22]

Here, we can observe how the struggles in British media ended up with a narrative of protecting and legitimizing GCHQ ("our boys") in order to use it as a weapon against the Guardian by its competitors, instead of the trend that many activists feel they had been seeing before. In sum, while the constraints that investigative journalists face usually have more to do with judiciary pressures and efforts to delegitimize their sources, in the case of general reporting, the Snowden coverage suffered from journalists that recurred to official statements and explanations that covered their knowledge gaps, and from previous cleavages that were used by rivals to attack the Post in the United States, and the Guardian in the United Kingdom.

Opinion pieces

As described by sociologist Robert Park almost a hundred years ago, when we refer to the "power of the press" what we usually refer to is not that of the reporter, but that of the editorial.[23] Newspaper opinion pieces are essential to political reforms, since they

> have the power to set the dominant political agenda, as elaborated over weeks, months and years, in editorials, columns and other forms of pro-active, opinionated journalism, amounting to extended narratives of unity and division, success and failure, rise and fall. In this capacity the institutions of the press take the lead in establishing the dominant interpretative frameworks within which ongoing political events are made sense of.[24]

In fact, the power of opinion pieces not only sets the agenda of elite policy makers; we also have evidence about the fact that it influences the views of readers.[25] In terms of who makes up the writers of op-eds (contributions from figures that are not affiliated to the newspaper), while these vary country to country, in the Anglo-American world they are mostly elite pundits,[26] relatively close to government officials and business magnates. Since contributors are not beat reporters, the resource at stake is different: mostly, influence. This explains the interest and strategies of these authors, who in the cases of

the United States and the United Kingdom worked to discredit Snowden much more than other forms of journalism.

Take for instance the case of the *New York Times*: while its investigative journalists covered the Snowden story in a rigorous way, not only amplifying the Guardian or the Post's documents but also digging out the technical details, its pundits attacked Snowden. David Brooks, one of the *New York Times* best-known commentators, assessed Snowden's action in the following way: "He betrayed honesty and integrity, the foundation of all cooperative activity", "He betrayed his friends", "He betrayed his employers", "He betrayed the privacy of us all", and "He betrayed the Constitution".[27] He went as far as affirming that "He betrayed the cause of open government".

Not only this: Brooks also described Snowden as someone who lived "a life unshaped by the mediating institutions of 'civil society'" which for him explained why he "unilaterally leak[ed] secret NSA documents, Snowden has betrayed all of these things".[28] As we have seen in this section, this description goes beyond opinion, as it is *factually* wrong.[29] Snowden did not leak those documents on the Internet without mediating institutions; he actually claimed the tradition of resorting to traditional investigative journalists.

The case of the *New York Times* is interesting because it highlights the differences between sub-fields of journalism, especially between investigative journalists and opinion contributors. A revision of the most influential outlets shows similar efforts of delegitimation: the *Wall Street Journal*,[30] *Bloomberg*,[31] the *New Yorker*,[32] *Chicago Tribune,*[33] and *CNN*.[34] Even the Washington Post published op-eds that watered down the relevance of their own investigation.[35] Far from anecdotal, the academic literature shows that this was the dominant trend in opinion pieces in both the United States and the United Kingdom:

> In our newspaper sample, the most frequently expressed view was that surveillance should be increased or is acceptable/necessary (present in 9% of stories). Sources expressing this view suggested that surveillance is crucial to national security, and particularly important to strengthen in the light of terrorist threat. For example, Colonel Tim Collins (a former SAS officer), justified practices of surveillance with reference to the threat from "Islamic fundamentalists".[36]

As they show, opinion sections in newspapers mainly worked as a vehicle of surveillance normalization, which can be explained by the proximity of pundits to the field of power.

The description of these different sub-fields of journalism illustrates the reality of media oversight: this can range from revealing wrongdoings in the case of investigative journalism, to the normalization of the practices revealed like many op-eds. In between, normal reporting can set the agenda in a way that pressures policy makers to act, or reproduce the arguments of the agencies, a strategy that will be likely determined by the previous cleavages in that particular media landscape, and the resources (i.e., a scoop) at their

availability. Media, in sum, is not a single agent, but a complex network of actors in constant relations of conflict or cooperation.

Activism

Mapping the structure and the recent transformations of the field of activism is somehow a more complicated task, due to the difficulty to delineate its limits. At least, it encompasses non-governmental organizations, unions, churches, foundations, and translocal voluntary membership associations; in other words, what usually comes to mind when we think of "civil society". However, if we want to understand this field at the time of the Snowden disclosures and the strategies it followed, it is essential to account for the radical transformations it has suffered in the past decades: what sociologist Theda Skocpol calls the "shift from membership to management". As she argues, until the 1960s members of associations "could strengthen their ties to friends, neighbors, and family members in the local community and at the same express values and an identity shared by large numbers of other people they never met personally".[37] The backbone of activism was the involvement of everyday members, whose identity and circles were shaped by their participations.

Since the development of what we could loosely refer to as neoliberalism, these bonds broke, being replaced: "professionally run advocacy groups and nonprofit institutions now dominate 'civil society', as people seek influence and community through a very new mix of largely memberless voluntary organizations".[38] Skocpol's argument goes in line with Robert Putnam's essay *Bowling Alone*, which argues that social capital has been in the decline in the past years with the loss of spaces of socialization[39] – something that can also be observed in the "cartelization" of political parties[40] or the collapse of trade unions[41]. It is in this context, where anti-surveillance organizations look more and more like interest groups than grassroot organizations, that Snowden breaks.[42] However, this does not entail that social capital has lost importance in the field of activism. On the contrary, what we can observe is a transformation of the structure of this capital which could be described as a shift from large networks of grassroot organizations to more elite-bounded groups. Here, what becomes essential to study is the interaction between the two fields studied in this chapter (journalism and activism), and their embeddedness in the field of politics.

The importance of social capital is encapsulated in this interview with a chief of communications of the Electronic Frontier Foundation, who had previously worked as a senior staffer for a US senior politician in Washington D.C.:

> It is all about building relationships. It's being able to know the people who are your key sources, or the reporters covering your beats and have a familiar relationship with them as a reporter. I would call up elected officials and their staffs sometimes just to, you know, make idle conversation. When I was just starting as a reporter in my first job, I was a city hall

> reporter. I'd go to city hall every day. I would listen to the planning directors' terrible jokes. It's not a matter of being disingenuous. But you have to be familiar if people are going to entrust you with information as a journalist, right? You must be somebody that they know and trust. Emails, texts, you know, phone calls, it's just a constant touch, so that when I did come asking for information, I was certainly not a stranger. I was somebody that they felt they liked and respected.[43]

It is important that this process is by no means recent. In the history of anti-surveillance activism, groups like the ACLU spent an important amount of time "carefully cultivating" political network in DC.[44] What is new is the limited focus on smaller network strategies, which would stem on the shift of focusing exclusively on strategic litigation. This shift is not a conscious decision that activist organizations took at a certain moment of history; rather, it is the consequence of the accumulation of decades of sociological change, with factors as diverse as the use of television and the growth of the Internet but also urban transformations such as the rise of suburbanization.[45] It is in this new context, where the decline of membership-based organizations, such as political parties, labor unions, and other civic groups, has contributed to a shift toward a more managerial style of governance,[46] where anti-surveillance activist groups have to find new strategies (such as those described above), and where essentially non-participatory organizations that derive their influence in the symbolic power of their "technical knowledge" find their moment to consolidate as extremely important actors.

NGOs: From campaigns to lobbying and strategic litigation

The decline of traditional membership-based organizations has had a profound impact on the way that activist groups operate and the strategies they choose to pursue. In the past, these organizations were often able to rely on mass mobilization, such as protests and demonstrations, to exert pressure on decision-makers and raise awareness about their causes. While there were some grassroot mobilizations, they were not near the uproar of the late 1960s and early 1970s, which created the political opportunity for anti-surveillance organizations to advance their agenda. However, in the current context of declining social capital and a shift toward a more managerial style of governance, these tactics may be less available than they once were, as it is extremely hard to mobilize people when you only have *subscribers*.

As a result, activist groups have had to find new ways to make their voices heard and achieve their goals. Some have turned to social media and other online platforms to reach a wider audience and mobilize support for their causes. Others have focused on more targeted advocacy efforts, working behind the scenes to influence policy decisions and build coalitions with like-minded organizations through strategies like open letters.[47] These strategies of working with policy makers and pressuring them with letters might prove

useful in certain issues, but national security and surveillance do not seem to be one of them. As Patrick G. Eddington (former CIA whistleblower that went through Congress to reveal internal wrongdoings) explained in a personal interview with me,

> the ACLU and a few other large groups that took an extremely conventional approach to dealing with these issues, which was to get meetings with Hill staff, which was to write letters to committee members and all the rest of that and try to get opportunities to testify and so on and so forth. And the underlying assumption, of course, is if you go through that exercise, that somehow, you're going to get the outcome, that you're looking for something close to it. But when you ignore the fact that these that these committees are basically organizationally captured, functionally organizationally captured by the very agencies and departments that they were supposed to be overseeing, then the entire premise that you're operating on is invalidated.[48]

The story in the United Kingdom is similar. There, the most important initiative that reacted to Snowden and the subsequent *Investigatory Powers Act* was the "Don't Spy on Us" coalition, which brought together organizations such as Privacy International, Liberty, Big Brother Watch, or Reporters Without Borders. However, the strategy was not one of protest and direct confrontation: as in the US case, the repertoire of strategies ranged from lobbying MPs to open letters. When the coalition realized that neither the Conservative government nor Labor, the opposition, would support these proposed amendments, they recurred to a letter signed by over 200 senior lawyers that opposed the piece of legislation.[49] The repertoire of these organizations did not change in the sense of adopting these elite strategies, which were indeed part of campaigns in the 1970s; they shifted in the sense of failing to build grassroot protests and in the sense of building coalitions with other movements.

Furthermore, the other card that most post-Snowden anti-sruveillance organization played was that of strategic litigation. The main reason behind this was that with Snowden's documents, these organizations had for the first time in decades something they had craved for: evidence. As a former senior manager in Privacy International who at the time was involved in these struggles, "because of him, we were able to shift gears and get into litigation. We finally had the data".[50] While they did strike significant victorious cases in the United Kingdom (not so much in the United States), many activists felt like it was not enough. The same senior manager told us that

> Moving in to post Snowden litigation was the biggest mistake strategically we could have made for continuing to bring the public with us.

This can probably be explained by, on top of the sociological changes that led to a diminishment of social capital mentioned above, to a transformation

in the habitus of activists, as they have become less inclined to rely on traditional forms of mass mobilization. As one interviewee noted,

> We very rarely have in-person protests because that is not who we are as a group. We are primarily digital rights activists who are followed by others who share our values. Additionally, the work we do is often specialized and may not lend itself to protesting in a physical space.[51]

In this sense, while the constraints and difficulty of mobilizing people for an in-place protest are real, there is another layer of complexity derived from this new activist habitus, more skeptical of even attempting it, together with other factors such as the fact that today is harder to mobilize people and the loss of activist culture. This habitus is also evident on the other side of the Atlantic, where a former senior activist involved in the Don't Spy on Us coalition recalled:

> The next thing says that they were all professional NGOs. None of those groups were grassroots campaign protest groups. So, there was no discussion about, you know, "should this be a different sort of movement?". That's not what any of these organizations did All those organizations did is policy campaigning mainly in parliament and press work, basically. Those were their tools. So, it was already kind of narrowed set. So, there wasn't a huge debate around should we be using all these other methods? It was these the tools that we use for all sorts of reasons. We will deployed them as we do and everyone playing to their relative strengths where they could.[52]

In other words, while constraints mentioned above exist, there is "a way of doing things" that is internalized by professional activists that rule out, prima facie, other forms of activism beyond those of lobbying.

All in all, the decline of traditional membership-based organizations has left activist groups struggling to find effective ways to make their voices heard and achieve their goals. Despite attempts to utilize social media and targeted advocacy efforts, as well as resorting to strategic litigation using evidence from sources like Edward Snowden, these tactics have proven largely futile in bringing about any real change in the realm of national security and surveillance. In fact, activist groups have faced significant challenges in mobilizing mass support and in successfully influencing policy decisions through methods such as open letters and lobbying. In desperation, some have even returned to more traditional tactics like protests and demonstrations, but it remains uncertain whether these strategies will be any more effective in the current political climate. Overall, it seems that the decline of traditional membership-based organizations has severely hampered the ability of activist groups to make a meaningful impact on issues related to national security and surveillance.

The raise of the "think tank paradigm"

Concomitant to the shift from participative to managerial activism, another player came to town in the business of pressuring for policy reforms: think tanks. While the exact extent of their influence seems difficult to estimate,[53] there is little doubt they have become important players in the policy process. While the commonsensical narrative about these centers is that, in the United States, they were co-constitutive of the conservative revolution of the 1980s that culminated with the victory of Ronald Reagan, it was in fact a trend inaugurated by the Carter administration. During his mandate, Democrats increasingly replaced the reliance on grassroots movements toward that of think tanks that embraced the principles of neoclassical economics (especially in the cases of the Brookings Institution and the RAND Corporation), a process that explains the shift in center-left parties from the principle of equality to that of efficiency.[54] What remains true of the usual narrative of the emergence of think tanks is that in the 1970s an incipient conservative revolution coupled with the involvement in politics of business multiplied the budgets of conservative think tanks, whose capacity accounts for part of the success in the expansion of those ideas among the Anglo-American policy makers at both sides of the Atlantic. In this sense, the United Kingdom experienced too a similar process, with the Center for Policy Studies' influence over Margaret Thatcher's policies and public discourses,[55] and a myriad of think tanks in the raise of New Labor in the 1990s.[56]

In a context where think tanks have an enormous influence not only over policy makers but generally over the intellectual and political elite (i.e., journalists, pundits, businesspeople, and scholars), most of them served as a vehicle of delegitimation of Edward Snowden. This influence can be explained by their capacity to influence the opinion through the frequent publication of op-eds opinions.[57] Think tanks are not like universities or other kinds of research centers; they obtain that influence through aggressive campaigns. As Berry explains,

> Virtually all think tanks employ media specialists whose job is to put journalists in touch with the research staff and to gain publicity for studies when they are published. The media staffers pitch stories to journalists much the same way public relations specialists do, but think tanks have considerably more credibility than public relations firms because their *raison d'etre* is policy expertise. This credibility, along with aggressive marketing, has given think tanks considerable success in gaining media attention.[58]

Think tanks can also wield significant influence through this social capital, or the networks they build with journalists, policy makers, and interest groups. These networks can be used to promote the ideas and research produced by the think tank, giving them a platform to shape the public discourse on a particular

issue. This was evident in the aftermath of the Snowden leaks, as think tanks with strong connections to government agencies and policy makers were able to get their perspectives on the controversy featured prominently in the media.

Waging this influence, most think tanks not only echoed the official "traitor" attack (like the Brookings Institution[59] did); the Rand Corporation[60] went as far as saying in 2013 that Snowden "got everything wrong" and in 2020 argued against pardoning him on the basis that it would endanger official secrets. We find similar arguments in the Council on Foreign Relations[61] and in the Center for Strategic and International Studies,[62] which insist not only on the "danger" of the disclosures, but also accuse Snowden of endangering diplomacy or even "escalating the cyber war with China". Here, we find a trend that Denham and Garnett already observed in many think tanks in the survey they conducted in the late 1990s: think tanks "act as political shields, making the public more willing to accept policies which might be badly received if they were first mooted by a government spokesman".[63]

This response from think tanks was not surprising, given that many of these organizations have close ties to the government and receive funding from government sources. This funding can create a bias in the research and analysis produced by these think tanks, as they may be more likely to promote the interests of their funders.

In conclusion, think tanks have become influential players in the policy process and public discourse on various issues. They have the ability to shape public opinion through their media campaigns and connections with policy makers, journalists, and interest groups. In the case of Edward Snowden and the disclosures he made about government surveillance, think tanks played a significant role in delegitimizing his actions and perpetuating the narrative that he was a traitor. Many think tanks with connections to government agencies and policy makers were able to get their perspectives featured prominently in the media and influenced the public's understanding of the controversy. More so than most activist organizations.

Once our societies move in the direction of a more managerial civil society, activist organizations have everything to lose vis-à-vis think tanks if they keep playing *exclusively* by their rules. There are many parallelisms between the strategies from the 1970s and the post-2013 repertoire but are lacking the reality that offered the political opportunity for reformers: the grassroots, radical protests surrounding these campaigns.[64]

Conclusion

The purpose of this chapter was twofold: first, providing an ethnographic description of the strategies of journalists and activists working on national security in the United States and the United Kingdom after the Snowden revelations. It has insisted on the importance of understanding the different categories within each of these fields, as well as their incentives and habits. Second, hinting at what can partially explain the failure to limit the capabilities

of intelligence services on both sides of the Atlantic. For this, it has traced historical shifts in the fields of journalism and activism, showing how their capacity has been crippled by a myriad of factors, from a more aggressive stance of administrations vis-à-vis whistleblowers to a political economy that has deprived civil society of its traditional participatory facet.[65] In this sense, another transformation within the field of journalism that should be considered is the diminishing of investigative team budgets.

While these explanations should be analyzed together with transformations of the political field, whereby professionals of politics have progressively become disjointed from civil society, these historical shifts can explain to a certain extent the "Snowden Paradox".

Notes

1 Félix Tréguer, 'Intelligence Reform and the Snowden Paradox: The Case of France', *Media and Communication* 5, no. 1 (22 March 2017): 17–28, 10.17645/mac.v5i1.821.
2 These in-depth interviews constitute a multi-sited ethnography conducted over the course of four years with investigative journalists, general reporters, scholars, activists, former agents and policymakers.
3 For this reason, I use throughout the paper the concept in quotation marks.
4 Marina Caparini, *Media in Security and Governance: The Role of the News Media in Security Oversight And Accountability: 8* (Baden-Baden, 2004).
5 Claudia Hillebrand, "The Role of News Media in Intelligence Oversight," *Intelligence and National Security* 27, no. 5 (October 1, 2012): 689–706, 10.1080/02684527.2012.708521.
6 Jonathan Moran, "The Role of the Security Services in Democratization: An Analysis of South Korea's Agency for National Security Planning," *Intelligence and National Security* 13, no. 4 (December 1, 1998): 8, 10.1080/02684529808432503; Geoffrey R. Weller, "Political Scrutiny and Control of Scandinavia's Security and Intelligence Services," *International Journal of Intelligence and CounterIntelligence* 13, no. 2 (April 1, 2000): 185, 10.1080/08850600050129709; H. Born, Loch K. Johnson, and I. Leigh, *Who's Watching the Spies? Establishing Intelligence Service Accountability*, 1st ed (Washington, DC: Potomac Books, 2005); Richard J. Aldrich, "Global Intelligence Co-Operation versus Accountability: New Facets to an Old Problem," *Intelligence and National Security* 24, no. 1 (February 2009): 35, 10.1080/02684520902756812; Peter Gill, "Evaluating Intelligence Oversight Committees: The UK Intelligence and Security Committee and the 'War on Terror,'" *Intelligence and National Security* 22, no. 1 (February 1, 2007): 31, 10.1080/02684520701200756.
7 Bernardino León-Reyes, 'Towards a Reflexive Study of Intelligence Accountability', in *Problematising Intelligence Studies: Towards A New Research Agenda* (Routledge, 2022), 30–47, 10.4324/9781003205463-3.
8 Christopher Smith Ochoa, Frank Gadinger, and Taylan Yildiz, "Surveillance under Dispute: Conceptualising Narrative Legitimation Politics," *European Journal of International Security* 6, no. 2 (May 2021): 210–32, 10.1017/eis.2020.23.
9 The earliest examples of proto-investigative journalism in the US can be traced to the late 17th century; however, this remained embryonic and marginal until the sociological conditions for it developed (mass circulation, the expansion of education and economic industrialisation) Mark Feldstein, "A Muckraking Model: Investigative Reporting Cycles in American History," *Harvard International Journal of Press/Politics* 11, no. 2 (April 1, 2006): 107–9, 10.1177/1081180×X06286780.

10 Julia Cage
11 Crawford Kilian, "Why Edward Snowden Chose Glenn Greenwald," The Tyee (The Tyee, May 30, 2014), https://thetyee.ca/Books/2014/05/30/No-Place-to-Hide/.
12 Some of the reasons why he did not choose the New York Times, perhaps the most obvious choice, was that they had held on a wiretapping investigation for more than a year from 2004 to 2005, and the WMD stories fed by the Bush administration to justify the invasion of Iraq in 2003.
13 David L. Protess et al., *The Journalism of Outrage: Investigative Reporting and Agenda Building in America* (New York, 1991); Gerry Lanosga and Jason Martin, "Journalists, Sources, and Policy Outcomes: Insights from Three-plus Decades of Investigative Reporting Contest Entries," *Journalism* 19, no. 12 (December 1, 2018): 1686, 10.1177/1464884916683555.
14 Bernardino Leon-Reyes, Interview with senior journalist and civil society actor (US), 19 January 2023.
15 Jack Shafer, "Edward Snowden and the Selective Targeting of Leaks," *Reuters News*, June 12, 2013, http://global.factiva.com/redir/default.aspx?P=sa&an=LBA0000020130612e96c000q6&cat=a&ep=ASE.
16 This is one of the reasons why news like Snowden must be broke by large organizations such as the Guardian or the Washington Post: because they have the legal teams to protect their sources and journalists. See, for instance, the sections on legal counsel: Barton Gellman, *Dark Mirror: Edward Snowden and the American Surveillance State* (New York: Penguin Press, 2020).
17 Bernardino Leon-Reyes, Interview with journalist, national security beat (US), 11 January 2021.
18 Bernardino Leon-Reyes, Interview with former staffer, US Senate (US), n.d.
19 Bernardino Leon-Reyes, Interview with Barton Gellman (US), March 23, 2022.
20 Bernardino Leon-Reyes, Interview with Paul Lashmar (UK), January 26, 2021.
21 Bernardino Leon-Reyes, Interview with former activist, Senior Manager (UK), 2 September 2023.
22 Mc Cluskey and Leon-Reyes, Interview with Former Senior Manager, Privacy International (UK).
23 Robert E. Park, "The Natural History of the Newspaper," *American Journal of Sociology* 29, no. 3 (1923): 273–89.
24 Brian McNair, "JOURNALISM AND DEMOCRACY: An Evaluation of the Political Public Sphere," n.d., 30.
25 Alexander Coppock, Emily Ekins, and David Kirby, "The Long-Lasting Effects of Newspaper Op-Eds on Public Opinion," *Quarterly Journal of Political Science* 13, no. 1 (March 29, 2018): 59–87, 10.1561/100.00016112.
26 Karin Wahl-jorgensen, "Playground of the Pundits or Voice of the People? Comparing British and Danish Opinion Pages," *Journalism Studies* 5, no. 1 (February 2004): 59–70, 10.1080/1461670032000174747.
27 David Brooks, "The Solitary Leaker," *The New York Times*, June 11, 2013, sec. Opinion, https://www.nytimes.com/2013/06/11/opinion/brooks-the-solitary-leaker.html.
28 Brooks.
29 Conservative op-ed contributors have a significant record ignoring evidence. See: Shaun W. Elsasser and Riley E. Dunlap, "Leading Voices in the Denier Choir: Conservative Columnists' Dismissal of Global Warming and Denigration of Climate Science," *American Behavioral Scientist* 57, no. 6 (June 1, 2013): 754–76, 10.1177/0002764212469800.
30 Michael B. Mukasey, "Leaking Secrets Empowers Terrorists," WSJ, June 9, 2013, http://online.wsj.com/article/SB10001424127887324634304578535492421480524.html.

31 Ratnesar Romesh, "The Unbearable Narcissism of Edward Snowden," *Bloomberg.Com*, November 1, 2013, https://www.bloomberg.com/news/articles/2013-11-01/the-unbearable-narcissism-of-edward-snowden.
32 Jeffrey Toobin, "Edward Snowden Is No Hero," The New Yorker, 2013, https://www.newyorker.com/news/daily-comment/edward-snowden-is-no-hero.
33 Alex Lyda, "Edward Snowden Is More Narcissist than Patriot," chicagotribune.com, 2014, https://www.chicagotribune.com/opinion/commentary/ct-snowden-cia-citizenfour-oscars-korea-perspec-1225-jm-20141223-story.html.
34 By Douglas Rushkoff CNN Special to, "Opinion: Edward Snowden Is a Hero," CNN, accessed April 11, 2021, https://www.cnn.com/2013/06/10/opinion/rushkoff-snowden-hero/index.html.
35 Richard Cohen, "Richard Cohen: NSA Is Doing What Google Does," *Washington Post*, June 10, 2013, sec. Opinions, https://www.washingtonpost.com/opinions/richard-cohen-nsa-is-doing-what-google-does/2013/06/10/fe969612-d1f7-11e2-8cbe-1bcbee06f8f8_story.html In a later op-ed, Cohen retracted from some of the positions he defended in his piece.
36 Karin Wahl-Jorgensen, Lucy Bennett, and Gregory Taylor, "The Normalization of Surveillance and the Invisibility of Digital Citizenship: Media Debates After the Snowden Disclosures," *International Journal of Communication* 11, no. 0 (February 14, 2017): 9.
37 Theda Skocpol, *Diminished Democracy: From Membership to Management in American Civic Life*, The Julian J. Rothbaum Distinguished Lecture Series, v. 8 (Norman: University of Oklahoma Press, 2003), 78.
38 Skocpol, 127.
39 Robert D. Putnam, *Bowling Alone: The Collapse and Revival of American Community* (New York: Simon & Schuster, 2000).
40 Peter Mair, *Ruling the Void: The Hollowing of Western Democracy* (Place of publication not identified: Verso, 2013).
41 Jorge Tamames, *For the People Left Populism in Spain and the US* (London: Lawrence & Wishart, 2020), 93.
42 Of course, interest groups did also exist in anti-surveillance activism in the 1970s. However, they had considerably less weight in their activities than grassroot activities.
43 Bernardino Leon-Reyes, Interview with Senior Manager, Media, EFF (US), December 21, 2022.
44 Katherine A Scott, 'Reining in the State: Civil Society, Congress, and the Movement to Democratize the National Security State (1970–1978)' (Philadelphia, Pennsylvania, Temple University, 2009), 211.
45 Putnam, *Bowling Alone*.
46 Skocpol, *Diminished Democracy*.
47 Consider for instance the following letters, directed to constituents in the US and to MPs in the UK (respectively): Cindy Cohn, "An Open Letter to Our Community On Congress's Vote to Extend NSA Spying From EFF Executive Director Cindy Cohn," Electronic Frontier Foundation, January 18, 2018, https://www.eff.org/deeplinks/2018/01/open-letter-our-community-congresss-vote-extend-nsa-spying-eff-executive-director; "Don't Spy on Us | Investigatory Powers Bill: How to Make It Fit-for-Purpose," Don't Spy on Us, accessed January 1, 2023, https://www.dontspyonus.org.uk/blog/2016/02/26/investigatory-powers-bill-how-to-make-it-fit-for-purpose/.
48 Bernardino Leon-Reyes, Interview with CIA whistleblower (US), November 17, 2022.
49 "Don't Spy on Us | Our Campaign," Don't Spy on Us, accessed September 10, 2022, https://www.dontspyonus.org.uk/our-campaign.

50 Emma Mc Cluskey and Bernardino Leon-Reyes, Interview with Former Senior Manager, Privacy International (UK), May 20, 2021.
51 Bernardino Leon-Reyes, Interview with Senior Manager, Strategy, EFF (US), November 29, 2022.
52 Leon-Reyes, Interview with former activist, Senior Manager (UK).
53 Richard Higgott and Diane Stone, "The Limits of Influence: Foreign Policy Think Tanks in Britain and the USA," *Review of International Studies* 20, no. 1 (January 1994): 15–34, 10.1017/S0260210500117760; Murray Weidenbaum, "Measuring the Influence of Think Tanks," *Society* 47, no. 2 (March 2010): 134–37, 10.1007/s12115-009-9292-8; "Old World, New World: The Evolution and Influence of Foreign Affairs Think-Tanks," 2022, 19.
54 Elizabeth Popp Berman, *Thinking like an Economist: How Efficiency Replaced Equality in U.S. Public Policy* (Princeton, 2022), 180.
55 Aled Davies, Ben Jackson and Florence Sutcliffe-Braithwaite, *The Neoliberal Age? Britain since the 1970s* (UCL Press, 2021), 10.14324/111.9781787356856.
56 Philip Schlesinger, "Creativity and the Experts: New Labour, Think Tanks, and the Policy Process," *The International Journal of Press/Politics* 14, no. 1 (January 1, 2009): 3–20, 10.1177/1940161208328898; Stephen J. Ball and Sonia Exley, "Making Policy with 'Good Ideas': Policy Networks and the 'intellectuals' of New Labour," *Journal of Education Policy* 25, no. 2 (2010): 151–69, 10.1080/02680930903486125; Hartwig Pautz, "New Labour in Government: Think-Tanks and Social Policy Reform, 1997–2001," *British Politics* 6 (June 1, 2011): 187–209, 10.1057/bp.2011.9.
57 David M. Ricci, *The Transformation of American Politics: The New Washington and the Rise of Think Tanks* (New Haven, 1993), 164.
58 Jeffrey M. Berry and Clyde Wilcox, *The Interest Group Society* (New York: Routledge, 2018).
59 Paul R. Pillar, "Snowden's Treason," *Brookings* (blog), November 30, 1AD, https://www.brookings.edu/opinions/snowdens-treason/.
60 Andrew Liepman, "What Did Edward Snowden Get Wrong? Everything," August 12, 2013, https://www.rand.org/blog/2013/08/what-did-edward-snowden-get-wrong-everything.html; Sina Beaghley and Marek N. Posard, "A Snowden Pardon Could Have a Snowball Effect on Protecting National Security Secrets," September 4, 2020, https://www.rand.org/blog/2020/09/a-snowden-pardon-could-have-a-snowball-effect-on-protecting.html.
61 "Extraditing Edward Snowden," Council on Foreign Relations, accessed September 12, 2022, https://www.cfr.org/interview/extraditing-edward-snowden.
62 "How Edward Snowden Escalated Cyber War With China," accessed September 12, 2022, https://www.csis.org/news/how-edward-snowden-escalated-cyber-war-china.
63 Andrew Denham and Mark Garnett, "The Nature and Impact of Think Tanks in Contemporary Britain," *Contemporary British History* 10, no. 1 (March 1996): 57, 10.1080/13619469608581367.
64 Scott, 'Reining in the State: Civil Society, Congress, and the Movement to Democratize the National Security State (1970-1978)', xiv.
65 Theda Skocpol, *Diminished Democracy: From Membership to Management in American Civic Life*, The Julian J. Rothbaum Distinguished Lecture Series, v. 8 (Norman: University of Oklahoma Press, 2003); Robert D. Putnam, *Bowling Alone: The Collapse and Revival of American Community* (New York: Simon & Schuster, 2000).

References

Abelson, Donald E. "Old World, New World: The Evolution and Influence of Foreign Affairs Think-Tanks." *International Affairs* 90 (2014): 125–142.

Aldrich, Richard J. "Global Intelligence Co-Operation versus Accountability: New Facets to an Old Problem." *Intelligence and National Security* 24, no. 1 (February 2009): 26–56. 10.1080/02684520902756812.

Ball, Stephen J., and Sonia Exley. "Making Policy with 'Good Ideas': Policy Networks and the 'intellectuals' of New Labour." *Journal of Education Policy* 25, no. 2 (2010): 151–169. 10.1080/02680930903486125.

Basaran, Tugba, Didier Bigo, Emmanuel-Pierre Guittet, and R. B. J. Walker, eds. *International Political Sociology: Transversal Lines*. London: Routledge, 2016. 10.4324/9781315693293.

Beaghley, Sina, and Marek N. Posard. "A Snowden Pardon Could Have a Snowball Effect on Protecting National Security Secrets." September 4, 2020. https://www.rand.org/blog/2020/09/a-snowden-pardon-could-have-a-snowball-effect-on-protecting.html.

Berman, Elizabeth Popp. *Thinking like an Economist: How Efficiency Replaced Equality in U.S. Public Policy*. Princeton, 2022.

Berry, Jeffrey M., and Clyde Wilcox. *The Interest Group Society*. New York: Routledge, 2018.

Born, H., Loch K. Johnson, and I. Leigh. *Who's Watching the Spies? Establishing Intelligence Service Accountability*. 1st ed. Washington, DC: Potomac Books, 2005.

Bourdieu, Pierre. *L'intérêt au désintéressement*. Raisons d'agir, 2022. http://journals.openedition.org/lectures.

Bricker, Jesse, Lisa J. Dettling, Alice Henriques, Joanne W. Hsu, Kevin B. Moore, John Sabelhaus, and Jeffrey Thompson. "Changes in U.S. Family Finances from 2010 to 2013: Evidence from the Survey of Consumer Finances," 2014, 41.

Brooks, David. "The Solitary Leaker." *The New York Times*, June 11, 2013, sec. Opinion. https://www.nytimes.com/2013/06/11/opinion/brooks-the-solitary-leaker.html.

Caparini, Marina. *Media in Security And Governance: The Role of the News Media in Security Oversight And Accountability: 8*. Baden-Baden, 2004.

CNN, By Douglas Rushkoff, Special to. "Opinion: Edward Snowden Is a Hero." *CNN*. Accessed April 11, 2021. https://www.cnn.com/2013/06/10/opinion/rushkoff-snowden-hero/index.html.

Cohen, Richard. "Richard Cohen: NSA Is Doing What Google Does." *Washington Post*, June 10, 2013, sec. Opinions. https://www.washingtonpost.com/opinions/richard-cohen-nsa-is-doing-what-google-does/2013/06/10/fe969612-d1f7–11e2–8cbe-1bcbee06f8f8_story.html.

Cohn, Cindy. "An Open Letter to Our Community On Congress's Vote to Extend NSA Spying From EFF Executive Director Cindy Cohn." *Electronic Frontier Foundation*, January 18, 2018. https://www.eff.org/deeplinks/2018/01/open-letter-our-community-congresss-vote-extend-nsa-spying-eff-executive-director.

Coppock, Alexander, Emily Ekins, and David Kirby. "The Long-Lasting Effects of Newspaper Op-Eds on Public Opinion." *Quarterly Journal of Political Science* 13, no. 1 (March 29, 2018): 59–87. 10.1561/100.00016112.

Council on Foreign Relations. "Extraditing Edward Snowden." Accessed September 12, 2022. https://www.cfr.org/interview/extraditing-edward-snowden.

Davies, Aled, Ben Jackson, and Florence Sutcliffe-Braithwaite. *The Neoliberal Age? Britain since the 1970s*, UCL Press, 2021. 10.14324/111.9781787356856.

Denham, Andrew, and Mark Garnett. "The Nature and Impact of Think Tanks in Contemporary Britain." *Contemporary British History* 10, no. 1 (March 1996): 43–61. 10.1080/13619469608581367.

Don't Spy on Us. "Don't Spy on Us | Investigatory Powers Bill: How to Make It Fit-for-Purpose." Accessed January 1, 2023. https://www.dontspyonus.org.uk/blog/2016/02/26/investigatory-powers-bill-how-to-make-it-fit-for-purpose/.

Don't Spy on Us. "Don't Spy on Us | Our Campaign." Accessed September 10, 2022. https://www.dontspyonus.org.uk/our-campaign.

Elsasser, Shaun W., and Riley E. Dunlap. "Leading Voices in the Denier Choir: Conservative Columnists' Dismissal of Global Warming and Denigration of Climate Science." *American Behavioral Scientist* 57, no. 6 (June 1, 2013): 754–776. 10.1177/0002764212469800.

Feldstein, Mark. "A Muckraking Model: Investigative Reporting Cycles in American History." *Harvard International Journal of Press/Politics* 11, no. 2 (April 1, 2006): 105–120. 10.1177/1081180X06286780.

Gellman, Barton. *Dark Mirror: Edward Snowden and the American Surveillance State*. New York: Penguin Press, 2020.

Gill, Peter. "Evaluating Intelligence Oversight Committees: The UK Intelligence and Security Committee and the 'War on Terror.'" *Intelligence and National Security* 22, no. 1 (February 1, 2007): 14–37. 10.1080/02684520701200756.

Hartig, Hannah, and Carroll Doherty. "Two Decades Later, the Enduring Legacy of 9/11." *Pew Research Center - U.S. Politics & Policy* (blog), September 2, 2021. https://www.pewresearch.org/politics/2021/09/02/two-decades-later-the-enduring-legacy-of-9-11/.

Higgott, Richard, and Diane Stone. "The Limits of Influence: Foreign Policy Think Tanks in Britain and the USA." *Review of International Studies* 20, no. 1 (January 1994): 15–34. 10.1017/S0260210500117760.

Hillebrand, Claudia. "The Role of News Media in Intelligence Oversight." *Intelligence and National Security* 27, no. 5 (October 1, 2012): 689–706. 10.1080/02684527.2012.708521.

"How Edward Snowden Escalated Cyber War With China." Accessed September 12, 2022. https://www.csis.org/news/how-edward-snowden-escalated-cyber-war-china.

Kilian, Crawford. "Why Edward Snowden Chose Glenn Greenwald." *The Tyee. The Tyee*, May 30, 2014. https://thetyee.ca/Books/2014/05/30/No-Place-to-Hide/.

Landert, Daniela, and Gianluca Miscione. "Narrating the Stories of Leaked Data: The Changing Role of Journalists after Wikileaks and Snowden." *Discourse, Context & Media* 19 (October 2017): 13–21. 10.1016/j.dcm.2017.02.002.

Lanosga, Gerry. "The Power of the Prize: How an Emerging Prize Culture Helped Shape Journalistic Practice and Professionalism, 1917–1960." *Journalism* 16, no. 7 (October 1, 2015): 953–967. 10.1177/1464884914550972.

Lanosga, Gerry, and Jason Martin. "Journalists, Sources, and Policy Outcomes: Insights from Three-plus Decades of Investigative Reporting Contest Entries." *Journalism* 19, no. 12 (December 1, 2018): 1676–1693. 10.1177/1464884916683555.

Lashmar, Paul. "No More Sources?: The Impact of Snowden's Disclosures on Journalists and Their Confidential Sources." *Journalism Practice* 11, no. 6 (July 3, 2017): 665–688. 10.1080/17512786.2016.1179587.

Lebaron, Frédéric. "Symbolic Capital." In *Encyclopedia of Quality of Life and Well-Being Research*, edited by Alex C. Michalos, 6537–6543. Dordrecht: Springer Netherlands, 2014. 10.1007/978-94-007-0753-5_2961.

Leon-Reyes, Bernardino. Interview with former staffer, US Senate (US), n.d.

Leon-Reyes, Bernardino. Interview with journalist, national security beat (US), January 11, 2021.

Leon-Reyes, Bernardino. Interview with Paul Lashmar (UK), January 26, 2021.
Leon-Reyes, Bernardino. Interview with CIA whistleblower (US), November 17, 2022.
Leon-Reyes, Bernardino. Interview with Barton Gellman (US), March 23, 2022.
Leon-Reyes, Bernardino. Interview with Senior Manager, Media, EFF (US), December 21, 2022.
Leon-Reyes, Bernardino. Interview with Senior Manager, Strategy, EFF (US), November 29, 2022.
Leon-Reyes, Bernardino. Interview with former activist, Senior Manager (UK), September 2, 2023.
Leon-Reyes, Bernardino. Interview with senior journalist and civil society actor (US), January 19, 2023.
León-Reyes, Bernardino. 'Towards a Reflexive Study of Intelligence Accountability'. In *Problematising Intelligence Studies: Towards A New Research Agenda*, 30–47. Routledge, 2022. 10.4324/9781003205463-3.
Liepman, Andrew. "What Did Edward Snowden Get Wrong? Everything." August 12, 2013. https://www.rand.org/blog/2013/08/what-did-edward-snowden-get-wrong-everything.html.
Lyda, Alex. "Edward Snowden Is More Narcissist than Patriot." chicagotribune.com, 2014. https://www.chicagotribune.com/opinion/commentary/ct-snowden-cia-citizenfour-oscars-korea-perspec-1225-jm-20141223-story.html.
Mair, Peter. *Ruling the Void: The Hollowing of Western Democracy*. Place of publication not identified: Verso, 2013.
Mc Cluskey, Emma, and Bernardino Leon-Reyes. Interview with Former Senior Manager, Privacy International (UK), May 20, 2021.
McNair, Brian. "JOURNALISM AND DEMOCRACY: An Evaluation of the Political Public Sphere," n.d., 217.
Moran, Jonathan. "The Role of the Security Services in Democratization: An Analysis of South Korea's Agency for National Security Planning." *Intelligence and National Security* 13, no. 4 (December 1, 1998): 1–32. 10.1080/02684529808432503.
Mukasey, Michael B. "Leaking Secrets Empowers Terrorists." *WSJ*, June 9, 2013. http://online.wsj.com/article/SB10001424127887324634304578535492421480524.html.
Ochoa, Christopher Smith, Frank Gadinger, and Taylan Yildiz. "Surveillance under Dispute: Conceptualising Narrative Legitimation Politics." *European Journal of International Security* 6, no. 2 (May 2021): 210–232. 10.1017/eis.2020.23.
Park, Robert E. "The Natural History of the Newspaper." *American Journal of Sociology* 29, no. 3 (1923): 273–289.
Pautz, Hartwig. "New Labour in Government: Think-Tanks and Social Policy Reform, 1997–2001." *British Politics* 6 (June 1, 2011): 187–209. 10.1057/bp.2011.9.
Pillar, Paul R. "Snowden's Treason." *Brookings* (blog), November 30, 1AD. https://www.brookings.edu/opinions/snowdens-treason/.
Protess, David L., Fay Lomax Cook, Jack C. Doppelt, James S. Ettema, and Margaret T. Gordon. *The Journalism of Outrage: Investigative Reporting and Agenda Building in America*. New York, 1991.
Putnam, Robert D. *Bowling Alone: The Collapse and Revival of American Community*. New York: Simon & Schuster, 2000.
Ricci, David M. *The Transformation of American Politics: The New Washington and the Rise of Think Tanks*. New Haven, 1993.

Rollings, Neil. "Cracks in the Post-War Keynesian Settlement? The Role of Organised Business in Britain in the Rise of Neoliberalism Before Margaret Thatcher." *Twentieth Century British History* 24, no. 4 (December 1, 2013): 637–659. 10.1093/tcbh/hwt005.

Romesh, Ratnesar. "The Unbearable Narcissism of Edward Snowden." *Bloomberg.Com*, November 1, 2013. https://www.bloomberg.com/news/articles/2013-11-01/the-unbearable-narcissism-of-edward-snowden.

Rossi, Agustín. "How the Snowden Disclosures Saved the EU General Data Protection Regulation." *The International Spectator* 53, no. 4 (October 2, 2018): 95–111. 10.1080/03932729.2018.1532705.

Schlesinger, Philip. "Creativity and the Experts: New Labour, Think Tanks, and the Policy Process." *The International Journal of Press/Politics* 14, no. 1 (January 1, 2009): 3–20. 10.1177/1940161208328898.

Schmidt, Vivien A., and Mark Thatcher. "Why Are Neoliberal Ideas so Resilient in Europe's Political Economy?" *Critical Policy Studies* 8, no. 3 (July 3, 2014): 340–347. 10.1080/19460171.2014.926826.

Scott, Katherine A. *Reining in the State: Civil Society, Congress, and the Movement to Democratize the National Security State (1970–1978)*. Temple University, 2009.

Shafer, Jack. "Edward Snowden and the Selective Targeting of Leaks." *Reuters News*. June 12, 2013. http://global.factiva.com/redir/default.aspx?P=sa&an=LBA0000020130612e96c000q6&cat=a&ep=ASE.

Skocpol, Theda. *Diminished Democracy: From Membership to Management in American Civic Life*. The Julian J. Rothbaum Distinguished Lecture Series, v. 8. Norman: University of Oklahoma Press, 2003.

Tamames, Jorge. *For the People Left Populism in Spain and the US*. London: Lawrence & Wishart, 2020.

Toobin, Jeffrey. "Edward Snowden Is No Hero." *The New Yorker*, 2013. https://www.newyorker.com/news/daily-comment/edward-snowden-is-no-hero.

Tréguer, Félix. "Intelligence Reform and the Snowden Paradox: The Case of France." *Media and Communication* 5, no. 1 (March 22, 2017): 17–28. 10.17645/mac.v5i1.821.

Wahl-Jorgensen, Karin, Lucy Bennett, and Gregory Taylor. "The Normalization of Surveillance and the Invisibility of Digital Citizenship: Media Debates After the Snowden Disclosures." *International Journal of Communication* 11, no. 0 (February 14, 2017): 23.

Wahl-jorgensen, Karin. "Playground of the Pundits or Voice of the People? Comparing British and Danish Opinion Pages." *Journalism Studies* 5, no. 1 (February 2004): 59–70. 10.1080/1461670032000174747.

Weidenbaum, Murray. "Measuring the Influence of Think Tanks." *Society* 47, no. 2 (March 2010): 134–137. 10.1007/s12115-009-9292-8.

Weller, Geoffrey R. "Political Scrutiny and Control of Scandinavia's Security and Intelligence Services." *International Journal of Intelligence and CounterIntelligence* 13, no. 2 (April 1, 2000): 171–192. 10.1080/08850600050129709.

6 Transversal intelligence oversight in the United States

Squaring the circle?

Arnaud Kurze

Introduction

Under the leadership of Robert Mueller, then director of the Federal Bureau of Investigation (FBI), members of his agency were allegedly pulled from the CIA blacksite interrogations in the aftermath of the 9/11 terrorist attacks after reports of torture surfaced. Mueller publicly stressed having rung internal alarm bells informing the Department of Justice (DOJ) when he was questioned during a public hearing at the House of Representatives in relation to torture practices in 2008.[1] More recent reporting, however, has cast doubts on the cleanliness approach taken by the agency.[2] This example underlines the intricate web of entangled cooperation between intelligence agencies in the United States. It accentuates the extent to which mutual accusations of human rights violations lack oversight authority that can verify these claims thus effectively hiding them from the public eye because of the lack of access to intelligence information.

In this chapter, I explore the multifaceted US intelligence oversight issues as part of a larger endeavor to understand the continuing leadership impunity in liberal democracies against the backdrop of illegal practices, including torture and breaches of privacy. In order to do so, it is fundamental to lay out the concept of oversight in the historical and political context of the United States, particularly congressional practices. In association with this, it is helpful to inquire about the different roles and rules of stakeholders within different institutional structures to better grasp the challenges in relation to existing oversight mechanisms. I lay out a conceptual framework that underscores the need for transversal analysis based on the multilayered stakes and actors involved in the decision making process.

Relying on different empirical evidence, I illustrate that despite the intricate institutional framework and unwritten rules and practices between oversight advocates and the intelligence community, transversal legal advances in an increasing number of court cases prove potentially powerful to fuel accountability and fight impunity. While the normative and legislative changes for transnational change remain uncertain in the short term, they are

DOI: 10.4324/9781003354130-7

nonetheless a formidable stepping stone in tandem with other, existing forces at play, including external actors, such as the media.

To explore the intricate oversight issues with respect to intelligence in the United States, the paper first lays out a framework of transversal oversight. It then problematizes some basic concepts and offers a mapping of past congressional oversight practices. In connection with this, I review challenges faced by Congress and critically look at the institutions involved in oversight as well as engaged stakeholders and their practices. Drawing from this initial topographical mapping, I point to the transversal character of oversight politics. I then employ a transversal oversight perspective to analyze a number of empirical cases to further our understanding of actors, practices, and norms of intelligence and security oversight.

Introducing transversal oversight and methodological considerations

Large parts of the social capital of Anglo Saxon intelligence studies have been made up by scholars with close ties to the intelligence community,[3] forming an almost symbiotic relationship. One of the principal challenges of such a knit-tight collaborative approach is the limited disciplinary perspective that is applied when scrutinizing intelligence practices and ultimately tackling oversight issues on the ground. Yet other disciplinary approaches, including anthropology, critical cultural theory, feminist theory, international political sociology, or postmodern theory provide important insights that could further our knowledge of intelligence studies. Such knowledge, such center specifically, but not exclusively on questions such as: "(a) how intelligence is used to insulate public officials from accountability and security institutions from democratic control; (b) how national security decision-making becomes centralized in the hands of elites at the expense of congressional and public debate; (c) how intelligence activities interfere with legitimate democratic processes; and (d) how the economic imperatives of intelligence contractors distort public policy and shape understandings of security threats."[4] As these questions and above theories address broader issues of power, control, and domination, they offer a formidable roadmap for advancing contemporary theories in the field.

A transdisciplinary perspective underlying any scholarly efforts to produce timely knowledge on transnational and global intelligence and security issues is therefore fundamental.[5] This undertaking requires an active engagement of a multitude of approaches and voices from different academic disciplines. Moreover, contemporary challenges require us to seek tools that are not only reactionary to trends in the field but provide analytical depth to undo some of the existing doxas by practitioners and scholars alike,[6] and to highlight the multitude of layers, political, institutional, and relational that stakeholders are confronted with.

To help capture these differences in terms of positioning, identity, and values, I suggest drawing from a transversal perspective. While conventional

research has struggled to overcome fragmentations due to the multiple levels of analysis and efforts to differentiate the internal from the external, a growing current of scholars has urged pushing beyond disciplinary boundaries in favor of transdisciplinarity.[7] In this context, some have also argued to go beyond traditional notions of transnational politics, which separate actors, nation-states, and other institutions into fragmented categories. Instead, it is more useful to abandon a transnational framework in favor of exploring and underlining transversal practices in the field.

Such a conceptual shift helps better capture and understand the interdependencies between different stakeholders. As Didier Bigo put it, the latter "deploy and (re)construct chains of interdependencies and fields of power by opening new connections – violent or not – or by trying to reinforce boundaries, not necessarily territorially at the state borders, but through management at a distance of suspicion and use of digital technologies."[8] This begs the question to what extent examining transversal lines of inquiry might fuel new insights by resisting "entrenched categorisations" affirming "an idealized and even nostalgic view of social and political orders?"[9] The answer lies in thinking of these transversal lines "as fracturing the bureaucracies themselves to find the set of dispositions of groups in relations, inside these bureaucracies, which drive them toward solidarities at a distance and enmity in proximity."[10]

Here it is helpful to recall the relation between individuals and large groups, notably in disciplinary societies. Drawing on Gilles Deleuze's notion of "dividuum," an individual does not form a bipolar pair vis-a-vis a group of individuals or a mass.[11] According to Deleuze, "power individualizes and masses together, that is, constitutes those over whom it exercises power into a body."[12] In terms of intelligence services, this creates bodies molding "the individuality of each member of that body."[13]

In juxtaposition to the the concept of dividuality, the notion of transversal politics as conceptual and political differentiation is of use to capture the concept of transversality laid out in this work.[14] Leaders in social groups or networks, for instance, do not necessarily represent their entire constituency and do not always have to be an integral part of the community.[15] This is not only true at the grassroots level but also visible in international politics, particularly with regard to diplomatic matters and actors. A dinner party, for instance, hosted at an ambassador's residence is generally considered an ideal setup for diplomatic negotiations by diplomatic standards. "As transversal actors, diplomatic partners are found to occupy a social realm, which straddles both private and public spheres, and to have effects within this realm on state-to-state politics."[16]

For the purposes of this piece, I build on this theoretical backbone to elaborate on a selection of empirical illustrations to help us understand the politics of oversight through a transversal lens. In order to do so, I rely on qualitative methods based on content analysis.[17] My empirical research draws on three instances some of which are based on legal cases. The examples were

selected to emphasize common challenges across cases and the transversal characteristics of stakeholder practices in seeking intelligence access and overview.[18]

Navigating Pandora's box of intelligence oversight

To grasp the multifaceted oversight issues with respect to US intelligence and transnational practices, it is initially helpful to discuss some basic concepts before providing an historical overview of the predominant oversight mechanisms carried out by Congress. Following this initial survey, I lay out some of the congressional dilemmas and examine stakeholders, institutions, and practices. By connecting the epistemological underpinnings of statecraft and the political sociology of law, I highlight the transversal nature of oversight politics. Based on this mapping, I lay out a theoretical foundation for a transversal oversight perspective to help further our knowledge of challenges associated with oversight practices and processes.

At the core of the problem lies the concept of state secrecy in democracies. As the democratic process requires transparency and scrutiny in order to account for abuses, the lack of publicity (legitimately) claimed by governments thus poses a dilemma that, according to Rahul Sagar, can only be solved by "*circumvention* [sic] (commonly referred to as 'leaking')."[19] This, in turn, requires a significant reliance on "private institutions and personal virtues."[20] While transparency can be blocked by secrecy, scrutiny is harder to circumvent. Public scrutiny therefore is facing the veil of secrecy in the name of the reason of state. My work will further scrutinize individual actions with regard to intra- and inter-institutional dynamics between stakeholders, notably members of the intelligence community and congressional representatives. Accountability and, respectively, impunity are consequently deeply rooted in institutionalized practices that form the foundation for the continuingly challenging idea of intelligence oversight.

Closely related to secrecy is the notion of intelligence as statecraft. "Although intelligence may or may not be the world's second oldest profession, it has long been a key instrument of national statecraft and even survival."[21] Inevitably, tensions arise between basic democratic principles, such as transparency and accountability, and the government's claim to withhold information often on the basis of national security. Here, one more distinction proves helpful for our broader understanding of the key stakes at hand. Traditionally, a state-centric definition of security refers to "the security of the state, including matters of territorial integrity and control, political autonomy, and absence of war, as well as the ability to counter suberversive activities by foreign states or terrorists."[22] Whereas the definition of intelligence has sparked much debate, according to Njord Wegge, three elements are key: "the acquisition, or use of information for decisionmakers; a connection to state security or state power; and assumptions or facts about the behavior, beliefs, capabilities or intentions of the other."[23]

With these premises in mind, let us now turn to the principle of oversight in the US context. While the term itself is very broad, it has nonetheless a specific meaning worthwhile exploring historically and culturally. It is also noteworthy that it does not specify the timeframe of when the control occurs, including ex-ante (before), during, or ex-post (after) periods of when an activity takes place. Neither does it distinguish between internal and external control mechanisms. According to Marvin Ott,

> oversight tends to pragmatically include both internal control conducted by personnel from within the services (for example, in the U.S., the Office of the Inspector General in the Central Intelligence Agency or the Federal Bureau of Investigation), as well as systems where external bodies scrutinize or inspect the services.[24]

For the purposes of our analysis, intelligence oversight includes all three temporal possibilities but focuses on the external control function. They tend to be independent from "both the executive branch and the services themselves in the daily work and line of reporting."[25]

A mapping of US intelligence oversight

From a historical perspective, the development of US oversight practices falls within four broad phases, dating back to the post-1945 period.[26] In the aftermath of World War II and the emerging Cold War the US Congress created the Central Intelligence Agency (CIA), the successor of the Office of Strategic Services (OSS), and the immediate question to be answered centered around how Congress would oversee this newly created, secretive body?[27] The initial answer was "to vest the authority in subcommittees of the Armed Services Committees of the House and Senate."[28] Yet practice this setup resulted in a very restricted oversight authority with minimal control. This changed in the early 1970s with CIA covert operations, including supporting the coup against the democratically elected socialist Salvador Allende government.[29] As a result, Congress established two investigatory committees in the House and Senate, the Pike and Church committees, respectively, which had broad authority to examine intelligence activities.[30]

The revelations came shortly after the Watergate scandal, leading to the resignation of President Richard Nixon and the ascension of Gerald Ford – the only nominated, not elected, Vice President in US history – to the highest executive office. In a compromised position, President Ford could not afford to appear weak, aggressively impeding the work of the Congressional committee under the leadership of New York Representative, Otis Pike.[31] The administration ceased to supply documentation to the committee and Secretary of State Henry Kissinger pushed for unconditional secrecy, leading newspaper editorials, such as the *New York Times*, to compare the actions by the executive branch to neo-Mccarthyist politics.[32]

Eventually, the findings of the published Church report helped create the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI) in 1976 and 1977. The next phase consolidated the consumption of intelligence information by Congress, leading to the committees' jurisdiction over intelligence oversight by 1980. More importantly, however, the relationship between the oversight committees and the intelligence community – notably what intelligence would be provided and other basic ground rules – developed "through agreement and practice rather than legislation and regulation."[33] During the 1980s, generally considered the third phase as well as the golden age, "a fair degree of mutual trust and respect animated these institutional interactions."[34] No serious leaks emanated from the legislative branch, one of the major concerns of the intelligence community and a relative nonpartisanship reigned during this period. Interestingly, SSCI staff occupied a remarkable number of very senior intelligence community positions, including the Director of Central Intelligence, the CIA Inspector General, and the Deputy Assistant Secretary of Defense (Intelligence), to name only a few. This, however, changed in the 1990s with an increasing politicization of oversight practices and partisanship.[35] The 9/11 attacks in 2001 and the subsequent invasions of Afghanistan and Iraq led to the extraordinary renditions programs[36] and torture practices, further underlining the gaping lack of oversight practices.[37] As a result, the Obama administration switches from HUMANINT to SIGINT practices in the aftermath of the torture scandals. The extraction of information is shifted from humans to the computer and legitimizes the intelligence information gathering at a new level.

In 2013, an NSA contractor, Edward Snowden, leaked classified documents exposing the malpractice especially in view of his employer, adding to the list of agencies in the crossfire. One could wonder to what extent some of these issues also are home to the Defense Intelligence Agency (DIA), an agency within the US Department of Defense, specializing in defense and military intelligence. Yet due to the often classified nature of DIA's work publicly available document stress the effectiveness of internal oversight[38] and issues reported to Congress have been limited to internal mismanagement or fraud.[39] While the Snowden scandal forced the Obama administration to take actions to address accountability and oversight issues with respect to the NSA, these steps were taken against the backdrop of defending existing mechanisms[40] and the legality of the agency's work.[41] To counter this, the administration sought to rely on the investigative work of the Privacy and Civil Liberties Oversight Board (PCLO)[42], an independent body inside the executive branch. Yet skepticism arose not only because of the presidential appointing mechanism, but also because it was little functional at the time of the revelations.[43]

Cultural factors also play a role in how oversight is carried out. Referring back to the revolving door effect between subcommittee members and senior-level intelligence positions in the executive branch earlier, it is also essential to point out the close ties between academe and the intelligence

community. As certain scholars have underlined, "some of the leading figures in intelligence studies are former American intelligence officials and that US intelligence agencies often rely on specialists from academe."[44] In fact, "US intelligence agencies actually seek the expertise and advice of the academic community to enhance their analysis and to understand their mistakes."[45] This is not only true for experts and specialists at higher education establishments, but also research institutions, such as think tanks.[46] It is part of a privatization and outsourcing strategy that has linked intelligence services with the private sector for quite some time now.[47] The intelligence service culture and question of outsourcing varies from country to country.

The 2022 war in Ukraine, for instance, sparked a public debate of increasing Germany's defense budget due to the imminent national security threat. If this trend persists, it might ring in a new era in German defense and foreign policy, generally referred to as "Zeitenwende (or turning point)."[48] This illustrates the conundrum associated with implementing intelligence oversight, as intelligence services generally are reluctant to outside oversight and compete against other services.[49]

The rule of law and congressional oversight dilemmas

The above observations call for further scrutiny of the legal mechanisms in place to provide intelligence oversight in line with democratic principles, including transparency and accountability. One may wonder whether the relationship between Congress and the intelligence community should be characterized as confrontation or collaboration?[50] Often the issue is not caused by a lack of allowing some form of control, but instead, it lies in the lack of required expertise or technical knowledge to address the problem in question. The Foreign Intelligence Service Act (FISA)[51] Amendment of 2008, for instance, highlights the "difficulties Congress faces when trying to modify intelligence legislation. Members, for reasons of classification or technical complexity, did not share a common understanding of the law, let alone how it should be adjusted."[52] This problem emerged much earlier. The need for deeper knowledge and understanding of the subject matter can already be found in one of the key 2004 recommendations by the 9/11 commission after the intelligence failures in connection with the 9/11 terrorist attacks. The commission suggested abolishing subcommittee members' term limits to "build their expertise to enhance their oversight abilities," which Congress implemented in 2005.[53]

Review practices of the intelligence community are thus often relying on administrative regulations that serve as a veil, obstructing transparency and increased participation from lawmakers. The FISA Court (FISC), which was established under the 1978 Act as a federal court, further accentuates this dilemma. Its reliance on administrative rules to gauge the reasonableness of Fourth Amendment decisions[54] has led to calls for institutional reforms. More precisely, by empowering, for instance, the PCLOB, rulemaking by the intelligence community would become more transparent and participatory.[55]

The unhinged administrative power of intelligence practices and the trust from review mechanisms became particularly evident in the aftermath of the Edward Snowden revelations. FISC became aware of the National Security Agency (NSA) practices of upstream data collection[56] that "wholly unrelated communications involving US persons or persons inside the United States were getting swept up in these multiple communications transactions as well."[57] The court questioned the motives behind broad sweeping data collection by the NSA, which led the latter to eventually revise some of its procedures. Yet the incident also highlights the continuing risks of institutional proximity among stakeholders and an ex-post review mechanism built on insider understanding of administrative and institutional processes. Intelligence, here in the form of collected data, becomes a form of knowledge that is produced by the relevant agency, thus creating, according to some, "knowledge regimes."[58] While they continue to be shaken with leaks, affairs, or scandals, these events do not fuel transformative changes or reforms. Quite the contrary. Some have gone further, pointing to the impact of "non-knowledge" in view of governing intelligence-related activities, such as border control.[59] More specifically, they point to the power constellations and subjectivities emerging from the "unknowns" and the effects of authority-driven errors on the fate of migrants. "Errors are part of processes of making true and objective knowledge, even when they emerge out of subjective failures."[60] These observations lead to the conclusion that the practices implemented by intelligence services follow a regime of justification. Intelligence services are in fact creating an amnesia of arbitrariness.

Furthermore, the House and Senate subcommittees's oversight power limitations are rooted in congressional practices of dividing the authorization and appropriation authorities. In other words, appropriations for intelligence activities are often integrated as a "classified section of the defense appropriation bill, meaning that the real control over the intelligence lies with the defense subcommittees of the House and Senate Appropriations Committees."[61] As intelligence budgets are only a fraction of the defense budget, members of the defense subcommittees generally give it very little attention due to other larger defense spending concerns.[62] More so, "the intelligence committees have exclusive authorizing jurisdiction over only a small portion of the overall intelligence community […] and share authorization jurisdiction for the other intelligence agencies with the relevant standing committees."[63] Reflecting on congressional jurisdiction regarding oversight matters begs the question of the role played by the judiciary in this context.

Judicial oversight practices and challenges

While there is no stipulation in the US Constitution that prevents judicial review of security matters of our nation, the courts have not expanded their jurisdiction to the same extent as Congress has on these matters. Compared to Congress, the judiciary has traditionally expressed more reluctance in the

past to investigate breaches in regard to intelligence matters, as some have found. Some have pinpointed the causes of judicial absence to the early (in) famous 1803 ruling in *Marbury* v. *Madison*, which "allows the judiciary to express no opinion on matters that it feels are better left to be worked out by the other branches of government."[64] Although this watershed moment cemented the power of the judiciary with respect to the executive and legislative branches in US history, it limited the scope of judicial review particularly in the area of national security and intelligence. Courts have nonetheless weighed in on a number of cases, including rulings on the rights for citizens who were detained as enemy combatants or Fourth Amendment rulings based on FISA.[65] From a legal perspective, rethinking judicial oversight, however, remains problematic. The Constitution "does not expressly authorize the judiciary to create investigative bodies or to review security politics outside a trial."[66] That said, development points to an urge of envisioning new forms of review procedures that allow for a greater role of the judiciary in these processes.[67]

Interestingly, the origin of this reluctant behavior is not the notion of secrecy, which would hamper any court's ability to receive classified information and therefore impede any proper functioning of the judicial process.[68] In part, because the Classified Information Procedure Act (2012) now facilitates court's handling of classified information during public trials. Courts, however, are politicized institutions, despite relentless efforts to showcase the contrary. The FISC, mentioned above for instance, oversees requests for surveillance warrants against foreign spies inside the United States by federal law enforcement and intelligence services. Yet the bulk of its work could best be described as judicial oversight on details and not on substantive matters. The rejection rate of warrants in over three decades since its inception until 2012 including over 15,000 requests added up to merely a dozen of cases.[69]

Aside from the FISC, US district courts, trial courts of the federal judiciary, have also seized cases on intelligence matters, as long as they pertain to questions of federal law or federal crimes. Unlike the Supreme Court, which was established based on Article III of the US Constitution, district courts, reminiscent of FISC, were mandated by Congress under the Judiciary Act of 1789. Rulings of district courts can be appealed at the US courts of appeals that are in the same federal circuit as the ruling district court. A couple of empirical examples will help illustrate the tensions and challenges emanating from the work of the courts.

The Snowden case is telling in this context. In June 2013, US federal prosecutors filed a criminal complaint with a court in the Eastern district in Virginia, where Snowden's former employer, Booz Hamilton is located, shortly after the leaks were made public.[70] Given that Snowden is currently still residing in Russia (he was given permanent residency in 2020), he never appeared in a courtroom. The 1917 Espionage Act, which served as basis for the criminal complaint, does not address leaking and information sharing based on not-for-profit driven motivations.[71] Others have further investigated

the legal frameworks in view of public leaks of classified information and pointed to loopholes and a remaining open question with regard to the First Amendment Right by the media or press vis-à-vis state secrecy.[72]

Yet another example of the judicial intricacies concerns the Syrian-Canadian, Maher Arar, a dual citizenship holder. Confined in the US in 2002 after a trip to Tunisia on his way back to Canada, the US government did not release him to Canada, but to Syria, where he was held and tortured for one year. Canadian courts ruled on his behalf and the Harper government paid over 8 million US dollars and formally apologized to Arar for the wrongdoings.[73] The US Supreme Court, however, refused to hear the case in 2010.[74] Other filings brought by advocacy groups or human rights organizations to plead cases of violations by the US government in terms of intelligence matters include, for instance, *Jewel* v. *NSA*,[75] but which was also dismissed by the US Supreme Court in 2022.

These cases underscore the politicized and intricate challenges of the judiciary with respect to intelligence issues on the ground. These limits of the courts are further accentuated by the fact that the Executive branch has the power to nominate federal judges, confirmed by the Senate. And consequently, this raises a substantive question of judicial oversight on intelligence matters. Given the focus on penal-related outcomes to condemn wrongdoings, which then turns into a struggle over impunity, it dodges the fundamental question at the core of this chapter, namely, the independent, adequate oversight of intelligence. Once again the basic framework and institutional objectives are at odds with the practices addressed here.

Understanding intelligence stakeholders, institutions, and practices

The above observations invite us to further explore some of the concerns, practices, and challenges faced by stakeholders in the field. It also provides an excellent opportunity to reflect on conceptual advances in the field, notably efforts to formulate an intelligence theory and assess the ramifications and difficulties associated with it. A concern often raised within the intelligence community that justifies their skepticism vis-à-vis lawmakers is the politics of irrational intelligence oversight.[76] According to research data, interviewed members of the intelligence community see "parliamentary oversight committees as less reliable than appointed expert bodies in so far as being able to keep matters secret and not utilizing classified information for political gain."[77] From a policymaker perspective, there is an information disadvantage between congressional committees and the executive branch in addition to "Gerrymandered jurisdictional lines" committees have to maneuver and partisanship issues.[78] In the view of some, this leads to the question of efficiency in terms of overview models, which could be described as "police patrols" versus "fire alarms" oversight.[79]

The former relies on standing committee work, which, in a centralized and direct manner, examines specific operations carried out by the executive branch.

The latter, in contrast, is decentralized and indirect. Monitoring thus occurs through a set of rules and informal practices in which individuals and interest groups report breaches or violations of the ground rules. The real question here, however, is whether there is a debate about hierarchical control. This is important because in a hierarchical structure inquiries and investigations about violations, rule breaking, and abuse of intelligence services are met with the obligation of the latter to answer. In the absence of such a structure, the pressure to receive answers and exert control over the intelligence services diminishes.

Despite Congress' power of the purse to press for access to information in this context, the Administration may use political leverage to foil any congressional attempts to force oversight. Moreover, US intelligence services have been referred to as a "cottage industry," in other words, a system of subcontracting work due to its extended reach and hundreds of thousands of individuals who work in the field.[80] Consequently, as James Baker sharply notes, "the intelligence community is vast and congressional staffs are small, no matter how experienced and professional they may be."[81] The human capital limitations and the changing intelligence landscape urge us to rethink not only oversight mechanisms themselves but also how we study, assess, and understand them.[82]

The capability of oversight mechanisms, notably legislative frameworks, to change and undergo appropriate reform in the event of substantial changes of intelligence practices constitutes another key concern of decision makers in democracies. The multilayered nature of review processes – including vertical, horizontal, and a third (international) dimension[83] – complicates timely regulatory adjustments or legislative reforms. Yet the blurred lines and transversal nature of individual relationships across different institutional boundaries also allow for innovation to occur if the oversight reaches the intelligence community as a whole rather than being fractured.[84]

Consequently, if specialized oversight mechanisms or practices are in place, there is still a need for communication and coordination between various oversight types. This is crucial in terms of fueling effective national and transnational oversight. Fractured and specialized forms of oversight too often get drowned in details and the big picture of an issue or wrongdoing is lacking. As an example, if there is an issue involving multiple intelligence services, but only one of the services is investigated, the full extent of the story is difficult to fathom. In addition, it downplays struggles and tensions between services that may exist.

One of the positive effects based on increasing leaks, litigation, and a growing volume of domestic laws and regulations is "peer constraints," which could best be described as oversight-fueling effects by the intelligence community of another country, and more rights-protective intelligence practices.[85] In this context, foreign intelligence in the digital age and across cyberspace has increasingly gained traction and scholarly attention.[86]

One may rightly wonder where all this leaves us with efforts to craft a broader intelligence theory? The emerging field was quickly dominated by US

intelligence studies, as scholars gathered at the International Studies Association (ISA) meeting in Montreal in 2004 and subsequently, in a 2005 workshop organized by the global nonprofit think tank RAND Corporation to define intelligence more precisely.[87] Yet researchers and scholars from other disciplines and world regions also dedicated time and resources to these questions already prior to these gatherings, including advocates of international political sociology. A few key takeaways are noteworthy here. They include the need to continue defining intelligence in the light of changing information collection, national and global threats, and security concerns. In addition, instead of conceptually focusing on organizations, actors, and institutions, the process character of intelligence is essential to capture changing conditions, contexts, and relational dynamics between stakeholders, as well as scrutinize alternative, non-state actors more accurately in the field given their increasing roles.[88]

The Pegasus scandal is an excellent case in point. It involved an Israeli cyber-arms company, NSO Group, and its mobile phone spyware of the same name, developed, according to the firm, for criminal and national security investigations only. Yet human rights activists and media disclosed that it was used not only to spy on dissidents in autocratic regimes with the knowledge of the Israeli government,[89] but also to surveil citizens in democratic nations, including Europe.[90] Now, I will explore and scrutinize more recent intelligence oversight practices in the United States and beyond.[91]

Contemporary intelligence oversight struggles in the US context

As laid out earlier, US oversight efforts face three principle challenges, which I explore with empirical samples below. First, the transversal positioning of stakeholders involved in intelligence matters is a double-edged sword. While it carries the potential for review and whistleblowing, more often compliance with internal rules and practices diminish the oversight capacity. In association with the first issue are institutional prerogatives and practices, shielding responsible individuals from accountability requests. Last, hurdles are also rooted in the legal dimension of fueling oversight that entails accountability and an end of impunity. Addressing these challenges across the selected cases will help us better understand the complex issues and point to potential silver linings on these issues. Listing the present oversight mechanisms across some of the main intelligence services in the United States in the form of a table below, I hope to provide an overview of current oversight struggles and underline services that have received less attention in the media.

Overall, each one of the larger intelligence services (there is a total of 18 services)[92] has their own internal inspector general (IG) who carries out investigations and audits on the intelligence activities under their purview. The IGs's responsibilities have been codified in the Inspector General Act (1978) and have been amended over time.[93] The most important reforms include, for instance, the creation of the Council of Inspector Generals on

Integrity and Efficiency (CIGIE) (2008), which represents the unified council of all statutory IGs. In addition, the Inspector General Empowerment Act of 2016 ensures that "IGs are entitled to full and prompt access to agency records, thereby eliminating any doubt about whether agencies are legally authorized to disclose potentially sensitive information to IGs."[94] While these reforms showcase an Executive branch-driven effort to underline oversight efforts in light of a history of breaches and violations by the intelligence services, it is essential to underscore that the IGs remain presidentially appointed and Senate confirmed. This posed an issue recently under the Trump administration, when the President removed the federal government's internal watchdogs in 2016.[95] In light of these developments, Congress introduced a bill in March 2021 to limit the presidential powers of removing an IG (Table 6.1).[96]

These internal oversight mechanisms, however, have rightfully raised the question of "who watches the watchmen," which was also the title of an expert panel organized at the Wilson Center in the aftermath of the 2016 scandal.[98] In this context, it is worth noting that the 2014 Defense Intelligence Agency (DIA) sparked some media attention when the Pentagon scaled back "its plans to assemble an overseas spy service that could have rivaled the CIA in size," after lawmakers raised concerns about its goals and the price tag.[99] It further demonstrates the intra-intelligence services' struggle and competition over service-specific prerogatives and responsibilities in times when foreign policy matters encompass a plethora of challenges and risks.

From an oversight perspective, this begs the question as to what extent the DIA might also have been implicated in breaches and violations that have not garnered sufficient attention from the public eye. The Department of Defense drone strikes killing innocent civilians in Afghanistan in August 2021, which were revealed by the *New York Times* after a Freedom of Information Act lawsuit. Despite public scrutiny, steps by the US government to remedy the wrongdoing and establish procedures to account for the harm inflicted remain incomplete.[100] Let us here turn to a selection of various cases that further illustrate the oversight struggles.

Table 6.1 List of Major US Intelligence Services with International Scope and Oversight Mechanism[97]

Intelligence Service	*Internal Oversight Mechanism*	*Other Oversight*
National Security Agency (NSA)	NSA Office of the IG	Congress and Judiciary
Central Intelligence Agency (CIA)	CIA Office Office of the IG	Congress
Federal Bureau of Investigation (FBI)	DOJ Office of the IG	Congress
Defense Intelligence Agency (DIA)	DIA Office of the IG	Congress

The case of Abu Zubaydah and other Guantanamo detainees

Initially, we turn to the case of Abu Zubaydah, a Saudi Arabian national (also known as Zayn al-Abidin Muhammad Husayn), who is currently held by the United States in the Guantanamo Bay detention camp in Cuba. He was captured in Pakistan about 6 months after the 9/11 attacks and held in various CIA blacksites and part of the rendition program.[101] After the media pointed to the unlawful practices by the US intelligence services, the government transferred him, and other individuals held in custody since their capture, to Guantanamo Bay in 2005.[102] The long and unsuccessful legal battle, described by one of his defense lawyers, sheds light on the human tragedy.[103] The March 2022 opinion by the US Supreme Court[104] upholds the government's state-secrets doctrine and thus protects disclosure of any blacksite locations.[105] Yet the latter has also opened up avenues of legal probing, exploring alternatives to seek accountability and more so, engage in access to intelligence classified information to break the state secrecy veil. In October 2021, for instance, a US federal court passed a verdict on a different case, an Afghan detainee at Guantanamo, captured in 2007, ruling his detention unlawful. However, the "court does not have the authority to dictate how the government should comply," on the constitutional basis of separation of power. The release date of the prisoner is pending therefore caught in a slowly grinding bureaucratic process.[106]

A number of other court cases in jurisdictions outside the United States help us scope the power of normative transversal struggles. The European Court of Human Rights (ECHR), for instance, ruled on the Zubaydah case in a number of instances, condemning US military practices, CIA interrogation techniques and holding European governments accountable for assisting the US government in their efforts of illegal mistreatment.[107] The court established the legal liability of European governments, including Lithuania, Romania, and Poland. While the latter paid compensation to the victims, it has not fully complied in terms of investigatory requirements.[108] In addition, the court's jurisdiction precluded any liability of US government officials. This is nonetheless important as it constitutes the foundation and paves the road for any further inquiries into government impunity in view of breaches and violations.

Paradoxically, at the center of the debate in the United States case was not declassified intelligence information with incriminating evidence of torture practices of the claimant. Instead, the US Supreme Court's decision on the Zubaydah case in early March 2022 focused on the notion of state secrecy and the notion of trust. Justices, including Elena Kagan and Neil Gorsuch, insisted on the importance of secrecy in intelligence cooperation between the US government and foreign states.[109] Despite the constitutional victory for agencies, like the CIA, the broader impact of increasing case law against withholding intelligence information is affecting legal standards and judicial perceptions on who bears the responsibility under which jurisdiction. References of legal precedents, such as Supreme Court Justices did in their opinions with sentences of the ECHR solidify this emerging trend.

In this context, it is also important to elaborate on the transversal legal effects of the Zubaydah case in the United Kingdom (UK). A UK appeals court ruled that British intelligence agents who collaborated in the rendition program in some of the various locations[110] ought to be held accountable not as originally determined under the legal system in the location where the mistreatment occurred, but rather under English law.[111] Unlike some of the findings in a 2014 US Senate report stating that these secret locations are abroad and outside the US legal system,[112] the UK judge is creating a legal case for holding British intelligence and security (MI5 and MI6) accountable for "torts of misfeasance in public office."[113] Interestingly, Zubaydah's lawyer does not accuse the services directly, but allege

> that the UK intelligence services sent numerous questions to the CIA, to be used in interrogations of him for the purpose of attempting to elicit information of interest to them and without seeking any assurances that he would not be tortured or mistreated or taking steps to discourage or prevent such treatment.[114]

It remains to be seen to what extent this legal precedent further prepares the ground for other cases against not only UK cases, but reverberates across Europe and countries in which the rendition took place and eventually all the way back to the United States, where the nation's highest court has dealt a victory to the country's security services and confirmed the right to withhold information based on secrecy. Yet in some cases, as we will further examine below, while legal stipulations are at times in favor of information sharing, practices on the ground make the application of the law challenging.

Mueller report as an example of failed intelligence sharing despite the law

Here, we turn the attention to the lack of intelligence sharing against the backdrop of the release of a report written by special counsel Robert Mueller (mentioned in the introduction), a lawyer and government official who served as the sixth director of the FBI from 2001 to 2013. The report was the result of a bipartisan investigation with regard to Russian interference in the 2016 US presidential elections.[115] In sum, Mueller's task was to examine allegations of conspiracy or coordination between Donald Trump's presidential campaign and Russia, and allegations of obstruction of justice. Mueller submitted the report to the DOJ, headed by Attorney General William Bar at the time, in March 2019 and roughly a month later, the DOJ released a redacted version of the 700-page report.[116] The redactions were justified by Barr according to four categories, including grand jury materials, harm to ongoing criminal matters, personal privacy, and investigative techniques or other secret sources and methods of US government information collection.[117] In the weeks following the redacted release, President Trump made use of a temporary "protective assertion" of executive order to prevent the full report from being

shared with Congress. President Trump eventually won the legal battle when the Supreme Court upheld it with a decision in late May 2020.[118]

This episode is particularly revealing for two reasons. First, directly related to the court decision, it highlights the *raison d'être* of Barr's strategic objectives heading the DOJ, to further carve out executive powers, here through an executive privilege pretext through legal precedent.[119] This outcome does not bode well for advances with regard to intelligence oversight. But the incident also underlines the importance of using existing rules and norms against established practices, particularly if they are pushed by key stakeholders, such as the President or Attorney General. In fact, lawmakers missed a crucial opportunity, particularly the House Intelligence Committee – the Senate Intelligence Committee due to partisan reasons would have failed for political reasons[120] – to demand the full unredacted report to be shared with Congress. According to former general counsel of the Senate Intelligence Committee, Vicki Divoll, who served from 2001 to 2003,

> Federal law requires that the attorney general provide to the director of national intelligence any foreign intelligence information collected during a criminal investigation. Then the director must by law provide it to the intelligence committees of Congress — either by sending a notification or acting in response to a request from the committees. The director has an obligation to inform policymakers, including Congress, of intelligence assessments so that they can take steps to protect the American people.[121]

Ironically, it would have used the legal tools crafted under the Patriot Act[122] and made use of the national security doctrine to share foreign intelligence acquired in a criminal investigation.[123] Even if some of the information may have not fallen directly under these stipulations, it must still be "handed over if the intelligence committees ask for it."[124] Hence, if the Director of National Intelligence did not share the information, the committees could have demanded it. Further research in the future could certainly help shed more light on why this opportunity was not seized by the stakeholders but the professional climate and work culture described in the first part of this work point to obstacles and hurdles that are embedded in the practices of the institutional hallways in Washington DC. Yet the power of the law, and paradoxically here under the veil of national security, could have helped intelligence oversight to prevail. As Divoll put it: "No court has ever ruled that the executive can withhold such information from Congress."[125]

Here it is important to recall the distinction between the role of judicial control and oversight. It would be interesting to further examine the impact of court rulings in terms of US oversight practices that go beyond the national realm, spanning to transnational collaborations, such as Five Eyes, an intelligence alliance comprising Australia, Canada, New Zealand, the UK, and the United States. The alliance's internal oversight structure, however, is little transparent and sheltered from public scrutiny.[126] Creating transnational

control mechanisms is the more challenging in the US context as any international treaty requires ratification by Congress, whereas in the context of the European Union, international treaties are above member states' constitutions and require changes to the latter if stipulated by an agreement or treaty. As a result, case law by the European Court of Justice illustrates the impact of judicial decisions in fueling debates and practices on oversight in member states.[127]

Concluding remarks and road ahead

In this chapter, I sought to capture the multifaceted oversight issues with respect to intelligence in the United States and to some extent a few transnational ramifications. For this, I first problematized some basic concepts and provided an historical overview of the predominant oversight mechanisms carried out by Congress. Following this initial survey, I scrutinized some of the congressional dilemmas and examined stakeholders, institutions, and practices. By connecting the epistemological underpinnings of statecraft and the political sociology of law, I emphasized the transversal nature of oversight politics. Based on this mapping, I then employed this transversal oversight perspective on empirical cases to further our understanding of actors, practices, and norms of intelligence and security oversight.

The empirical evidence analyzed above illustrated that despite the intricate institutional framework and unwritten rules and practices between advocates for oversight and the intelligence community, transversal legal advances in an increasing number of court cases prove potentially powerful to fuel accountability and fight impunity. While the normative and legislative changes for transnational change remain uncertain in the short term, they are nonetheless a formidable stepping stone in tandem with other, existing forces at play, including external actors, such as the media. The interdependencies between different stakeholders deserve further scholarly attention relying on transversal lines of inquiry. Hence, it remains to be seen if the role of investigative journalists in uncovering state secret-related scandals might be an endangered species in the age of the internet.[128]

Instead, the boundaries of the field of intelligence oversight are in constant flux and call for efforts to redefine it. As stakeholders explore the liminal space at the intersection of organizational boundaries and professional practices, members of intelligence services and stakeholders pushing for enhanced oversight procedures and systems do so transversally and often operate "in between spaces."[129] In this context, informal institutions may serve as important focal points for synergies between different actors. Yet contemporary trend shifts in the intelligence community that strengthen a market-driven rationale in intelligence collection and sharing are problematic. Further streamlining these processes with a business analytics-oriented approach, only bolsters already existing public–private partnerships of intelligence services and private-sector partners, usually contractors.[130] Moreover, it provides members of the

intelligence services with an enhanced sense of powerful ownership of the data vis-a-vis their client(s), usually governments. Such dramatic change in corporate governance and harnessing private-sector tools to extend the reach, ownership, and accountability mechanisms in the hands of the intelligence community and corporate leadership is worrisome in view of the integration of democratic and independent oversight stakeholders.

Finally, the challenges associated with accessibility of intelligence documentation can be in part circumvented by accessing and interpreting public documents, including different government bodies and agencies.[131] Other related research can also be helpful in this context.[132] And further legal case studies, such as questions of surveillance against the backdrop of FISA and FISC, deserve continued attention. Future observations will tell whether the interplay of law, congressional realpolitik, and practices on the ground will help forge stronger oversight ties and shift the professional work culture.

Notes

1 See public hearing broadcast on C-SPAN, RepCohen, "Rep. Cohen Questions FBI Director Robert Mueller on Torture" (Youtube, April 24, 2008), https://www.youtube.com/watch?v=6neVBK5dSeI.
2 Margot Williams, "The FBI Was Deeply Involved in CIA Black Site Interrogations Despite Years of Denials, Guantánamo Defense Lawyer Says," The Intercept, September 11, 2019, https://theintercept.com/2019/09/11/fbi-cia-black-site-guantanamo/.
3 James Wirtz in Damien Van Puyvelde et al., "Comparing National Approaches to the Study of Intelligence," *International Studies Perspectives* 21, no. 3 (2020): 327–31.
4 Hamilton Beans in James Writz, "Article Review: Peter Gill, Stephen Marrin, and Mark Pythian, Eds. 'Developing Intelligence Theory' Special Issue of Intelligence and National Security 33:4 (June 2018)," *H-Diplo*, no. 815 (December 13, 2018), https://networks.h-net.org/node/28443/discussions/3332078/h-diplo-article-review-815-peter-gill-stephen-marrin-and-mark.
5 For transdisciplinary research on EU institutions, see Hartmut Aden, "Information Sharing, Secrecy and Trust among Law Enforcement and Secret Service Institutions in the European Union," *West European Politics* 41, no. 4 (July 4, 2018): 981–1002; see als Marie-Christine Dähn et al., "Privacy and Cyber Security on the Books and on the Ground" (August 1, 2018), https://papers.ssrn.com/abstract=3250354; Peter Sund, "The Rationality Gap between Cyber Security and Rule of Law in Extra-Territorial Processing of Classified Information on Cloud Environments" (theseus.fi, 2020), https://www.theseus.fi/handle/10024/344725.
6 Kniep, Herren Der Information "-Die Transnationale Autonomie Digitaler Überwachung," *Zeitschrift Fur Politik*, 2021, https://www.econstor.eu/handle/10419/240926.
7 Félix Guattari, "Transdisciplinarity Must Become Transversality," *Theory, Culture & Society* 32, no. 5–6 (September 1, 2015): 131–37. For a discussion on transversality and international political sociology, see Tugba Basaran et al., *International Political Sociology: Transversal Lines* (Routledge, 2016).
8 "Adjusting a Bourdieusian Approach to the Study of Transnational Fields: Transversal Practices and State (trans) Formations Related to Intelligence and

Surveillance," *Charting Transnational Fields*, 2020, 58, https://doi.org/10.4324/9780429274947-4/adjusting-bourdieusian-approach-study-transnational-fields-didier-bigo.

9 Basaran et al., *International Political Sociology: Transversal Lines*, 2.
10 Bigo, "Adjusting a Bourdieusian Approach to the Study of Transnational Fields: Transversal Practices and State (trans) Formations Related to Intelligence and Surveillance," 59.
11 Gilles Deleuze, "Postscript on the Societies of Control," *October* 59, no. Winter (1992): 3–7.
12 Deleuze.
13 Deleuze.
14 Nira Yuval-Davis, "What Is 'Transversal Politics'?," *Soundings* Summer, no. 12 (1999): 95.
15 Yuval-Davis, 95.
16 Tania Domett, "Soft Power in Global Politics? Diplomatic Partners as Transversal Actors," *Australian Journal of Political Science* 40, no. 2 (June 1, 2005): 290.
17 Klaus Bruhn Jensen, "The Qualitative Research Process," in *A Handbook of Media and Communication Research* (Routledge, 2020), 286–306; Satu Elo and Helvi Kyngäs, "The Qualitative Content Analysis Process," *Journal of Advanced Nursing* 62, no. 1 (April 2008): 107–15.
18 Florian Kohlbacher, "The Use of Qualitative Content Analysis in Case Study Research," *Forum, qualitative social research / Forum, Qualitative Sozialforschung* 7, no. 1 (January 2006): 1–30.
19 Rahul Sagar, "On Combating the Abuse of State Secrecy," *The Journal of Political Philosophy* 15, no. 4 (December 2007): 405.
20 Sagar, 405.
21 Marvin C. Ott, "Partisanship and the Decline of Intelligence Oversight," *International Journal of Intelligence and CounterIntelligence* 16, no. 1 (January 1, 2003): 70.
22 Njord Wegge, "Intelligence Oversight and the Security of the State," *International Journal of Intelligence and CounterIntelligence* 30, no. 4 (October 2, 2017): 689.
23 Wegge, 689.
24 "Partisanship and the Decline of Intelligence Oversight," 76.
25 C. Ott, 76.
26 C. Ott, 73–88.
27 OSS was also marred with challenges and initial distrust from other services within the US administration. See for instance, George C. Chalou and United States. National Archives and Records Administration, *The Secrets War: The Office of Strategic Services in World War II*, viii, 392 p.: ill., map; 24 cm. (Washington, DC: National Archives and Records Administration, 1992), chaps. 2–6. and website of the National Parks Services at https://www.nps.gov/articles/postwar-period-end-of-the-oss-and-return-to-the-park-service.htm, accessed June 7, 2022.
28 C. Ott, "Partisanship and the Decline of Intelligence Oversight," 75.
29 Congress passed the Hughes-Ryan Amendment to the Foreign Assistance Act, which legally required the administration to formally authorize covert actions. The US president had to justify that a covert action was important to US national security interests.
30 While the Church Committee report was published, the Pike report was never officially released to the public. Parts of it leaked and were published outside the US, see for instance, Annie Jacobsen, *Surprise, Kill, Vanish: The Definitive History of Secret CIA Assassins, Armies and Operators* (John Murray, 2019), 224–225. It is now available in its unabridged length, see for instance United States., Congress., House., Select Committee on Intelligence., Pike, and Otis. *CIA: The Pike Report*. Nottingham: Spokesman Books for the Bertrand Russell Peace Foundation, 1977.

31 Pike was nominated after the initial commission under Lucien Nezdi was abolished, due to his symbolization of protective congressional patronage of covert CIA operations. See for instance, "The House Inquiry Into CIA," *The Washington Post (1974-)*, July 20, 1975.
32 United States. et al., *CIA: The Pike Report* (Nottingham: Spokesman Books for the Bertrand Russell Peace Foundation, 1977), 17.
33 C. Ott, "Partisanship and the Decline of Intelligence Oversight," 76.
34 C. Ott, 76.
35 For a detailed account on the Clinton years, see Gregory C. McCarthy, "GOP Oversight of Intelligence in the Clinton Era," *International Journal of Intelligence and CounterIntelligence* 15, no. 1 (January 1, 2002): 26–51.
36 While not a legal term, it refers to US government practices in the aftermath of the 9/11 terrorist attacks, in which US (often illegally) apprehended terrorist suspects -- or sometimes with the help of local authorities -- and transferred them to countries known to torture prisoners or employ harsh interrogation techniques that may rise to the level of torture. See for instance Malika Danoy, "Des Etats-Unis à La Corne d'Afrique. Le 'Programme de Restitutions Extraordinaires': L'extension Du Pouvoir Chasseur Dans La Lutte Antiterroriste," ed. Bertrand Guillarme and Vanessa Codaccioni (Ph.D., Centre de Recherches Sociologiques et Politiques, 2021), https://www.theses.fr/s125084.
37 For malpractice and human rights violations by the CIA then, see John M. Diamond, *The CIA and the Culture of Failure: U.S. Intelligence from the End of the Cold War to the Invasion of Iraq* (Stanford University Press, 2008).
38 See for instance Department of Defense intelligence oversight course, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://dodsioo.defense.gov/Portals/46/Documents/DoD%20Basic%20Intelligence%20Oversight%20Course.pdf, accessed August 1, 2022.
39 For a list of reports by the the DIA Office of the Inspector General, see https://oig.dia.mil/Reports/Semiannual-Reports/, accesses August 8, 2022.
40 "Obama Says the NSA Has Had Plenty of Oversight. Here's Why He's Wrong," *The Washington Post*, June 7, 2013, https://www.washingtonpost.com/news/wonk/wp/2013/06/07/obama-says-the-nsa-has-had-plenty-of-oversight-heres-why-hes-wrong/.
41 Sudha Setty, "Surveillance, Secrecy, and the Search for Meaningful Accountability Symposium," *Stanford Journal of International Law* 51, no. 1 (2015): 69–104.
42 The board was created in 2004 upon recommendation of the 9/11 Commission.
43 Timothy H. Edgar, *Beyond Snowden: Privacy, Mass Surveillance, and the Struggle to Reform the NSA*, 1 online resource (Washington, D.C.: Brookings Institution Press, 2017), 102–03.
44 James Wirtz in Van Puyvelde et al., "Comparing National Approaches to the Study of Intelligence," 330.
45 James Wirtz in Van Puyvelde et al., 330.
46 Darren E. Tromblay, "Intelligence and the Intelligentsia: Exploitation of U.S. Think Tanks by Foreign Powers," *International Journal of Intelligence and CounterIntelligence* 31, no. 1 (January 2, 2018): 1–18.
47 See for instance Damien Van Puyvelde, *Outsourcing US Intelligence: Contractors and Government Accountability* (Edinburgh University Press, 2019); Tim Shorrock, *Spies for Hire: The Secret World of Intelligence Outsourcing* (Simon and Schuster, 2008).
48 The Economist, "A Risk-Averse Germany Enters an Age of Confrontation," *The Economist*, March 17, 2022, https://www.economist.com/europe/2022/03/19/a-risk-averse-germany-enters-an-age-of-confrontation.

49 Robert Jervis, "Foreword. Intelligence, Civil-Intelligence Relations, and Democracy," in *Reforming Intelligence* (University of Texas Press, 2021), vii–xx.
50 Eric Rosenbach et al., "Congressional Oversight of the Intelligence Community," Belfer Center for Science and International Affairs, accessed March 16, 2022, https://www.belfercenter.org/publication/congressional-oversight-intelligence-community.
51 FISA was passed in 1978 and regulates certain types of foreign intelligence collection including certain collections with the support of US telecom companies.
52 Rosenbach et al.
53 Rosenbach et al.
54 The Fourth Amendment protects people from unreasonable searches and seizures by the government.
55 Daphna Renan, "The FISC's Stealth Administrative Law," in *Global Intelligence Oversight* (Oxford University Press, 2016).
56 This term is used by NSA and refers to intercepting telephone and Internet traffic from the Internet backbone, i.e. major Internet cables and switches, both domestic and foreign.
57 Renan, 126.
58 Peter de Werd, "Reflexive Intelligence and Converging Knowledge Regimes," *Intelligence & National Security* 36, no. 4 (June 7, 2021): 515.
59 Claudia Aradau and Sarah Perret, "The Politics of (non-)knowledge at Europe's Borders: Errors, Fakes, and Subjectivity," *Kokusaigaku Revyu = Obirin Review of International Studies* 48, no. 3 (July 2022): 405–24.
60 Aradau and Perret, 420.
61 Jennifer Kibbe, "Congressional Oversight of Intelligence: Is the Solution Part of the Problem?," *Intelligence & National Security* 25, no. 1 (February 1, 2010): 30.
62 Under the Obama administration Congress drafted alternatives after legislation to create a Joint Committee on Oversight did not materialize. See for instance, L. Elaine Halchin and Frederick M. Kaiser, "Congressional Oversight of Intelligence: Current Structure and Alternatives" (LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE, 2012), https://apps.dtic.mil/sti/citations/ADA560388.
63 Kibbe, "Congressional Oversight of Intelligence: Is the Solution Part of the Problem?," 2.
64 Elizabeth Rindskopf Parker and Bryan Pate, "2. Rethinking Judicial Oversight of Intelligence," in *Reforming Intelligence* (University of Texas Press, 2021), 58.
65 Parker and Pate, "2. Rethinking Judicial Oversight of Intelligence."
66 Parker and Pate, 68.
67 The question of legal standards and best practices has resonated in scholarly circles also beyond the US case, see for instance Marina Caparini and Hans Born, "Controlling and Overseeing Intelligence Services in Democratic States," in *Democratic Control of Intelligence Services* (Routledge, 2016), 25–46; Hans Born, "Parliamentary and External Oversight of Intelligence Services," in *Democratic Control of Intelligence Services* (Routledge, 2016), 185–98; H. Born and I. D. Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (Oslo: Publishing House of the Parliament of Norway, 2005); Hans Born, "Towards Effective Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practices," *Connections* 3, no. 4 (2004): 1–12.
68 18 U.S. Code app. III §§ 1–16, see also https://www.govinfo.gov/app/details/USCODE-2011-title18/USCODE-2011-title18-app-classifie, accessed August 7, 2022.

69 Evan Perez, "Secret Court's Oversight Gets Scrutiny," *Wall Street Journal*, June 9, 2013, https://www.wsj.com/articles/SB10001424127887324904004578535670310514616.
70 Peter Finn and Sari Horwitz, "U.S. Charges Snowden with Espionage," *The Washington Post*, June 21, 2013, https://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1–11e2-a016–92547bf094cc_story.html.
71 See Snowden interview with the public German TV channel ARD, available at https://archive.org/details/SnowdenInterviewInEnglishARD480p, accessed August 11, 2022.
72 Stephen P. Mulligan and Jennifer K. Elsea, "Criminal Prohibitions on Leaks and Other Disclosures of Classified Defense Information" (Congressional Research Service, March 7, 2017).
73 Jane Mayer, "Outsourcing Torture," *The New Yorker*, February 6, 2005, https://www.newyorker.com/magazine/2005/02/14/outsourcing-torture.
74 For more details, see Arar v. Ashcroft, 585 F.3d 559 (2d. Cir. 2009).
75 See for instance, https://www.uscourts.gov/cameras-courts/jewel-v-nsa, accessed August 11, 2022.
76 Amy B. Zegart, "The Domestic Politics of Irrational Intelligence Oversight," *Political Science Quarterly* 126, no. 1 (2011): 1–25.
77 Wegge, "Intelligence Oversight and the Security of the State," 6.
78 Kibbe, "Congressional Oversight of Intelligence: Is the Solution Part of the Problem?," 2.
79 McCubbins and Schwartz in Kibbe, 27.
80 Wirtz in Van Puyvelde et al., "Comparing National Approaches to the Study of Intelligence," 327.
81 "Intelligence Oversight," *Harvard Journal on Legislation* 45 (2008): 205; for additional work on intelligence oversight and accountability, see for instance Claudia Hillebrand, "Intelligence Oversight and Accountability," in *Routledge Companion to Intelligence Studies* (Routledge, 2013), 323–30.
82 For a detailed account on global intelligence oversight see for instance Zachary K. Goldman and Samuel James Rascoff, *Global Intelligence Oversight: Governing Security in the Twenty-First Century* (Oxford University Press, 2016). For other discussions on challenges, see Njord Wegge and Thorsten Wetzling, "Contemporary and Future Challenges to Effective Intelligence Oversight," in *Intelligence Oversight in the Twenty-First Century* (Routledge, 2018), 25–40; Peter Gill, "Intelligence, Threat, Risk and the Challenge of Oversight," *Intelligence & National Security* 27, no. 2 (April 1, 2012): 206–22; Aidan Wills, "Understanding Intelligence Oversight," *Geneva: DCAF*, 2010, 25–27. For country specific examples of intelligence as democratic statecraft, see Bertrand Warusfel, "The Intensification of French Intelligence and Its Oversight under the Impact of Counter-Terrorism," *Intelligence Oversight in the Twenty-First Century: Accountability in a Changing World*, 2018, 124–34; or Alejandro M. Bihar, "Uruguay's Attempt at Intelligence Oversight," *International Journal of Intelligence and CounterIntelligence* 33, no. 2 (April 2, 2020): 214–47.
83 Schedler in Caparini and Born, "Controlling and Overseeing Intelligence Services in Democratic States," 10.
84 Christian Leuprecht, *Intelligence as Democratic Statecraft: Accountability and Governance of Civil-Intelligence Relations across the Five Eyes Security Community - the United States, United Kingdom, Canada, Australia, and New Zealand*, 1 online resource (272 pages): illustrations, First edition. (Oxford: Oxford University Press, 2021), 176.
85 Ashley Deeks, "Intelligence Services, Peer Constraints, and the Law," in *Global Intelligence Oversight* (Oxford University Press, 2016).

86 Dennis Broeders, Boeke Sergei, and Ilina Georgieva, "Foreign Intelligence in the Digital Age. Navigating a State of 'unpeace,'" *Navigating a State of "Unpeace"(September 1, 2019). Broeders, D., S. Boeke and I. Georgieva. Foreign Intelligence in the Digital Age. Navigating a State of "unpeace". The Hague Program For Cyber Norms Policy Brief*, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3493612.
87 Peter Gill and Mark Phythian, "Developing Intelligence Theory," *Intelligence & National Security* 33, no. 4 (June 7, 2018): 467.
88 Peter Gill, Stephen Marrin, and Mark Phythian, *Developing Intelligence Theory: New Challenges and Competing Perspectives* (Routledge, 2020).
89 Chaim Levinson, "With Israel's Encouragement, NSO Sold Spyware to UAE and Other Gulf States," *Haaretz*, August 25, 2020, https://www.haaretz.com/middle-east-news/2020-08-25/ty-article/.premium/with-israels-encouragement-nso-sold-spyware-to-uae-and-other-gulf-states/0000017f-dbf3-d856-a37f-fff3a4ba0000.
90 Bernardo de Miguel, "Pegasus: Europe's Deepening Spyware Scandal," *El País*, May 3, 2022, https://english.elpais.com/international/2022-05-03/pegasus-europes-deepening-spyware-scandal.html.
91 For an excellent discussion on transnational oversight challenges see for instance, Jelle van Buuren, "From Oversight to Undersight: The Internationalization of Intelligence," *Security and Human Rights* 24, no. 3–4 (April 30, 2014): 239–52.
92 For an overview of oversight mechanisms of US intelligence services, see also https://www.intelligence.gov/how-the-ic-works, accessed August 8, 2022.
93 H.R.8588 - 95th Congress (1977–1978), https://www.congress.gov/bill/95th-congress/house-bill/8588/. The act has been amended in
94 "IG Act History," accessed August 12, 2022, https://www.ignet.gov/content/ig-act-history.
95 Melissa Quinn, "The Internal Watchdogs Trump Has Fired or Replaced," CBS News, May 18, 2020, https://www.cbsnews.com/news/trump-inspectors-general-internal-watchdogs-fired-list/.
96 See official website at https://www.congress.gov/bill/117th-congress/senate-bill/587, accessed August 8, 2022.
97 The US government comprises 18 intelligence services, including the Office of Naval Intelligence (ONI), the Coast Guard Intelligence (CGI), or the Bureau of Intelligence and Research (INR), which is attached to the US Department of State. For a complete list, see https://www.dni.gov/index.php/what-we-do/members-of-the-ic, accessed August 10, 2022. While they are part of the intelligence services environment, they have fueled less media attention in terms of breaches and violations.
98 See event details at, https://www.wilsoncenter.org/event/who-watches-the-watchmen-the-new-intelligence-oversight, accessed June 9, 2022.
99 Greg Miller, "Pentagon's Plans for a Spy Service to Rival the CIA Have Been Pared Back," *The Washington Post*, November 1, 2014, https://www.washingtonpost.com/world/national-security/pentagons-plans-for-a-spy-service-to-rival-the-cia-have-been-pared-back/2014/11/01/1871bb92–6118-11e4–8b9e-2ccdac31a031_story.html.
100 Charlie Savage et al., "Newly Declassified Video Shows U.S. Killing of 10 Civilians in Drone Strike," *The New York Times*, January 19, 2022, https://www.nytimes.com/2022/01/19/us/politics/afghanistan-drone-strike-video.html.
101 For a discussion on the rendition program, see for instance Robert Johnson, "Extraordinary Rendition: A Wrong without a Right," *University of Richmond Law Review. University of Richmond* 43 (2008): 1135.

102 For changes in interrogation responsibilities after the revelations in public, see Douglas Jehl, David Johnston, and Neil A. Lewis, "C.I.A. Is Seen as Seeking New Role on Detainees," *The New York Times*, February 16, 2005, https://www.nytimes.com/2005/02/16/politics/cia-is-seen-as-seeking-new-role-on-detainees.html.
103 Helen Duffy, "Dignity Denied: The Abu Zubaydah Case Study," *Human Dignity and Human Security in Times of* (2020), https://doi.org/10.2139/ssrn.3562402.
104 *United States v. Zubaydah* 595 US ___ (2022).
105 Robert Barnes, "Supreme Court Says State-Secrets Doctrine Protects Disclosure of 'black Site' Locations in Torture Allegation Case," *The Washington Post*, March 3, 2022, https://www.washingtonpost.com/politics/2022/03/03/supreme-court-abu-zubaydah/.
106 Carol Rosenberg, "Detention of an Afghan at Guantánamo Bay Is Ruled Unlawful," *The New York Times*, October 20, 2021, https://www.nytimes.com/2021/10/20/us/politics/guantanamo-afghan-detainee.html.
107 See for instance, *Abu Zubaydah v. Lithuania* (2018) and *Abu Zubaydah v. Poland* (2014). In a related 2018 ruling, the ECHR rendered its guilty verdict against another European government, holding it responsible in the case *Al Nashiri v. Romania*.
108 "Landmark Rulings Expose Romanian and Lithuanian Complicity in CIA Secret Detention Programme," Amnesty International, May 31, 2018, https://www.amnesty.org/en/latest/news/2018/05/landmark-rulings-expose-romanian-and-lithuanian-complicity-in-cia-secret-detention-programme/.
109 *United States v. Zubaydah* 595 US ___ (2022).
110 The locations include Thailand, Lithuania, Poland, the United States Base at Guantánamo Bay, Cuba, Afghanistan and Morocco.
111 Haroon Siddique, "UK Spies Who Allegedly Passed Questions to CIA Torturers Subject to English Law, Court Rules," *The Guardian*, March 16, 2022, https://www.theguardian.com/law/2022/mar/16/abu-zubaydah-uk-spies-cia-torture-english-law.
112 The 2014 Senate Select Committee on Intelligence's report, often referred to as the "torture report" is available here, https://www.intelligence.senate.gov/sites/default/files/publications/CRPT-113srpt288.pdf, accessed March 1, 2022.
113 Siddique.
114 Siddique.
115 A public version with redaction can be found on the Department of Justice website at, https://www.justice.gov/archives/sco/file/1373816/download, accessed March 2, 2022.
116 Sharon LaFraniere and Katie Benner, "Mueller Delivers Report on Trump-Russia Investigation to Attorney General," *The New York Times*, March 22, 2019, https://www.nytimes.com/2019/03/22/us/politics/mueller-report.html.
117 Andy Wright et al., "On Mueller Report, Barr Says No Executive Privilege Redactions. But Look for Assertion Later," Just Security, April 18, 2019, https://www.justsecurity.org/63692/on-mueller-report-barr-says-no-executive-privilege-redactions-but-look-for-assertion-later/.
118 Adam Liptak, "Supreme Court Blocks Release of Full Mueller Report for Now," *The New York Times*, May 20, 2020, https://www.nytimes.com/2020/05/20/us/supreme-court-blocks-mueller-report-release.html.
119 See also Barr's speech delivered at the Federalist Society's 2019 National Lawyers Convention in November, published by a Harvard law journal, William P. Barr, "The Role of the Executive," *Harv. JL & Pub. Pol'y* 43 (2020): 605.
120 "116th United States Congress," Ballotpedia, accessed March 21, 2022, https://ballotpedia.org/116th_United_States_Congress.

121 Vicki Divoll, "Subpoena Isn't the Only Way to Get the Mueller Report," *The New York Times*, April 8, 2019, https://www.nytimes.com/2019/04/08/opinion/subpoena-mueller-report-intelligence-.html.
122 For a copy of the law, see https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf, accessed March 3, 2022.
123 See for instance, https://www.law.cornell.edu/uscode/text/50/3040, accessed March 4, 2022.
124 Divoll.
125 Divoll.
126 For more information see organizational website and executive meeting summaries at https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc, accessed August 8, 2022.
127 See organizational website for case law at https://curia.europa.eu/, accessed August 1, 2022.
128 Owen cited in Richard J. Aldrich and Daniela Richterova, "Ambient Accountability: Intelligence Services in Europe and the Decline of State Secrecy," *West European Politics* 41, no. 4 (July 4, 2018): 1005.
129 Sida Liu, "Between Social Spaces," *European Journal of Social Theory* 24, no. 1 (February 1, 2021): 123–39.
130 "What the Intelligence Community Doesn't Know Is Hurting the United States," Center for American Progress, September 18, 2020, https://www.americanprogress.org/article/intelligence-community-doesnt-know-hurting-united-states/; Peter Gill, "Of Intelligence Oversight and the Challenge of Surveillance Corporatism," *Intelligence & National Security* 35, no. 7 (November 9, 2020): 970–89.
131 "Foreign Military Training and DoD Engagement Activities of Interest, 2019–2020," United States Department of State, August 4, 2021, https://www.state.gov/reports/foreign-military-training-and-dod-engagement-activities-of-interest-2019–2020/; "Foreign Military Training and DoD Engagement Activities of Interest," United States Department of State, August 15, 2018, https://www.state.gov/foreign-military-training-and-dod-engagement-activities-of-interest/.
132 "The Costs of War Papers," The Costs of War Project, accessed March 14, 2022, https://watson.brown.edu/costsofwar/papers. Counterterrorism ops are particularly useful, see for instance, S. Savell, "United States Counterterrorism Operations 2018--2020," *Costs of War Project*, 2021.

References

Aden, Hartmut. "Information Sharing, Secrecy and Trust among Law Enforcement and Secret Service Institutions in the European Union." *West European Politics* 41, no. 4 (July 4, 2018): 981–1002.

Aldrich, Richard J., and Daniela Richterova. "Ambient Accountability: Intelligence Services in Europe and the Decline of State Secrecy." *West European Politics* 41, no. 4 (July 4, 2018): 1003–1024.

Amnesty International. "Landmark Rulings Expose Romanian and Lithuanian Complicity in CIA Secret Detention Programme," May 31, 2018. https://www.amnesty.org/en/latest/news/2018/05/landmark-rulings-expose-romanian-and-lithuanian-complicity-in-cia-secret-detention-programme/.

Aradau, Claudia, and Sarah Perret. "The Politics of (non-)knowledge at Europe's Borders: Errors, Fakes, and Subjectivity." *Kokusaigaku Revyu = Obirin Review of International Studies* 48, no. 3 (July 2022): 405–424.

Baker, James A. "Intelligence Oversight." *Harvard Journal on Legislation* 45 (2008): 199.

Barnes, Robert. "Supreme Court Says State-Secrets Doctrine Protects Disclosure of 'black Site' Locations in Torture Allegation Case." *The Washington Post*. March 3, 2022. https://www.washingtonpost.com/politics/2022/03/03/supreme-court-abu-zubaydah/.

Ballotpedia. "116th United States Congress." Accessed March 21, 2022. https://ballotpedia.org/116th_United_States_Congress.

Barr, William P. "The Role of the Executive." *Harv. JL & Pub. Pol'y* 43 (2020): 605.

Basaran, Tugba, Didier Bigo, Emmanuel-Pierre Guittet, and R. B. J. Walker. *International Political Sociology: Transversal Lines*. Routledge, 2016.

Bigo. "Adjusting a Bourdieusian Approach to the Study of Transnational Fields: Transversal Practices and State (trans) Formations Related to Intelligence and Surveillance." *Charting Transnational Fields*, 2020. https://doi.org/10.4324/9780429274947-4/adjusting-bourdieusian-approach-study-transnational-fields-didier-bigo.

Bihar, Alejandro M. "Uruguay's Attempt at Intelligence Oversight." *International Journal of Intelligence and CounterIntelligence* 33, no. 2 (April 2, 2020): 214–247.

Born, H., and I. D. Leigh. *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies*. Oslo: Publishing House of the Parliament of Norway, 2005.

Born, Hans. "Towards Effective Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practices." *Connections* 3, no. 4 (2004): 1–12.

Born, Hans. "Parliamentary and External Oversight of Intelligence Services." In *Democratic Control of Intelligence Services*, 185–198. Routledge, 2016.

Broeders, Dennis, Boeke Sergei, and Ilina Georgieva. "Foreign Intelligence in the Digital Age. Navigating a State of 'unpeace.'" *Navigating a State of "Unpeace" (September 1, 2019). Broeders, D., S. Boeke and I. Georgieva. Foreign Intelligence in the Digital Age. Navigating a State of "unpeace". The Hague Program For Cyber Norms Policy Brief*, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3493612.

Buuren, Jelle van. "From Oversight to Undersight: The Internationalization of Intelligence." *Security and Human Rights* 24, no. 3–4 (April 30, 2014): 239–252.

Caparini, Marina, and Hans Born. "Controlling and Overseeing Intelligence Services in Democratic States." In *Democratic Control of Intelligence Services*, 25–46. Routledge, 2016.

Chalou, George C., and United States. "National Archives and Records Administration." *The Secrets War: The Office of Strategic Services in World War II*. Viii, 392: ill., map; 24 cm. Washington, DC: National Archives and Records Administration, 1992.

Center for American Progress. "What the Intelligence Community Doesn't Know Is Hurting the United States," September 18, 2020. https://www.americanprogress.org/article/intelligence-community-doesnt-know-hurting-united-states/.

Danoy, Malika. "Des Etats-Unis à La Corne d'Afrique. Le 'Programme de Restitutions Extraordinaires': L'extension Du Pouvoir Chasseur Dans La Lutte Antiterroriste." Edited by Bertrand Guillarme and Vanessa Codaccioni. Ph.D., Centre de Recherches Sociologiques et Politiques, 2021. https://www.theses.fr/s125084.

Deeks, Ashley. "Intelligence Services, Peer Constraints, and the Law." In *Global Intelligence Oversight*. Oxford University Press, 2016.

Deleuze, Gilles. "Postscript on the Societies of Control." *October* 59, no. Winter (1992): 3–7.

Diamond, John M. *The CIA and the Culture of Failure: U.S. Intelligence from the End of the Cold War to the Invasion of Iraq*. Stanford University Press, 2008.

Divoll, Vicki. "Subpoena Isn't the Only Way to Get the Mueller Report." *The New York Times*. April 8, 2019. https://www.nytimes.com/2019/04/08/opinion/subpoena-mueller-report-intelligence-.html.

Domett, Tania. "Soft Power in Global Politics? Diplomatic Partners as Transversal Actors." *Australian Journal of Political Science* 40, no. 2 (June 1, 2005): 289–306.

Duffy, Helen. "Dignity Denied: The Abu Zubaydah Case Study." *Human Dignity and Human Security in Times of*, 2020. 10.2139/ssrn.3562402.

Dähn, Marie-Christine, Ingolf Pernice, Jörg Pohle, Zachary Goldman, Paul Nemitz, Theodore Christakis, Randal S. Milch, et al. "Privacy and Cyber Security on the Books and on the Ground." August 1, 2018. https://papers.ssrn.com/abstract=3250354.

Edgar, Timothy H. *Beyond Snowden: Privacy, Mass Surveillance, and the Struggle to Reform the NSA*. 1 online resource. Washington, D.C.: Brookings Institution Press, 2017.

Elo, Satu, and Helvi Kyngäs. "The Qualitative Content Analysis Process." *Journal of Advanced Nursing* 62, no. 1 (April 2008): 107–115.

Finn, Peter, and Sari Horwitz. "U.S. Charges Snowden with Espionage." *The Washington Post*. June 21, 2013. https://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1–11e2-a016–92547bf094cc_story.html.

Gill, Peter. "Intelligence, Threat, Risk and the Challenge of Oversight." *Intelligence & National Security* 27, no. 2 (April 1, 2012): 206–222.

Gill, Peter. "Of Intelligence Oversight and the Challenge of Surveillance Corporatism." *Intelligence & National Security* 35, no. 7 (November 9, 2020): 970–989.

Gill, Peter, and Mark Phythian. "Developing Intelligence Theory." *Intelligence & National Security* 33, no. 4 (June 7, 2018): 467–471.

Gill, Peter, Stephen Marrin, and Mark Phythian. *Developing Intelligence Theory: New Challenges and Competing Perspectives*. Routledge, 2020.

Goldman, Zachary K., and Samuel James Rascoff. *Global Intelligence Oversight: Governing Security in the Twenty-First Century*. Oxford University Press, 2016.

Guattari, Félix. "Transdisciplinarity Must Become Transversality." *Theory, Culture & Society* 32, no. 5–6 (September 1, 2015): 131–137.

Halchin, L. Elaine, and Frederick M. Kaiser. "Congressional Oversight of Intelligence: Current Structure and Alternatives." *Library of Congress Washington DC Congressional Research Service*, 2012. https://apps.dtic.mil/sti/citations/ADA560388.

Hillebrand, Claudia. "Intelligence Oversight and Accountability." In *Routledge Companion to Intelligence Studies*, 323–330. Routledge, 2013.

"IG Act History." Accessed August 12, 2022. https://www.ignet.gov/content/ig-act-history.

Jacobsen, Annie. *Surprise, Kill, Vanish: The Definitive History of Secret CIA Assassins, Armies and Operators*. John Murray, 2019.

Jehl, Douglas, David Johnston, and Neil A. Lewis. "C.I.A. Is Seen as Seeking New Role on Detainees." *The New York Times*. February 16, 2005. https://www.nytimes.com/2005/02/16/politics/cia-is-seen-as-seeking-new-role-on-detainees.html.

Jensen, Klaus Bruhn. "The Qualitative Research Process." In *A Handbook of Media and Communication Research*, 286–306. Routledge, 2020.

Jervis, Robert. "Foreword. Intelligence, Civil-Intelligence Relations, and Democracy." In *Reforming Intelligence*, vii–xx. University of Texas Press, 2021.

Johnson, Robert. "Extraordinary Rendition: A Wrong without a Right." *University of Richmond Law Review. University of Richmond* 43 (2008): 1135.

Kibbe, Jennifer. "Congressional Oversight of Intelligence: Is the Solution Part of the Problem?" *Intelligence & National Security* 25, no. 1 (February 1, 2010): 24–49.

Kohlbacher, Florian. "The Use of Qualitative Content Analysis in Case Study Research." *Forum, qualitative social research / Forum, Qualitative Sozialforschung* 7, no. 1 (January 2006): 1–30.

Kniep. ""Herren Der Information "-Die Transnationale Autonomie Digitaler Überwachung." *Zeitschrift Fur Politik*, 2021. https://www.econstor.eu/handle/10419/240926.

LaFraniere, Sharon, and Katie Benner. "Mueller Delivers Report on Trump-Russia Investigation to Attorney General." *The New York Times*. March 22, 2019. https://www.nytimes.com/2019/03/22/us/politics/mueller-report.html.

Leuprecht, Christian. *Intelligence as Democratic Statecraft: Accountability and Governance of Civil-Intelligence Relations across the Five Eyes Security Community - the United States, United Kingdom, Canada, Australia, and New Zealand*. 1 online resource (272 pages): illustrations. First edition. Oxford: Oxford University Press, 2021.

Levinson, Chaim. "With Israel's Encouragement, NSO Sold Spyware to UAE and Other Gulf States." *Haaretz*, August 25, 2020. https://www.haaretz.com/middle-east-news/2020-08-25/ty-article/.premium/with-israels-encouragement-nso-sold-spyware-to-uae-and-other-gulf-states/0000017f-dbf3-d856-a37f-fff3a4ba0000.

Liptak, Adam. "Supreme Court Blocks Release of Full Mueller Report for Now." *The New York Times*. May 20, 2020. https://www.nytimes.com/2020/05/20/us/supreme-court-blocks-mueller-report-release.html.

Liu, Sida. "Between Social Spaces." *European Journal of Social Theory* 24, no. 1 (February 1, 2021): 123–139.

Mayer, Jane. "Outsourcing Torture." *The New Yorker*. February 6, 2005. https://www.newyorker.com/magazine/2005/02/14/outsourcing-torture.

McCarthy, Gregory C. "GOP Oversight of Intelligence in the Clinton Era." *International Journal of Intelligence and CounterIntelligence* 15, no. 1 (January 1, 2002): 26–51.

Miguel, Bernardo de. "Pegasus: Europe's Deepening Spyware Scandal." *El País*, May 3, 2022. https://english.elpais.com/international/2022-05-03/pegasus-europes-deepening-spyware-scandal.html.

Miller, Greg. "Pentagon's Plans for a Spy Service to Rival the CIA Have Been Pared Back." *The Washington Post*. November 1, 2014. https://www.washingtonpost.com/world/national-security/pentagons-plans-for-a-spy-service-to-rival-the-cia-have-been-pared-back/2014/11/01/1871bb92-6118-11e4-8b9e-2ccdac31a031_story.html.

Mulligan, Stephen P., and Jennifer K. Elsea. "Criminal Prohibitions on Leaks and Other Disclosures of Classified Defense Information." *Congressional Research Service*, March 7, 2017.

Ott, Marvin C. "Partisanship and the Decline of Intelligence Oversight." *International Journal of Intelligence and CounterIntelligence* 16, no. 1 (January 1, 2003): 69–94.

Parker, Elizabeth Rindskopf, and Bryan Pate. "2. Rethinking Judicial Oversight of Intelligence." In *Reforming Intelligence*, 51–72. University of Texas Press, 2021.

Perez, Evan. "Secret Court's Oversight Gets Scrutiny." *Wall Street Journal*, June 9, 2013. https://www.wsj.com/articles/SB10001424127887324904004578535670310514616.

Quinn, Melissa. "The Internal Watchdogs Trump Has Fired or Replaced." *CBS News*, May 18, 2020. https://www.cbsnews.com/news/trump-inspectors-general-internal-watchdogs-fired-list/.

Renan, Daphna. "The FISC's Stealth Administrative Law." In *Global Intelligence Oversight*. Oxford University Press, 2016.

RepCohen. "Rep. Cohen Questions FBI Director Robert Mueller on Torture." *Youtube*, April 24, 2008. https://www.youtube.com/watch?v=6neVBK5dSeI.

Rosenbach, Eric, Aki J. Peritz, Calder Walton, Stephen M. Walt, Harvey Brooks, and Sean M. Lynn-Jones. "Congressional Oversight of the Intelligence Community." *Belfer Center for Science and International Affairs*. Accessed March 16, 2022. https://www.belfercenter.org/publication/congressional-oversight-intelligence-community.

Rosenberg, Carol. "Detention of an Afghan at Guantánamo Bay Is Ruled Unlawful." *The New York Times*. October 20, 2021. https://www.nytimes.com/2021/10/20/us/politics/guantanamo-afghan-detainee.html.

Sagar, Rahul. "On Combating the Abuse of State Secrecy." *The Journal of Political Philosophy* 15, no. 4 (December 2007): 404–427.

Savage, Charlie, Eric Schmitt, Azmat Khan, Evan Hill, and Christoph Koettl. "Newly Declassified Video Shows U.S. Killing of 10 Civilians in Drone Strike." *The New York Times*. January 19, 2022. https://www.nytimes.com/2022/01/19/us/politics/afghanistan-drone-strike-video.html.

Savell, S. "United States Counterterrorism Operations 2018–2020." *Costs of War Project*, 2021.

Setty, Sudha. "Surveillance, Secrecy, and the Search for Meaningful Accountability Symposium." *Stanford Journal of International Law* 51, no. 1 (2015): 69–104.

Shorrock, Tim. *Spies for Hire: The Secret World of Intelligence Outsourcing*. Simon and Schuster, 2008.

Siddique, Haroon. "UK Spies Who Allegedly Passed Questions to CIA Torturers Subject to English Law, Court Rules." *The Guardian*. March 16, 2022. https://www.theguardian.com/law/2022/mar/16/abu-zubaydah-uk-spies-cia-torture-english-law.

Sund, Peter. "The Rationality Gap between Cyber Security and Rule of Law in Extra-Territorial Processing of Classified Information on Cloud Environments." theseus.fi, 2020. https://www.theseus.fi/handle/10024/344725.

The Costs of War Project. "The Costs of War Papers." Accessed March 14, 2022. https://watson.brown.edu/costsofwar/papers.

The Economist. "A Risk-Averse Germany Enters an Age of Confrontation." *The Economist*. March 17, 2022. https://www.economist.com/europe/2022/03/19/a-risk-averse-germany-enters-an-age-of-confrontation.

The Washington Post (1974). "The House Inquiry Into CIA." July 20, 1975.

The Washington Post. "Obama Says the NSA Has Had Plenty of Oversight. Here's Why He's Wrong." June 7, 2013. https://www.washingtonpost.com/news/wonk/wp/2013/06/07/obama-says-the-nsa-has-had-plenty-of-oversight-heres-why-hes-wrong/.

Tromblay, Darren E. "Intelligence and the Intelligentsia: Exploitation of U.S. Think Tanks by Foreign Powers." *International Journal of Intelligence and CounterIntelligence* 31, no. 1 (January 2, 2018): 1–18.

United States., Congress., House., Select Committee on Intelligence., Pike, and Otis. *CIA: The Pike Report*. Nottingham: Spokesman Books for the Bertrand Russell Peace Foundation, 1977.

United States Department of State. "Foreign Military Training and DoD Engagement Activities of Interest," August 15, 2018. https://www.state.gov/foreign-military-training-and-dod-engagement-activities-of-interest/.

United States Department of State. "Foreign Military Training and DoD Engagement Activities of Interest, 2019–2020," August 4, 2021. https://www.state.gov/reports/foreign-military-training-and-dod-engagement-activities-of-interest-2019–2020/.

Van Puyvelde, Damien. *Outsourcing US Intelligence: Contractors and Government Accountability*. Edinburgh University Press, 2019.

Van Puyvelde, Damien, James J. Wirtz, Jean-Vincent Holeindre, Benjamin Oudet, Uri Bar-Joseph, Ken Kotani, Florina Cristiana Matei, and Antonio M. Díaz Fernández. "Comparing National Approaches to the Study of Intelligence." *International Studies Perspectives* 21, no. 3 (2020): 298–337.

Warusfel, Bertrand. "The Intensification of French Intelligence and Its Oversight under the Impact of Counter-Terrorism." *Intelligence Oversight in the Twenty-First Century: Accountability in a Changing World*, (2018), 124–134.

Wegge, Njord. "Intelligence Oversight and the Security of the State." *International Journal of Intelligence and CounterIntelligence* 30, no. 4 (October 2, 2017): 687–700.

Wegge, Njord, and Thorsten Wetzling. "Contemporary and Future Challenges to Effective Intelligence Oversight." In *Intelligence Oversight in the Twenty-First Century*, 25–40. Routledge, 2018.

Werd, Peter de. "Reflexive Intelligence and Converging Knowledge Regimes." *Intelligence & National Security* 36, no. 4 (June 7, 2021): 512–526.

Williams, Margot. "The FBI Was Deeply Involved in CIA Black Site Interrogations Despite Years of Denials, Guantánamo Defense Lawyer Says." *The Intercept*, September 11, 2019. https://theintercept.com/2019/09/11/fbi-cia-black-site-guantanamo/.

Wills, Aidan. *Understanding Intelligence Oversight.* Geneva: DCAF, 2010, 25–27.

Wright, Andy, David Schwendiman, Maksym Vishchyk, Oona Hathaway, Ryan Goodman, Chimène Keitner, Zoe Tatarsky, et al. "On Mueller Report, Barr Says No Executive Privilege Redactions. But Look for Assertion Later." *Just Security*, April 18, 2019. https://www.justsecurity.org/63692/on-mueller-report-barr-says-no-executive-privilege-redactions-but-look-for-assertion-later/.

Writz, James. "Article Review: Peter Gill, Stephen Marrin, and Mark Pythian, Eds. 'Developing Intelligence Theory' Special Issue of Intelligence and National Security 33:4 (June 2018)." *H-Diplo*, no. 815 (December 13, 2018). https://networks.h-net.org/node/28443/discussions/3332078/h-diplo-article-review-815-peter-gill-stephen-marrin-and-mark.

Yuval-Davis, Nira. "What Is 'Transversal Politics'?" *Soundings* Summer, no. 12 (1999): 94–98.

Zegart, Amy B. "The Domestic Politics of Irrational Intelligence Oversight." *Political Science Quarterly* 126, no. 1 (2011): 1–25.

7 The anatomy of political impunity in New Zealand

Damien Rogers

Introduction

Two intelligence and security agencies foster a cadre of New Zealand intelligence professionals and, together, currently employ about 800 people. The Government Communications Security Bureau (GCSB), which specialises in signals intelligence and delivers information assurance and cybersecurity services, was formally established in 1977, though New Zealand's SIGINT capabilities existed since the Second World War and were initially managed within the Defence establishment.[1] Specialising in human intelligence and delivering protective security services, the New Zealand Security Intelligence Service (NZSIS) was established in 1956, though New Zealand's HUMINT capabilities had previously been part of the Special Branch of the New Zealand Police.[2] New Zealand intelligence professionals became foundational members of a transnational guild, which coheres around the National Security Agency (NSA) of the United States and its global surveillance network, upon joining the UKUSA Agreement in 1956.[3] Despite their position at the centre of different national bureaucracies, this politico-social group is a transnational guild in the sense that it comprises "actors whose struggles and solidarity at a distance are connected with a profession and, inside this profession, with a specific craft explaining the common dispositions between individuals who are very distant from each other."[4] The bonds of membership to this guild are forged not only through the regular exchange of information and the sharing of surveillance technologies and technical expertise, but also through staff exchanges, secondments, and the creation of liaison positions within foreign agencies, all of which create an *esprit de corps*, shared goals and a common worldview. As these transnational bonds strengthen over time, the liminality of New Zealand intelligence professionals might mean they have more in common with their foreign counterparts than with many members of the public they serve.[5]

The laws specifically concerning New Zealand intelligence and security agencies have evolved since they were first passed in 1969 but continue to facilitate New Zealand's ongoing engagement with this transnational guild. Because New Zealand's obligations under the UKUSA Agreement were kept

DOI: 10.4324/9781003354130-8

secret from the public and most parliamentarians, the NZSIS Act 1969 only states that in performing its functions the NZSIS "contributes to the participation of New Zealand in the maintenance of international security,"[6] and the GCSB Act 2003 only states that one of the Bureau's objectives is to provide "foreign intelligence to meet the international obligations and commitments of the Government of New Zealand."[7] The Intelligence and Security Act 2017 leaves open the possibility of sharing intelligence with international partners through the objective of contributing to "the international relations and well-being of New Zealand."[8] These international partnerships are anchored in the GCSB's obligations under the UKUSA Agreement, but also include so-called third-party agreements, such as SIGINT Seniors Pacific and SIGINT Seniors Europe,[9] though the 2017 Act explicitly requires ministerial approval before any more such agreements can be joined. Generally speaking, New Zealand law is highly permissive when it comes to authorising New Zealand intelligence activities and sections 110 and 111 of the Intelligence and Security Act 2017 provide immunity to the Director-General of an intelligence and security agency, and any employee of those agencies, from criminal liability for any act done in good faith to obtain an intelligence warrant or for carrying out any authorised activity, respectively. Lawful limits of these activities are enacted by the New Zealand Government's obligations under international human rights law, but international humanitarian law, international criminal law, or public international law concerning the use of armed force in international affairs are not mentioned in the Act.

Democratic control over New Zealand intelligence activities is exercised through ministerial responsibilities which form part of the public accountability arrangements that are the cornerstone of New Zealand's Westminster-styled system of cabinet government,[10] as well as through three inquisitorial oversight measures: the parliamentary Intelligence and Security Committee (ISC) that scrutinises the policies, administration, and expenditure of the GCSB and the NZSIS;[11] periodic statutory reviews undertaken to assure parliamentarians the legislative frameworks that enable and constrain activities undertaken by New Zealand intelligence professionals are fit for purpose;[12] and the Inspector-General of Intelligence and Security (IGIS) who offers assurance to parliamentarians that the intelligence professionals working at the GCSB and the NZSIS act lawfully and, following an amendment in 2013, with propriety.[13] These ministerial responsibilities and oversight measures have occasionally been augmented by ad-hoc inquisitorial reviews.[14] While parliament acts here as a kind of proxy for the watchful gaze of the body politic, the agencies make unclassified versions of their annual reports available to the public, and the ISC, statutory reviewers, and the IGIS have followed suit in an ongoing effort to provide a greater degree of transparency around non-secret intelligence matters. However, far from restricting the engagement of New Zealand intelligence professionals with the transnational guild, this chapter argues that these controls provide the politico-legal

conditions required for those professionals to maintain and develop their membership of that guild. Put simply, intelligence professionals need not navigate legal constraints imposed by oversight measures because these measures are designed to facilitate an increasing interdependence among their disciplinary counterparts located in the bureaucracies of other states.

A by-product of widespread methodological nationalism and an unwavering ontological commitment to the state as the primary entity of contemporary world affairs, the academic literature on the GCSB and the NZSIS gives focus to the establishment and development of the agencies,[15] their external relations,[16] related legislative reform,[17] and governance arrangements.[18] However, scholars have not yet offered a detailed examination of the role played by professionals of politics in enabling and constraining New Zealand intelligence activities.[19] This is somewhat surprising because ministers, as elected representatives of the public, are ultimately responsible for maintaining state sovereignty, ensuring the integrity of democratic institutions, and protecting the population from harms associated with various types of political violence. They are the national authorising agents allowing New Zealand intelligence professionals to operate within a transnational field of surveillance and intelligence populated not only by their counterparts from western democracies, but also their adversaries from Russia, China, and a host of non-democratic regimes.[20] This chapter aims to help remedy that deficiency while adding a too-often neglected case study to the intelligence studies literature concerned with the control of intelligence activities within western liberal democracies: specifically Australia, Canada, and the United Kingdom as well as the United States; but others too.[21] The ensuing examination of this case shows how, and explains why, public accountability arrangements and oversight measures are designed and reformed in ways that allow for, and legitimise, secret violence undertaken on behalf of governments and, more significantly, their foreign partners, thereby augmenting the criminal immunity enjoyed by intelligence professionals when they support that secret use of violence. This matters because "[t]he intensity and visibility of violence may seem to decrease in open conflicts, but as soon as the changes of forms of violence are taken into consideration, as well as the size of their targets and the implications for everyone, it is clear that violence performed by secret services in less visible ways than before continues and extends, nevertheless."[22] Drawing on Pierre Bourdieu's concept of the field to explain why political impunity was created and is seemingly strengthened at every opportunity, the case analysis that follows should be of interest not so much for what it shows about how a small state deals with far more powerful states within an alliance framework, but more for what it reveals about professionals of politics who, struggling within their national field of power over the right to rule their realm through legislative and executive power, position themselves in relation to those New Zealand intelligence professionals who belong to that transnational guild.

The chapter is structured in three sections. The first section demonstrates how successive scandals embroiling intelligence professionals have been

seized upon as opportunities to remediate democratic controls over New Zealand intelligence activities while shielding responsible ministers from any blame. The second section shows that inquisitorial oversight measures constitute important politico-legal conditions that facilitate New Zealand intelligence professionals' ongoing engagement with the transnational guild and, by extension, legitimise their complicity with various forms of state violence. The final section explains how cultivating an uninformed citizenry undermines the public's ability to hold responsible ministers to account and functions as a guarantor of political impunity.

Intelligence scandal as political opportunity

While several controversies feature in the history of New Zealand's intelligence and security agencies, more recent scandals continue to shape the public's low trust and confidence in intelligence professionals today.[23] In 2013, the public became aware that the GCSB unlawfully conducted surveillance of Kim Dotcom, a German-Finnish entrepreneur with permanent residence status in New Zealand, when it monitored his personal communications to assist the New Zealand Police with the execution of a search warrant on 22 January 2012.[24] In a spectacular raid that involved 76 black-clad armed officers, some arriving in helicopters, Dotcom and his associates were arrested that day for alleged violations of US copyright law in accordance with a Mutual Legal Assistance Treaty between New Zealand and the United States.[25] As the Dotcom affair unfolded, Edward Snowden's unauthorised disclosure of official information belonging to the NSA raised uncomfortable questions about the GCSB's partnership with the American spy agency and the extent to which their surveillance activities capture New Zealanders' private information and communications.[26] Concern grew over New Zealand intelligence professionals' awareness of, and involvement with, the torture and rendition programme operated by the United States Central Intelligence Agency (CIA) following Senator Feinstein's documentation of torture and abuse at US Prisons in Abu Gharib, Iraq and Guantanamo Bay, Cuba, which was declassified in 2014.[27] In 2015, two investigative journalists made serious allegations that the New Zealand Special Air Service (NZSAS) committed war crimes in Afghanistan after the United States had attacked, invaded, and occupied that country as part of its so-called war on terrorism.[28] At the heart of these scandals lies an unease about the relationship between New Zealand intelligence professionals, the United States Government, and the secret use of state violence.[29]

John Key, prime minister of New Zealand between 2008 and 2016, became embroiled in these scandals, among others. By insisting he had not heard of Dotcom until 17 September 2012, Key misled the public over when he first became aware of Dotcom's existence and learnt of the GCSB's interest in him because Key received a briefing that included a photo of Dotcom on a visit to the GCSB on 29 February 2012. Confronted with evidence that he misled the

public, Key corrected the Hansard record on 16 October 2012.[30] It then came to light in April 2013 that Key had appointed Ian Fletcher as Director of the GCSB, and that Fletcher was a family friend during Key's childhood and had not been aware of the vacancy until Key had called him about it. Having denied the allegation until Fletcher confirmed the facts of the matter, Key conceded he had intervened in the process, citing a faulty memory as his excuse. In 2014, the public became aware that the NZSIS released redacted documents in 2011 – concerning a meeting between the Director of NZSIS and the Leader of the Opposition that included a briefing on an investigation into Israeli intelligence activities – to a well-known blogger named Cameron Slater who claimed a close association to the Prime Minister and is the son of a former National Party President (the party to which Key belonged), but refused media requests for the same information.[31] A staffer within the prime minister's office gave more information provided by the NZSIS to Slater who then used that information to criticise the Opposition leader for Key's political advantage during an election year.

Official investigations responding to those scandals were seized upon as opportunities to undertake remedial intervention into the democratic controls over New Zealand intelligence activities while diffusing and obfuscating any ministerial responsibility. Following her review of the lawfulness of the GCSB's surveillance of New Zealanders, Rebecca Kitteridge found the GCSB conducted surveillance of a further 55 cases involving 85 individuals to support law-enforcement agencies that may have been unlawful because they contravened New Zealand law at the time, though the IGIS subsequently found these to be lawful.[32] Kitteridge's report made 80 recommendations, most of which concerned internal compliance processes and the organisation's capability to comply with its obligations to protect the privacy rights of New Zealanders. While the role played by the minister in charge of the GCSB was ruled out of scope by the terms of reference, Kitteridge recommended strengthening the IGIS by "broadening the pool of candidates, increasing the resources and staff supporting the IGIS, and making the work programme, audits and reporting expectations of the IGIS more explicit."[33] Following the implementation of Kitteridge's recommendations, Sir Michael Cullen and Dame Patsy Reddy were engaged to conduct the first comprehensive review of the legal framework governing the work of New Zealand intelligence professionals and to consider their proper role and what New Zealanders should expect of them.[34] Cullen and Reddy recommended a single act of legislation to consolidate the objectives, functions, and powers of the two intelligence and security agencies, as well as the provisions for oversight measures. However, when it came to strengthening the ministerial responsibilities for New Zealand intelligence activities, they merely suggested that "the Agencies should continue to consult with the Leader of the Opposition about matters relating to security and the GCSB's intelligence gathering and assistance functions. The Agencies should also, as they see fit, consult with the leader of any other political party in Parliament as defined in the Standing

Orders of the House of Representatives about such matters."[35] They recommended preserving the political independence of the IGIS while enhancing its functions and powers; increasing the membership of the parliamentary ISC to achieve a greater representation of political views while suggesting the prime minister need not always be the chairperson of the committee; and that the ISC be able to request the IGIS conduct an inquiry into matters of their concern.[36]

In response to the abovementioned scandals, Prime Minister Key reformed the public accountability arrangements for intelligence activities – which were focused on the prime minister who had traditionally served as minister-in-charge of the GCSB and the NZSIS – by creating separate ministerial portfolios for both agencies and then handing these ministerial responsibilities to a senior member of his cabinet in 2014. This change was then included in the Intelligence and Security Act 2017, which ensured the prime minister was no longer involved in authorising intelligence warrants as parliament introduced an authorisation regime using two types of intelligence warrants that required their ministerial sign off: the first of which are issued jointly by the minister responsible for the NZSIS and/or the GCSB and a commissioner of intelligence warrants; the second are issued only by the authorising minister(s) but can involve the minister of foreign affairs in certain situations. This new authorisation regime replaced the explicit prohibition on intercepting the communications of New Zealanders, making what was clearly unlawful under the GCSB Act 2003 lawful under the 2017 Act.[37] Whereas under the previous arrangement the prime minister was, in effect, holding him or herself to account for the conduct of the intelligence and security agencies, the minister responsible for the GCSB and the NZSIS is now held accountable for the proper and efficient performance of agency functions by the House of Representatives, through the ISC is still chaired by the prime minister.[38]

Yet those changes preserved the limits of ministerial responsibility for New Zealand intelligence activities. While separate ministerial portfolios now exist for the GCSB and the NZSIS, there appears to be an emerging custom whereby these two portfolios are allocated to the same minister.[39] When a senior cabinet minister holds multiple portfolios, crises in other portfolios, including a global pandemic, have limited their ability to lead on intelligence matters. Furthermore, having one minister responsible for both intelligence and security agencies creates a single intelligence account that removes the contestability of official advice on intelligence matters to cabinet. In discharging their ministerial duties, the minister responsible for both agencies necessarily consults with other ministers holding related portfolios concerning foreign affairs, defence, and law and order, and remains bound by the collective responsibility of cabinet. However, the scope of this ministerial responsibility does not extend to all intelligence activities conducted by all government departments that collect, analyse, and assess intelligence for their own organisational purposes.[40] This means that much of New Zealand's intelligence activities, including commercial intelligence services performed by

former state intelligence professionals, occur beyond the minister's purview.[41] Nor does it cover the conduct of those officers in the police or military who act forcefully on any such intelligence.

Bourdieu's concept of the field helps explain how and why this political impunity was created and seemingly strengthened at every opportunity by parliamentarians.[42] As agents in the national field of power, professionals of politics become parliamentarians when they gain membership to their national assembles and then, as parliamentarians, usually seek to occupy the so-called Treasury benches to obtain and hold the authority to rule through legislative and executive power. As ministers, these professionals of politics tend to use their executive power in ways that help them prevail over their parliamentary opponents and rivals. Ministerial performance becomes an object of contestation among parliamentarians – with poor performances exposed and ridiculed by members of the opposition and, sometimes, the cause for demotion among rivals within cabinet – as elected representatives within liberal democracies are more often concerned with defending their actions (or inactions) and avoiding blame than they are with claiming credit. This is because voters are more inclined to cast their ballots to register their disapproval of a politician's performance than to signal approval.[43] Unlike high-profile portfolios, such as finance or foreign affairs, that are sought after in part because these can be used to enhance a minister's prestige, ministerial portfolios for intelligence offer very little ammunition in the wider struggles that constitute parliamentary politics. In other words, like a metaphorical "ticking timebomb" intelligence portfolios constitute a high-risk but low-reward proposition for ministers. The contestation over ministerial responsibility for intelligence agencies appears lacklustre when compared to parliamentary struggles over, say, managing the economy, advancing tax policy, or delivering health and education outcomes, because most of the agents in the field, including the leader of the opposition and the opposition's spokesperson for intelligence matters, adopt conservative strategies. According to Bourdieu:

> Those in dominant positions operate essentially defensive strategies, designed to perpetuate the status quo by maintaining themselves and the principles on which their dominance is based. The world is as it should be, since they are on top and clearly deserve to be there; excellence therefore consists in being what one is, with reserve and understatement, urbanely hinting at the immensity of one's means by the economy of one's means, refusing the assertive, attention-seeking strategies which expose the pretensions of the young pretenders. The dominant are drawn towards silence, discretion and secrecy …[44]

Equipped with the power to set the legislative and executive agendas, the prime minister sits at the apex of parliamentary politics and wields a monopoly on the capital needed to consecrate parliamentary agents as ministers or to relieve ministers of their portfolios. Indeed, the national field of

power is not only structured by the relationship of each agent to the prime minister's dominance, but also by the struggles among those agents to secure the benefits associated with that dominant position. Few agents involved in parliamentary politics and who covet the prime minister's position wish to see its power fettered. Indeed, most agents have an interest in ensuring their dominance in the field by protecting the post's prestige from scandals and controversies flowing from intelligence activities. That is why, using their law-making powers, parliamentarians insulated the prime minister from further scandals through the introduction of the Intelligence and Security Act in 2017. It is a Faustian pact that allows intelligence professionals to inhabit the national bureaucracy while belonging to a transnational guild, but where intelligence scandals embroil responsible ministers those intelligence professionals must carry the blame.

Using oversight measures to turn a blind eye

Whereas intelligence scandals are seized as opportunities to remediate the democratic controls over New Zealand intelligence activities in ways that shield the responsible ministers from blame, inquisitorial oversight measures not only place those ministers beyond scrutiny but also facilitate the ongoing engagement of New Zealand intelligence professionals within the transnational guild while paying little regard to ways in which that guild enables the secret use of state violence.

The ISC performs its oversight by questioning the Directors-General of the GCSB and the NZSIS on matters expressed in their classified annual reports. Unlike regular select committees of the House of Representatives, the ISC is more or less closed to the public and does not call for public submissions to inform its deliberations.[45] While the ISC has a statutory responsibility to provide a report on its business to the House of Representatives each year, until very recently the committee issued reports which merely noted the dates upon which it met. It now notes changes in membership and the official information it received but remains silent on its deliberations.[46] The committee's inquisitorial gaze does not cover sensitive intelligence activities, nor is it self-reflective.[47] The quality of inquisitorial oversight is limited by the composition of the committee as few of its members have the subject-matter expertise on intelligence needed to engage meaningfully on complex and dynamic intelligence matters. While the ISC remains chaired by the prime minister and includes members of the opposition, its membership was expanded from five to seven parliamentarians in 2017. In any case, the minister responsible for the GCSB and the NZSIS is caught in a conflict of interest because they are a standing member of the committee, instead of being called before it to answer questions on the agencies. When that minister is involved in authorising intelligence warrants, they become deeply entangled in the agencies' routine operations and this can jeopardise the committee's willingness to hold the agency to account if required to do so. Chairing the ISC as the minister responsible for national security and

intelligence places the prime minister in a conflict of interest too. Put simply, the oversight performed by the ISC is compromised because the committee is holding itself to account and the executive power over intelligence matters wielded by prime minister is largely unfettered.

Periodic statutory reviews are a way of bolstering the ISC's limited inquisitorial reach, but only one such review has been completed, though a second is currently underway. These statutory reviews focus on the legislative frameworks governing the two intelligence and security agencies in part to demonstrate the oversight measures "provide sufficient safeguards at an operational, judicial and political level to ensure the GCSB and NZSIS act lawfully and maintain public confidence."[48] While the first reviewers' recommendations were wide-ranging, their report did not consider the roles played by relevant ministers and ISC members, thereby exempting those with executive power from scrutiny. Nor does it include an independent and expert assessment of the significance of the transnational dimension of New Zealand's intelligence activities and its relationship to state violence. It did not consider the material and ideational conditions that gave rise to the GSCB and the NZSIS in the first place, and whether or not those conditions had changed or are in the process of changing.

The scope of the IGIS's investigatory powers was recalibrated to match the intelligence agencies functions under the Intelligence and Security Act 2017. The prohibition on inquiring into any matter that is operationally sensitive, including matters relating to intelligence collection, methods, and sources, was removed in 2013 following the abovementioned revelations that the GCSB had unlawfully undertaken surveillance of Dotcom. The role also became a fulltime position too, having previously been held by a retired Judge who worked part-time without any investigatory capacity.[49] Notwithstanding those changes, important limits to the powers of the IGIS remain and the scope the Inspector-General's inquisitorial gaze still does not extend to parliamentarians. The Inspector-General cannot declare intelligence warrants invalid where serious deficiencies are identified in those authorisations and the IGIS's powers are easily undermined when intelligence professionals refuse to cooperate.[50] IGIS is not empowered to examine the use of all products and services provided by the NZSIS and the GCSB to all of its "customers" within the wider intelligence community or examine the use of all products, services, and capabilities shared by the NZSIS and/or the GCSB with its "cooperating agencies" who are authorised to use force.[51] Furthermore, the Inspector-General is not empowered to examine the use of intelligence reports by ministers of the Leader of the Opposition. The IGIS is not empowered to examine all information that flows between New Zealand intelligence professionals and their transnational guild, as well as the activities of New Zealand intelligence professionals working at foreign intelligence organisations and foreign liaison officers working at the NZSIS or the GCSB. IGIS does not have the power to inquire into the use of New Zealand intelligence, equipment, or techniques by foreign intelligence professionals.

These limitations mean the responsible minister is insulated from the IGIS's scrutiny when controversy arises. Having undertaken a *motu proprio* inquiry into any possible involvement of the GCSB and the NZSIS with the CIA's detention and interrogation programme between September 2001 and January 2009, the IGIS reported she was satisfied, neither New Zealand intelligence professionals were directly involved in the CIA's unlawful activities, nor were any complicit in any unlawful conduct, though she conceded that "the nature of signals intelligence activity means GCSB involvement of that kind cannot be completely ruled out. In any event such involvement would have been a step distant from any kind of direct involvement."[52] While the IGIS found evidence of New Zealand intelligence professionals receiving information from CIA detainee interrogations, and of the NZSIS providing questions for the CIA to put to a detainee and receiving intelligence reports in response to those questions, blame was put exclusively on the agencies as "the Prime Minister and ministers were not informed and enabled to make decisions about how to deal with the risks in the context of New Zealand's overall relationship with its foreign partners."[53] Moreover, having undertaking a *motu proprio* inquiry into the role played by the GCSB and the NZSIS in supporting the NZSAS in Afghanistan,[54] where the focus was broader than the legality of New Zealand intelligence activities by considering the propriety of those activities, the Acting IGIS found that the intelligence agencies "could have done more to ensure that the reasonable possibility there had been civilian casualties was considered at an interagency level and reported to ministers." It further insulated the ministers responsible when it states: "Our inquiry finds that the intelligence agencies must take responsibility for identifying and managing risks from their participation in the wider New Zealand military enterprise. These risks are not solely the responsibility of other parts of Government."[55] When the IGIS investigated the release of information concerning an NZSIS briefing to the Leader of the Opposition on Israeli intelligence matters, it found that the NZSIS provided information to Slater that was incomplete, inaccurate, and misleading and provided similar, yet more detailed, information to the Prime Minister and his office.[56] It found, too, that the NZSIS not only failed to clarify or correct the information they had disclosed after the impact of these errors became apparent, but also denied the information requests made by political news reporters while granting the request made by Slater. The report arising from the inquiry was highly critical of the NZSIS and of the Director-General's lack of judgement in managing the controversy. Even though the report revealed that a staff member from Key's office provided the NZSIS information to Slater for Key's political advantage, the inquiry could not focus on the conduct of the Prime Minister's office.

If these oversight measures facilitate the ongoing engagement of New Zealand intelligence professionals in the transnational guild that enables the secret use of state violence while shielding from scrutiny those who have the greatest responsibility for the agencies in question, then the invention of a

national security system has been an effective way of refocusing attention on the value New Zealand intelligence activities deliver to the New Zealand public. New Zealand intelligence professionals have long heralded the contribution their protective services make to preserving the integrity of New Zealand's democratic institutions, values, and traditions, as well as the role intelligence plays in protecting the population of New Zealand and New Zealanders abroad from harms caused by political violence.[57] However, defining national security as "the condition which permits the citizens of a state to go about their daily business confidently free from fear and able to make the most of opportunities to advance their way of life. It encompasses the preparedness, protection, and preservation of people, and of property and information, both tangible and intangible" radically expanded the "value add" of intelligence to a wide variety of policy areas.[58]

Constructing a national security system around this expansive definition enables the GCSB's responsibilities and duties under its international intelligence agreements to be reframed as a means of pursing national security ends, that is, as strategic and operational capability extenders. Even though the GCSB's routine surveillance operations on Solomon Telekom, Vodafone Fiji, and Nauru Digicel are undertaken in accordance with its division of effort responsibilities under the UKUSA Agreement,[59] these types of activities are justified publicly as adding value to New Zealand diplomacy in the region, especially in relation to questions of stability and security. The radio interception capability at Tangimoana and the satellite communications interception capability at Waihopai, both now decommissioned, which were essential for the GCSB to fulfil its division of collection effort responsibilities, were nonetheless portrayed as key to New Zealand national security.[60] Moreover, an Annual Report from the GCSB claims that:

> [i]t is not possible for an organisation the size of GCSB to collect foreign intelligence on all matters relevant to New Zealand's interests. However, through long-standing relationships with our Five Eyes partners we can draw on greater support, technology and information than otherwise be available to us.[61]

This reframing of international intelligence partnerships as indispensable means of achieving the ends of New Zealand's national security is uncritically accepted by intelligence professionals whose job security depends on accepting this logic, which has itself become conventional thinking and is now received wisdom within intelligence reviews.

In addition to its division of effort arrangements, the GCSB also makes so-called "niche" contributions to service the UKUSA Agreement, which are important to other signatories but are of no interest to New Zealand's security professionals.[62] The intelligence operations targeting the Bangladesh Rapid Action Battalion is case in point; the GCSB-led counter-terrorism operations in Bangladesh were useful to the CIA and served as one of the

primary sources of signals intelligence to the NSA.[63] Contributions, niche or otherwise, made by New Zealand intelligence professionals to the international partnerships are often cast as "paying our dues" and are heralded as a great return on a modest investment,[64] though few reports written for policymakers in Washington D. C. will speak directly to the most pressing concerns of New Zealand policymakers based in Wellington.

This invention of a national security system serves the interests of those ministers with responsibilities for New Zealand intelligence agencies because it reduces political risk accompanying ministerial portfolios. When intelligence activities are managed by public servants as part of the national security system, ministers can push blame onto them if scandals unfold, remaining above the fray when controversy attaches to espionage, torture, extraordinary rendition, black sites, and the intentional killing of civilians. Regardless of the definition at its heart, the invention of a national security system distracts attention away from the secret use of violence that intelligence enables, drawing debates over intelligence matters in terms that seek to "balance" between "security" and "liberty." Ministers are thus recused of justifying how and why New Zealand intelligence professionals support and enable the United States' use of violence in a global battlespace, which is currently without temporal and geographic restriction, and includes signature drone strikes that do not require target identities to be confirmed.[65] More than a direct form of violence against its adversaries, US-led economic globalisation is a form of war with disastrous consequences for the Global South and "US strategy – the framework by which it seeks both peace and security for itself and its allies – is essentially one of annihilation, derived from, and sustained at almost every turn by the historical development of the United States."[66] At the same time, security officials advise the prime minister that "… national security is also a way to promote and protect the achievement of national goals and outcomes; it is a lever that supports the pursuit of economic opportunities and the progression of international relationships, and helps to build a sense of community among citizens when faced with challenges." For instance, New Zealand's ongoing engagement with the transnational guild can be used as a diplomatic key to unlock doors in the corridors of power in Washington, D.C.[67] Instrumentalizing New Zealand's agency on the transnational field of surveillance and intelligence in this way is valuable to ministers seeking to prevail in contestations animating the national field of power. Minimising political risks and maximising political gain keeps New Zealand intelligence professionals engaged with their transnational guild.

Public ignorance as a guarantor of impunity

This chapter has argued that public accountability arrangements and oversight measures do not constitute strong forms of democratic control over New Zealand intelligence activities. This is, in part, because ministerial

responsibility is not effectively checked by an informed opposition, or by informed political news reporters, community leaders, academics, or members of the wider public that, together, might constitute a vibrant or robust civil society. This is also, in part, because the inquisitorial gaze that lies at the heart of the oversight measures genuflects to its authorising configurations of power and does not take a wide view that encompasses the transnational dimension of New Zealand's strategic and operational intelligence activities and its complicity with state violence. While the prime minister and the minister(s) responsible for the GCSB and the NZSIS have made occasional speeches on New Zealand's intelligence activities within and beyond parliament, widening the window of transparency on unclassified aspects of intelligence work, the primary concern of such speeches seems to be promoting the prime minister's or minister's performance.[68] Similarly, when the ISC, statutory reviewers, and the IGIS peer beneath the veil of secrecy that shrouds intelligence activities, they enact the limits of public knowledge on these matters because they cannot convey those secrets to the public. In situations when the classifications imposed by an originator of intelligence reports can restrict circulation and elude oversight, collection methods and targeted individuals remain secret but so too are some of the activities of the transnational guild which might be inimical to the interests and values of local communities and individual citizens.[69] Public gestures towards transparency do little to lift the veil of official secrecy that shrouds these agencies; even though accurate, timely and reliable information is important, this limited transparency is a necessary but insufficient condition because more information does not equate to a better informed public if the public do not possess the capability to understand that information or to act collectively on it. Consequently, those individuals with the greatest responsibilities for New Zealand's intelligence activities – by which I mean the prime minister, who remains responsible for New Zealand's national security and intelligence, and the relevant minister(s) responsible for the GCSB and the NZSIS – are granted the gift of impunity that ensures they are never held accountable for any violence committed at home and abroad which is enabled by the transnational guild.

This is not to say there is no dissent on intelligence matters within the national field of power. Agents adopting radical strategies, which aim to transform the field by redefining what is at stake in the professional struggles, tend to belong to minor political parties with little prospect of leading the government in the near term.[70] These agents tend to be newcomers or longer-standing agents who have weak prospects of being consecrated as a minister. Any radical strategies pursued within conventional practices, such as question time in the House of Representatives, appear naïve or out of order because they push against the received wisdom of the national field (or what Bourdieu might call the doxa) by questioning the value of New Zealand's involvement with the so-called Five-Eyes intelligence arrangement, disregarding the prestige that ministers might gain from attending high-profile

diplomatic gatherings overseas, including ministerial Five Eyes meetings and the occasional speaking opportunity at NATO. According to Bourdieu, "attempts at radical subversion have some chance of succeeding only if they can import the effects of external social change, such as morphological changes or economic constraints, and exploit them by retranslating them into the internal logics of the field."[71] The prospects of success in transforming this field are weak, however. While there is a large degree of homology between the social milieu and the national field of power which emerges from within that milieu, there is little public understanding of, interest in, or concern for intelligence activities within wider New Zealand society, except in the immediate aftermath of shocking events, such as Brenton Tarrant's attack on two Christchurch Mosques on 15 March 2019.

Indeed, Tarrant's attack was an act of terrorism that brought the activities of New Zealand's intelligence and security agencies into sharp focus for many parliamentarians, political news reporters, community leaders, and academics, prompting serious questions about the extent to which New Zealand's security arrangements were fit for purpose. Throughout the previous two decades, both the GCSB and the NZSIS had repeatedly justified their existence by highlighting their counter-terrorism credentials.[72] However, despite ever-growing budgets and staff numbers, as well as increased information collection and surveillance powers,[73] neither agency was able to help protect members of a religious community marginalised within New Zealand society from an Australian citizen who, livestreaming on social media, murdered fifty-one individuals and attempted to murder another forty. Perhaps more pernicious than the fear of harm from terrorist acts, a public unease developed around those intelligence professionals who conduct counter-terrorism activities within New Zealand.[74] Members of New Zealand's minority communities complained that, despite their well-founded fear of becoming the subject of hate crime and terrorism, they were regularly treated as a suspect community when intelligence professionals engaged with them for the sole purpose of cultivating informants as sources of information on their co-religionists. "They were watching us, not watching our backs," remarked one New Zealand Muslim for instance.[75] Public confidence in the intelligence and security agencies appeared to be quite low before Tarrant's attacks, however.[76] The ongoing circuits of exchange between the government's intelligence professionals and its violence workers lie at the heart of this unease.[77] This close working relationship is salient given the controversy surrounding the New Zealand Police's armed raids in the Urewera mountain range in October 2007 which, authorised under the Terrorism Suppression Act 2002, have been used to highlight New Zealand's history of colonial violence against Māori and the ongoing over-policing of indigenous communities.[78] More recently, unease arose around intelligence professionals' connection to the police surveillance team that shot at point blank range and killed Ahamed Aathil Mohamed Samsudeen (a Tamil Muslim refugee from Sri Lanka, with mental health problems) as he attacked shoppers with a knife

in a supermarket.[79] New Zealand intelligence professionals function as the eyes and ears of a new apparatus of control that emerges as the New Zealand Defence Force continues to undergo a process of civilianisation and the New Zealand Police become more militarised.[80]

It is to say, however, that there is not much in the way of electoral capital to contest ministerial power. Lacking here is an enfranchised public that can form an electorate rewarding or punishing at the ballot box those parliamentarian holding intelligence portfolios. While the limited degree to which the New Zealand public is informed about intelligence matters undermines this safeguard, the public's umpiring function is further circumscribed by New Zealand's Mixed Member Proportional electoral system and the pathways it provides for professionals of politics to become parliamentarians; that is, by winning 1 of 65 general electoral seats, or 1 of 7 Māori electorates, or by ranking sufficiently high on the list of a party that achieved more than 5% of the party vote an individual may enter the House of Representatives. When a minister's membership to the House of Representatives is obtained or maintained though the party list, as has been the case with the current and previous ministers for the GCSB and the NZSIS, the electorate's disapproval of that minister's performance is neutered. In the week preceding the 2014 General Election, new minor party Internet Mana hosted a public event, dubbed the "Moment of Truth," which sought publicly to "indict and convict the Prime Minister and his government in a single evening, based on testimony from celebrated 'leakers' [Edward Snowden and Julian Assange], joined by a US journalist [Glenn Greenwald] and Kim Dotcom himself."[81] The voting public did not appear to care, or if it did, it did not seem to harm the National Party's electoral fortunes as Key's political party was returned for a third term with its party vote, at 47%, consistent with its 2011 result.

Although the public accountability arrangements for New Zealand intelligence activities might be in the process of changing, this transformation is not intended to empower the citizenry to create new forms of capital that can restructure the national field of power. The Royal Commission of Inquiry into the Terrorist attack on Christchurch masjidain on 15 March 2019 kept blame off the minister by stating that "the subjects of counter-terrorism, intelligence and security had become politically and publicly toxic."[82] The inquiry recommended a minister be given responsibility to lead and coordinate New Zealand's counter-terrorism effort and be supported by a new national intelligence and security agency. Yet this proposal, if implemented, will likely obfuscate, rather than clarify, the line of accountability between intelligence activities and the minister responsible. The inquiry also recommended the ISC be strengthened "so that it can provide better and informed cross-parliamentary oversight of the national security system (including the counter-terrorism effort) and priority setting, and members can access sensitive information for such oversight."[83] Taking its lead from the government's social cohesion policy agenda, the inquiry forged strong links not only with the survivors and families of the victims, but also with Muslim groups and

indigenous communities as well. The commitment to social cohesion is evident, too, in the recommendations to introduce "public voice" to the governance aspects of the national security system.[84] However, the minister holding the intelligence portfolio is also now the minister leading the implementation of the inquiry's recommendations, undercutting the full remedial potential of the inquiry's intervention into intelligence oversight. Notwithstanding recommendations to include community representation on new committees and panels, and the establishment of the National Centre of Research Excellence for Preventing and Countering Violent Extremism, nothing appears to have been done to foster an informed citizenry. It seems that civil society participation in the national security system relies on winning coalitions built upon existing consensus between officials and civil society groups, which co-opts community leaders who are listened to but seldom heard, while marginalising dissenting voices. Although a poorly informed public and weak civil society make the art of governing populations easier, a docile and passive population undercuts the constitutional safeguards which comprise a set of umpiring-like practices that buttress the public accountability arrangements over intelligence matters. The minister's transformation agenda aims to enshrine a guarantee that the public remains unable to question the political impunity enjoyed by those who are supposed to be accountable to the public.

There are, of course, other actions that parliamentarians could choose to take, embracing a more inclusive notion of democratic security that rests on whole-of-society, rather than whole-of-government, approaches to security. The scrutiny performed by the ISC could be better informed by concerns integrity assurance officers raise over privacy rights and other human rights.[85] The terms of reference for periodic statutory reviews could include ministerial responsibilities. The scope of the IGIS's investigatory ambit could be expanded to include all users of intelligence products and services, including parliamentarians and security professionals who undertake violence work on behalf of their state. Parliamentarians could introduce a new function to be performed by the GCSB and the NZSIS where they must take active steps towards fostering a civil society sector, and complement these efforts with new rules on declassifying information as quickly as possible.[86] As I have argued elsewhere, parliamentarians could establish a Parliamentary Commission for Intelligence and Security as an independent source of authoritative information, analysis, and advice on New Zealand's security challenges.[87] The commission could raise the level of public awareness of intelligence matters and improve the public's capability to understand those matters, thereby fostering an informed citizenry. As an Officer of Parliament and independent from the executive, the lead commissioner(s) could investigate any matters where New Zealand's security may be adversely affected and they could assess the national security system – including New Zealand's intelligence professionals and violence workers, and their connections to each other, as well as transnational intelligence work – and the current public accountability arrangement and oversight measures. But intelligence executives and, more importantly, their

minister(s) and prime minister would baulk at such scrutiny and the attention it would draw because that would not help them to survive in the national field of power.

Conclusion

The anatomy of political impunity for those with the greatest responsibilities for New Zealand's intelligence and security agencies, including the ongoing engagement of New Zealand intelligence professionals with a transitional guild that coheres around the NSA and its global surveillance network, has two important elements that, in design and in practice, operate in symbiosis. The first element lies in a set of public accountability arrangements that comprise ministerial responsibilities, a parliamentary ISC, periodic statutory reviews, and an IGIS, as well as by occasional ad-hoc inquiries. The second element lies in official responses to various intelligence scandals, which are usually seized upon as opportunities to diffuse or obfuscate ministerial responsibility by allocating blame elsewhere, but always ensure the ongoing engagement of New Zealand intelligence professionals within the transnational guild. Despite the ongoing assurance, first given by former Prime Minister Sir Geoffrey Palmer but frequently echoed in official documents and reviews, that "[t]he reasons for having intelligence and security agencies to protect our countries interest at home in abroad are overwhelming … . The protections against misuse of powers are substantial … they are carefully regulated and controlled in the public interest,"[88] the public accountability arrangements are, in fact, made and remade to protect the interests of a transnational guild of intelligence professionals whose primary purpose is to enable various forms of state violence in contemporary world affairs without the citizenry's informed consent.

Bourdieu's concept of the field unlocks a compelling explanation for why this state of affairs prevails. New Zealand parliamentarians have long recognised that the ministerial portfolios for the GCSB and the NZSIS are a high-risk but low-value proposition, which makes ministerial responsibility, performance, and accountability for those agencies something of a comparatively minor, if not a trivial, sideshow in the wider struggles over the right to rule the realm that comprise the national field of power. Given most parliamentarians covet the position of the prime minister as the dominating agent in that field, they tend to pursue conservative strategies through their law-making powers because they want to benefit from the legislative and executive agenda-setting power of that position. Working together, parliamentarians have used their legislative power to remove the responsibility for intelligence matters from the prime minister. This chapter argues almost all the professionals of politics involved in parliamentary struggles pursue conversative strategies that tend to endorse efforts to insulate the position of the New Zealand prime minister from any serious blame flowing from intelligence scandals or failures for no other reason than because they hold in

common an ambition to become the dominant agent in the field or to maximise their benefit from that agent. Comparatively few professionals of politics prioritise the wellbeing of democracy ahead of their own parliamentary aspirations. The greatest obstacle to enacting stronger democratic controls over New Zealand intelligence activities is the conservative strategies used by parliamentarians to survive within their professional field and to ascend that field's hierarchy as far as their immediate circumstances, and own talents, allow.

This raises interesting questions about the position of New Zealand intelligence professionals as agents on the transnational field of surveillance and intelligence. New Zealand intelligence professionals were exceptional because they are the weakest of the five founding members of the transnational guild centred around NSA, though the fourth Labour Government's anti-nuclear policies placed that membership in jeopardy.[89] Many officials resisted this policy from its outset, frustrating then-Prime Minister David Lange.[90] But this indicates the strong degree of autonomy of that transnational field in relation to the national field of power. Given a raft of other smaller cadres of intelligence professionals from Belgium, Denmark, the Netherlands, Norway, and Sweden, among others, have joined the global surveillance network under SSEUR since the 1980s, New Zealand intelligence professionals might now be exemplary, offering a model of engagement for third parties. Given the expanding membership of this transnational guild, future research could cast more light on how the NSA manages its relationships with those who belong to the transnational guild in ways that ensure it continues to dominate the wider transnational field. How, for instance, does the NSA diffuse emerging surveillance technologies – from capabilities to intercept, firstly, radio communications and, secondly, satellite-borne communications and, now, digitalised communications over fibre-optic cables – among the transnational guild, enabling them to restructure the field in conservative ways? To what extent does the NSA's legal expertise inform surveillance laws passed by other national assembles? What goes on in Five Eyes ministerial meetings? What is the degree of autonomy that the transnational field enjoys from the wider field of power that constitutes the politics of contemporary world affairs, and who are the communities of interests or practice that might emerge from a global social milieu to enable strategies of resistance within that transnational field? If we want to better understand the ways in which the public accountability arrangements over intelligence activities operate in practice, then answers to these questions will be instructive, especially in efforts to dissect the anatomy of political impunity wherever it manifests.

Notes

1 Desmond Ball, Cliff Lord and Meredith Thatcher, *Invaluable Service: The Secret History of New Zealand's Signals Intelligence During Two World Wars* (Auckland: Resource Books, 2011).

2 Mary Wharton, "The Development of Security Intelligence in New Zealand, 1945–1957" Master of Defence Studies Thesis, Massey University, 2012.
3 New Zealand, alongside Australia, signed the UKUSA Agreement in 1956, eight years after Canada had done so and a decade after the Agreement was signed by its first parties: the United States of America and the United Kingdom. The original purpose of the UKUSA Agreement was to govern the relations of its parties in communications intelligence matters, which included the exchange of collateral material required for technical reasons. More specifically, each party agreed to exchange outputs produced by the following operations relating to foreign communications: collection and analysis of traffic; cryptanalysis, decryption, and translation; and acquisition of communications documents and equipment as well as information regarding communications organizations, procedures, practices, and equipment.
4 Didier Bigo, "Sociology of Transnational Guilds," *International Political Sociology* 10 (2016): 407–408.
5 I make this point in Damien Rogers, "Transversal Practices of Everyday Intelligence Work in New Zealand: Transnationalism, Commercialism, Diplomacy," in *Problematising Intelligence Studies: Towards a New Research Agenda*, ed. Hager Ben Jaffel and Sebastian Larsson. (London / New York: Routledge, 2022), 132–155. See also Didier Bigo, "Shared Secrecy in a Digital Age and a Transnational World" *Intelligence and National Security* 34, no. 3 (2019): 379.
6 S. 4AAA(1)(b) of the New Zealand Security Intelligence Service Act 1969 (repealed).
7 S. 7(1)(b) of the Government Communications Security Bureau 2003 Act (repealed).
8 S. 9(b) of the Intelligence and Security Act 2017.
9 SIGINT Seniors Pacific Group comprises agency leaders from Australia, Canada, France, India, Korea, New Zealand, Singapore, Thailand, the United Kingdom, and the United States, each with intelligence interests in the South Pacific region. SIGINT Seniors Europe Group includes agency leaders from Australia, Belgium, Canada, Denmark, France, Germany, Italy, Netherlands, New Zealand, Norway, Spain, Sweden, the United Kingdom, and the United States.
10 The *Cabinet Manual* (2017) states that: Ministers decide both the direction of and the priorities for their departments. They are generally not involved in their departments' day-to-day operations. In general terms, Ministers are responsible for determining and promoting policy, defending policy decisions, and answering in the House on both policy and operational matters. […] Ministers are concerned not only with the short-term performance of their departments, but also with the capability of their departments to continue to deliver government objectives in the longer term. Ministers' priorities for departments and the standard of performance expected of their departments are specified in key accountability documents. See paragraphs 3.7 & 3.14, respectively.
11 Part 6, subpart 2 of the Intelligence and Security Act 2017. See also Intelligence and Security Committee Act 1996 (repealed 28 September 2017).
12 S.235 of the Intelligence and Security Act 2017.
13 Part 6, subpart 2 of the Intelligence and Security Act 2017. See also Inspector-General of Intelligence and Security Act 1996 (repealed 28 September 2017).
14 See, for instance, William Young and Jacque Caine, *Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019*; See also the inquiry into the case of Dr William Sutch by Sir Guy Powles (16 July 1976), available at https://www.nzsis.govt.nz/assets/media/SutchOmbudsmanReport.pdf
15 Andrew D. Brunatti, "The architecture of community: Intelligence community management in Australia, Canada and New Zealand," *Public Policy and Administration*, 28 (2013): 119–143; Alexander Gillespie & Claire Breen, "The Security Intelligence Agencies in New Zealand: evolution, challenges and

progress," *Intelligence and National Security* 36, no. 5 (2021): 676–695; Geoffrey R, Weller, "Change and Development in the New Zealand Security and Intelligence Services," *Journal of Conflict Studies* 21, no. 1 (2001); and James Whibley, "One Community, Many Agencies: Administrative Developments in New Zealand's Intelligence Services," *Intelligence and National Security* 29, no. 1 (2014): 122–135.

16 Paul G. Buchanan, "Foreign Policy Realignment, Issue Linkage and Institutional Lag: The Case of the New Zealand Intelligence Community," in *New Zealand and the World: Past, Present and Future,* ed. Robert G. Patman et al. (Singapore: World Scientific, 2018): 373–390; Austin Gee & Robert G. Patman, "Small state or minor power? New Zealand's Five Eyes Membership, intelligence reforms, and Wellington's response to China's growing pacific role," *Intelligence and National Security* 36, no. 1 (2021): 34–50; and Anthony L. Smith, "Informing the National Interest: The Role of Intelligence in New Zealand's Independent Foreign Policy," in *New Zealand and the World: Past, Present and Future*, ed. Robert G. Patman et al. (Singapore: World Scientific, 2018): 343–358.

17 Robert G. Patman & Laura Southgate, "National security and surveillance: the public impact of the GCSB Amendment Bill and the Snowden revelations in New Zealand," *Intelligence and National Security* 31, no. 6 (2016): 871–887; and Valarie Redmond, "I Spy with My Not So Little Eye: A Comparison of Surveillance law in the United States and New Zealand," *Fordham International Law Journal* 37, no. 3 (2014): 733–776.

18 Jim Rolfe, "Intelligence, Accountability and New Zealand's National Security" in *New Zealand and the World: Past, Present and Future*, ed. Robert G. Patman et al. (Singapore: World Scientific, 2018): 359–371.

19 For an exception, see David Wilson, "The use of secret evidence in the New Zealand House of Representatives," *Australasian Parliamentary Review* 28, no. 2 (2013): 25–35.

20 For an excellent treatment of the genesis, autonomy, and heteronomy of this field, see the chapter by Ronja Kniep in this volume.

21 See, for instance, Andrew W. Neal, "The Parliamentarianism of Security in the UK and Australia" *Parliamentary Affairs* 74, no. 2 (2021): 464–482; Andrew Defty, "'Familiar but not intimate': executive oversight of the UK intelligence and security agencies," *Intelligence and National* Security 37, no. 1 (2022): 57–72; Andrew Defty, "Coming in from the cold: bringing the Intelligence and Security Committee into Parliament," *Intelligence and National Security* 34, no. 1 (2019): 22–37; and Ruth Blakeley, "Dirty Hands, Clean Conscience? The CIA Inspector General's Investigation of 'Enhanced Interrogation Techniques in the War on Terror and the Torture Debate," *Journal of Human Rights* 10, no. 4 (2011): 544–561.

22 Didier Bigo, "Violence Performed in Secret by State Agents: For an Alternative Problematisation for Intelligence Studies," in *Problematising Intelligence Studies: Towards a New Research Agenda*, ed. Hager Ben Jaffel and Sebastian Larsson (New York / London, Routledge, 2022), 223.

23 These controversies include: allegations of Soviet espionage by William Sutch, a senior public servant; the sabotage of the Greenpeace's Rainbow Warrior by French Secret Service agents; revelations about the GSCB's involvements in the secret Five Eyes alliance; Dr David Small's chance discovery of the NZSIS's unlawful surveillance of Aziz Choudhary, an anti-globalisation activist; and the deflation of a protective dome at GCSB Waihopai satellite communications interception station by peace protestors. See Graeme Hunt, *Spies and Revolutionaries: A History of New Zealand Subversion* (Auckland; Reed Publishing, 2007); Michael King, *Death of the Rainbow Warrior* (Auckland: Penguin, 1986); Nicky Hager, *Secret Power: New Zealand's Role in the International Spy Network* (Nelson: Craig Potton 1996); and Adi Learson, "Ploughshare at Waihopai" in *Pursing Peace in*

Godzone: Christianity and the Peace Tradition in New Zealand, ed. Geoffrey Troughton & Phillip Fountain (Wellington: Victoria University Press, 2018).

24 This was unlawful because the Government Communications Security Bureau Act 2003 stated that "the Director, any employee of the Bureau, and any person acting on behalf of the Bureau must not authorise or do anything for the purpose of intercepting the private communications of a person who is a New Zealand citizen or a permanent resident of New Zealand."

25 Darren Palmer & Ian J Warren, "Global Policing and the case of Kim Dotcom," *International Journal for Crime, Justice and Social Democracy* 2, no. 3 (2014): 105–119; and Damien Rogers, "Extraditing Kim Dotcom: a case for reforming New Zealand's intelligence community?" *Kotuitui: New Zealand Journal of Social Sciences Online* 10, no. 1 (2015): 44.

26 Kathleen M. Kuehn, "Framing mass surveillance: Analyzing New Zealand's media coverage of the early Snowden files," *Journalism,* 19, no. 3 (2017): 402–419; Kathleen Kuehn, *The Post- Snowden Era: Mass Surveillance and Privacy in New Zealand* (Wellington: Bridget Williams Books, 2016); and Damien Rogers, "Snowden and GCSB: Illuminating neoliberal governmentality?" in *Cyber Security and Policy: A Substantive Dialogue,* ed. Andrew Colarick et al. (Auckland: Massey University Press, 2017): 325–350.

27 United States Senate Select Committee on Intelligence, Committee Study of the Central Intelligence Agency's Detention and Interrogation Program (December 2014) (Senate Report); Executive Summary, available at https://www.intelligence.senate.gov/sites/default/files/press/executive-summary_0.pdf; see also Elsbeth Guild, Didier Bigo and Mark Gibney (ed.), *Extraordinary Rendition: Addressing the Challenges of Accountability* (London and New York, 2018).

28 Nicky Hager and Jon Stephenson, *Hit & Run: The New Zealand SAS in Afghanistan and the meaning of honour* (Nelson: Potton and Burton, 2017).

29 For more on intelligence scandals and public trust and confidence in New Zealand, see Damien Rogers and Shaun Mawdsley, "Restoring Public Trust and Confidence in New Zealand's intelligence and Security Agencies: Is a Parliamentary Commissioner for Security the missing key? *Policy Quarterly* 18, no. 1 (2022): 59–66; Damien Rogers and Shaun Mawdsley, "Reconfiguring the relationship between intelligence professionals and the public: A first step towards democratizing New Zealand's National Security?" *National Security Journal* 2021, 23 p. [online first September 2021, doi 10.36878/nsj20210929.02.]

30 Editorial, "Editorial: Kim Dotcom sets off year of fireworks for politicians"*New Zealand Herald* (online ed, Auckland, 27 December 2012); John Key, "PM releases results of the GCSB file review" (press release, 4 October 2002).

31 Nicky Hager, *Dirty Politics: How attack politics is poisoning New Zealand's political environment* (Craig Potton Publishing, Nelson, 2014).

32 Rebecca Kitteridge, *Review of Compliance at the Government Communications Security Bureau* (March 2013), 18.

33 *Ibid,* 9, but see also the full text of Recommendation 35, 75.

34 Michael Cullen and Patsy Reddy, *Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand* (29 February 2016), 14.

35 *Ibid,* 152.

36 *Ibid,* see also Annex C: Full List of Recommendation, 152–165.

37 Damien Rogers, "Intelligence and Security Act 2017: A Preliminary Critique" *New Zealand Law Review* 4 (2018): 656–692.

38 S. 193 of the Intelligence and Security Act 2017.

39 See Government Communications Security Bureau and the New Zealand Security Intelligence Service, *Briefing to the incoming minister* (2017); and Government

Communications Security Bureau and the New Zealand Security Intelligence Service, *Incoming Minister's briefing* (2020).

40 This includes New Zealand Police and the New Zealand Defence Force as well as Immigration New Zealand within the Ministry for Business, Innovation & Employment, the New Zealand Custom Service, the Ministry for Primary Industries, Department of Internal Affairs and the Inland Revenue Department, among others.

41 See Doug Martin and Simon Mount, *Inquiry into the Use of External Security Consultants by Government Agencies,* 2018.

42 According to Pierre Bourdieu, a field is brought into existence through a recognition of the everyday struggles among a particular set of agents over some object or outcome those agents value. Fields emerge for a time out of some wider social space, or milieu, and are best conceptualised through the positions held by dominating and dominated agents, the evolving relations among them, and by the temporality of those relations. Hierarchies of agents are established, preserved or contested within the field through the conservative or radical strategies of those agents, some of whom are consecrated while others are newcomers, all of whom, however, rely on their own access to unequally distributed economic, social or cultural capital to exercise power over others. See Pierre Bourdieu, *Habitus and Field. General Sociology, Volume 2. Lectures at the College de France* (1982–1983) (Cambridge: Polity Press, 2020); Pierre Bourdieu, *The Field of Cultural Production* (New York: Colombia University Press, 1993); Pierre Bourdieu, *Homo Academicus* (Stanford: Stanford University Press, 1984).

43 R. Kent Weaver, "The Politics of Blame Avoidance," *Journal of Public Policy* 6, no. 4 (1986): 371–398.

44 Bourdieu, *Cultural Production*, 3.

45 Young and Caine, *Report of the Royal Commission*, 737.

46 See Intelligence and Security Committee, *Report of the Intelligence and Security Committee: Activities of the* Intelligence and Security Committee in 2021. The available transcript of the meeting shows members of the committee asking basic question on how the agencies operate.

47 Young and Caine, *Report of the Royal Commission,* 737.

48 Cullen and Reddy, *Intelligence and Security in a Free Society*, 148.

49 Cheryl Gwyn, "Speech" New Zealand Centre for Public Law Public Officeholders" Lecture Series "Spotlight on Security" Victoria University of Wellington's Faculty of Law, 4 May 2016.

50 This occurred during 2015, 2016 and 2017 when the Inspector-General undertook a review of the NZSIS's access and use of information held on a system managed by the New Zealand Customs Service, but found the NZSIS "reluctant to engage with [her] office on the substantive issues." Cheryl Gwyn, *Annual Report: For the year ended 30 June 2017*, 16.

51 That is, the New Zealand Defence Force and the New Zealand Police

52 Cheryl Gwyn, *Inquiry into possible New Zealand intelligence and security agencies' engagement with the CIA detention and interrogation programme 2001–2009* (Wellington: Office of the Inspector-General of Intelligence and Security, 2019) 6.

53 *Ibid*, 7.

54 The Inspector-General of Intelligence and Security's investigation occurred at the same time as the Burnham Inquiry, established by the Attorney-General under the Inquiries Act 2013. See Terrence Arnold and Geoffrey Palmer, *Report of the Government Inquiry into Operation Burnham and Related Matters* (2020).

55 Madeleine Laracy, *Report of Inquiry into the role of the GCSB and the NZSIS in relation to certain specific events in Afghanistan* (Wellington: Office of the Inspector-General of Intelligence and Security, 2020).

56 Cheryl Gwyn, *Report into the release of information by the New Zealand Security Intelligence Service in July and August 2011* (Wellington: Office of the Inspector-General of Intelligence and Security, 2014).
57 Unclassified annual reports can be found here: www.nzsis.govt.nz and www.gcsb.govt.nz.
58 These priorities were last updated in 2021. See https://dpmc.govt.nz/our-programmes/national-security/national-security-intelligence-priorities.
59 Radio New Zealand, "Solomons officials 'suspected' NZ was spying," *Radio New Zealand,* 18 March 2015.
60 Department of the Prime Minister and Cabinet, *Securing Our Nations' Safety: How New Zealand Manages its Security and Intelligence Agencies* (Wellington, 2000), 27.
61 Government Communications Security Bureau, *Annual Report 2016,*19.
62 Government Communications Security Bureau, *Annual Report 2009,* 6.
63 Hager and Gallagher 2015, cited in Damien Rogers, "Snowden and GCSB: Illuminating neoliberal governmentality? In *Cyber Security and Policy: A Substantive Dialogue,* ed. Andrew Colarik et al. (Auckland: Massey University Press, 2017): 217–238.
64 Cullen and Reddy, *Intelligence and Security in a Free Society,* 45. In their review of the agencies, Cullen and Reddy suggest that "New Zealand also gains considerably more from its international partnerships than we provide in return. For every intelligence report the NZSIS provides to a foreign partner, it receives 170 international reports. Similarly, or every report the GCSB makes available to its partners, it receives 99 in return." They conclude that "[t]he Five Eyes is by far New Zealand's most valuable intelligence arrangement, giving us knowledge and capability far beyond what we could afford on our own," 46. This reasoning is cited verbatim by Young and Caine in their report of the Royal Commission of Inquiry into the terrorist attack on Christchurch mosques on 15 March 2019.
65 See Samuel Moyn, *Humane: How the United States Abandoned Peace and Reinvented War* (New York: Farrar, Straus and Gilroux, 2021).
66 Michael McKinley, *Economic Globalisation as Religious War: Tragic Convergence* (London / New York: Routledge, 2007), 213.
67 Rogers, "Transversal Practices,"132–155.
68 See, for instance: John Key, "Speech" New Zealand Institute of International Affairs, Wellington 6 November 2014; and Andrew Little "Opening Address to the Massey University National Security Conference 2018," Auckland 5 April 2018.
69 For the dangers associated with the third-party rules which permit intelligence professionals to withhold partner-provided intelligence from parliamentary committees because such a release would violate transnational confidentially, see Kniep chapter in this volume.
70 Only the Green Party of Aotearoa New Zealand voted against the passing of the intelligence and Security Act 2017, for example (21 March 2017) 721 NZPD 16833.
71 Bourdieu, *Habitus and Field*, 198.
72 See recurring statements made in both agencies' annual reports over the past twenty years, found at www.nzsis.govt.nz and www.gcsb.govt.nz. For an analysis of those statements, see Damien Rogers and Shaun Mawdsley, *Turning the Dial from 'Social Licence' to 'Democratic Security': New Zealand's Intelligence and Security Agencies and the Case for an Informed Citizenry, July 2021*, accessed 7 August 2022, http://www.damienrogers.ac.nz.
73 Rogers, "Intelligence and Security Act 2017," 657.
74 The term is taken from Didier Bigo, "Security and Immigration: Towards a Critique of the Governmentality of Unease", *Alternatives* 27 (2002): 63–92. For more on transnationally circulated intelligence, see Sophia Hoffmann,"Circulation, not Cooperation: Towards a new understanding of intelligence agencies as

transnationally constituted knowledge providers," *Intelligence and National Security* 36, no. 6 (2021): 807–826.
75 William Young and Jacqui Caine, *Summary of Submissions*, (28 November 2020), 140.
76 Rogers and Mawdsley, "Reconfiguring the Relationship," *National Security Journal* 2021 [Online first 29 Sept 2021, doi 10.36878/nsj20210929.02.].
77 The term 'violence worker' is taken from Micol Seigal, *Violence Work: State Power and the Limits of Police* (Durham and London: Duke University Press, 2018), 10–11.
78 Danny Keenan (ed.), *Terror in our midst? Searching for terror in Aotearoa New Zealand* (Wellington: Huia, 2008). See also Jeffrey A. Sluka, "The Ruatoki Valley 'Antiterrorism Police Raids: Losing 'Hearts and Minds' in Te Urewera," *Sites: New Series* 7, no. 1 (2010): 44–64; and Adele N. Norris and Juan Tauri, "Racialized Surveillance in New Zealand: From the Tuhoe Raids to the Extralegal Photographing on Indigenous Youth," *Race and Justice* [first published online 13 December 2021].
79 New Zealand Security Intelligence Service, *Security Intelligence Report: Faith-motivated violent extremist Ahamed Aathil Mohamed Samsudeen potential release into the community*, dated 1 June 2021. Report DM56-15-1147, NZSIS, released by Official Information Act request, 15 November 2021.
80 I make this point in Rogers, "Intelligence and Security Act 2017," 688.
81 Stephen Levine, "Moments of Truth: The 2014 New Zealand general election," in *Moments of Truth: The New Zealand General Election of 2014*, ed. Jon Johansson and Stephen Levine (Wellington: Victoria University Press, 2015), 49.
82 Young and Caine, *Report of the Royal Commission*, 15.
83 *Ibid,* 24–25.
84 *Ibid,* 23–27.
85 These are the Chief Human Rights Commissioner, Race Relations Commissioner, the Privacy Commissioner, the Chief Ombudsman, and the Auditor-General.
86 Rogers and Mawdsley, "Reconfiguring the relationship."
87 Rogers and Mawdsley, "Restoring Public Trust and Confidence."
88 Department of the Prime Minister and Cabinet, *Securing Our Nation's Safety*, 16.
89 Gerald Hensley, *Friendly Fire: Nuclear Politics and the collapse of ANZUS, 1984–1987* (Auckland: Auckland University Press, 2013).
90 David Lange*, My Life* (London: Viking, 2005).

References

Arnold, Terrence, and Geoffrey Palmer. *Report of the Government Inquiry into Operation Burnham and Related Matters*. Wellington, 2020.

Ball, Desmond, Cliff Lord, and Meredith Thatcher. *Invaluable Service: The Secret History of New Zealand's Signals Intelligence During Two World Wars*. Auckland: Resource Books, 2011.

Bigo, Didier. "Security and Immigration: Towards a Critique of the Governmentality of Unease." *Alternatives* 27 (2002): 63–92.

Bigo, Didier. "Sociology of Transnational Guilds." *International Political Sociology* 10 (2016): 398–416.

Bigo, Didier. "Shared Secrecy in a Digital Age and a Transnational World." *Intelligence and National Security* 34, no. 3 (2019): 379–395.

Bigo, Didier. "Violence Performed in Secret by State Agents: For an Alternative Problematisation for Intelligence Studies." In *Problematising Intelligence Studies: Towards a New Research Agenda*, edited by Hager Ben Jaffel and Sebastian Larsson, 220–240. New York/London: Routledge, 2022.

Blakeley, Ruth. "Dirty Hands, Clean Conscience? The CIA Inspector General's Investigation of 'Enhanced Interrogation Techniques in the War on Terror and the Torture Debate." *Journal of Human Rights* 10, no. 4 (2011): 544–561.

Bourdieu, Pierre. *Homo Academicus*. Stanford: Stanford University Press, 1984.

Bourdieu, Pierre. *The Field of Cultural Production*. New York: Colombia University Press, 1993.

Bourdieu, Pierre. *Habitus and Field. General Sociology, Volume 2. Lectures at the College de France (1982–1983)*. Cambridge: Polity Press, 2020.

Brunatti, Andrew D. "The Architecture of Community: Intelligence Community Management in Australia, Canada and New Zealand." *Public Policy and Administration* 28 (2013): 119–143.

Buchanan, Paul G. "Foreign Policy Realignment, Issue Linkage and Institutional Lag: The Case of the New Zealand Intelligence Community." In *New Zealand and the World: Past, Present and Future*, edited by Robert G Patman, Iati Iati, & Balazs Kiglics, 373–390. Singapore: World Scientific, 2018.

Cabinet Manual. (2017), https://dpmc.govt.nz/sites/default/files/2017-06/cabinet-manual-2017.pdf

Cullen, Michael, and Patsy Reddy. *Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand.*

Defty, Andrew. "Coming in from the Cold: Bringing the Intelligence and Security Committee into Parliament," *Intelligence and National Security* 34, no. 1 (2019): 22–37

Defty, Andrew. "'Familiar but not Intimate': Executive Oversight of the UK Intelligence and Security Agencies." *Intelligence and National Security* 37, no. 1 (2022): 57–72.

Department of the Prime Minister and Cabinet. *Securing Our Nations' Safety: How New Zealand Manages its Security and Intelligence Agencies*. Wellington, 2000.

Editor. "Editorial: Kim Dotcom sets off year of fireworks for politicians." *New Zealand Herald*, online edition, Auckland, 27 December 2012.

Gee, Austin, and Robert G. Patman. "Small state or minor power? New Zealand's Five Eyes Membership, intelligence reforms, and Wellington's response to China's growing pacific role." *Intelligence and National Security* 36, no. 1 (2021): 34–50.

Gillespie, Alexander, and Claire Breen. "The Security Intelligence Agencies in New Zealand: evolution, challenges and progress." *Intelligence and National Security* 36, no. 5 (2021): 676–695.

Government Communications Security Bureau. *Annual Report: For the year ending 30 June 2016*.

Government Communications Security Bureau. *Annual Report: For the year ending 20 June 2009*.

Government Communications Security Bureau and the New Zealand Security Intelligence Service. *Incoming Minister's briefing* (2020).

Government Communications Security Bureau and the New Zealand Security Intelligence Service. *Briefing to the Incoming Minister* (2017).

Government Communications Security Bureau Act 2003 (repealed 28 September 2017), https://www.legislation.govt.nz/act/public/2003/0009/latest/DLM187178.html

Guild, Elsbeth, Didier Bigo, and Mark Gibney (eds). *Extraordinary Rendition: Addressing the Challenges of Accountability*. London/New York: Routledge, 2018.

Gwyn, Cheryl. *Report into the release of information by the New Zealand Security Intelligence Service in July and August 2011*. Wellington: Office of the Inspector-General of Intelligence and Security, 2014.

Gwyn, Cheryl. "Speech." In *New Zealand Centre for Public Law Public Officeholders Lecture Series "Spotlight on Security*. Victoria University of Wellington's Faculty of Law, 4 May 2016.
Gwyn, Cheryl. *Annual Report: For the year ended 30 June 2017*. Wellington: Office of the Inspector-General of Intelligence and Security, 2017.
Gwyn, Cheryl. *Inquiry into possible New Zealand intelligence and security agencies' engagement with the CIA detention and interrogation programme 2001–2009*. Wellington: Office of the Inspector-General of Intelligence and Security, 2019.
Hager, Nicky. *Secret Power: New Zealand's Role in the International Spy Network*. Nelson: Craig Potton, 1996.
Hager, Nicky. *Dirty Politics: How attack politics is poisoning New Zealand's political environment*. Nelson: Craig Potton Publishing, 2014.
Hager, Nicky, and Jon Stephenson. *Hit & Run: The New Zealand SAS in Afghanistan and the meaning of honour*. Nelson: Potton and Burton, 2017.
Hensley, Gerald. *Friendly Fire: Nuclear Politics and the collapse of ANZUS, 1984-1987*. Auckland: Auckland University Press, 2013.
Hoffmann, Sophia. "Circulation, not Cooperation: Towards a New Understanding of Intelligence Agencies as Transnationally Constituted Knowledge Providers." *Intelligence and National Security* 36, no. 6 (2021): 807–826.
Hunt, Graeme. *Spies and Revolutionaries: A History of New Zealand Subversion*. Auckland: Reed Publishing, 2007.
Inspector-General of Intelligence and Security Act 1996. (repealed 28 September 2017). https://www.legislation.govt.nz/act/public/1996/0047/latest/DLM392285.html
Intelligence and Security Act 2017. https://www.legislation.govt.nz/act/public/2017/0010/latest/DLM6920823.html
Intelligence and Security Committee. *Report of the Intelligence and Security Committee: Activities of the Intelligence and Security Committee in 2021*.
Intelligence and Security Committee Act 1996 (repealed 28 September 2017). https://www.legislation.govt.nz/act/public/1996/0046/latest/whole.html
Keenan, Danny (ed). *Terror in our midst? Searching for terror in Aotearoa New Zealand*. Wellington: Huia, 2008.
Key, John. "PM releases results of the GCSB file review." Press release, 4 October 2002.
Key, John. "Speech." New Zealand Institute of International Affairs, Wellington 6 November 2014.
King, Michael. *Death of the Rainbow Warrior*. Auckland: Penguin, 1986.
Kitteridge, Rebecca. *Review of Compliance at the Government Communications Security Bureau*, March 2013.
Kuehn, Kathleen. *The Post- Snowden Era: Mass Surveillance and Privacy in New Zealand*. Wellington: Bridget Williams Books, 2016.
Kuehn, Kathleen M. "Framing mass surveillance; Analyzing New Zealand's media coverage of the early Snowden files." *Journalism* 19, no. 3 (2017): 402–419.
Lange, David. *My Life*. London: Viking, 2005.
Laracy, Madeleine. *Report of Inquiry into the role of the GCSB and the NZSIS in relation to certain specific events in Afghanistan*. Wellington: Office of the Inspector-General of Intelligence and Security, 2020.
Learson, Adi. "Ploughshare at Waihopai." In *Pursing Peace in Godzone: Christianity and the Peace Tradition in New Zealand*, edited byGeoffrey Troughton and Phillip Fountain, 171–184. Wellington: Victoria University Press, 2018.

Levine, Stephen. "Moments of Truth: The 2014 New Zealand general election." In *Moments of Truth: The New Zealand General Election of 2014*, edited byJon Johansson and Stephen Levine, 29–69. Wellington: Victoria University Press, 2015.

Little, Andrew. "Opening Address to the Massey University National Security Conference 2018." Auckland 5 April 2018.

Martin, Doug, and Simon Mount. *Inquiry into the Use of External Security Consultants by Government Agencies*, 2018.

McKinley, Michael. *Economic Globalisation as Religious War: Tragic Convergence*. London / New York: Routledge, 2007.

Moyn, Samuel. *Humane: How the United States Abandoned Peace and Reinvented War*. New York: Farrar, Straus and Gilroux, 2021.

Neal, Andrew W. "The Parliamentarianism of Security in the UK and Australia." *Parliamentary Affairs* 74, no. 2 (2021): 464–482.

New Zealand Security Intelligence Service. *Security Intelligence Report: Faith-motivated violent extremist Ahamed Aathil Mohamed Samsudeen potential release into the community*, dated 1 June 2021. Report DM56-15-1147, NZSIS, released by Official Information Act request, 15 November 2021.

New Zealand Security Intelligence Service Act 1969. (repealed 28 September 2017). https://www.legislation.govt.nz/act/public/1969/0024/latest/whole.html

Norris, Adele N., and Juan Tauri. "Racialized Surveillance in New Zealand: From the Tuhoe Raids to the Extralegal Photographing on Indigenous Youth." *Race and Justice* [first published online 13 December 2021].

Palmer, Darren, and Ian J. Warren. "Global Policing and the Case of Kim Dotcom." *International Journal for Crime, Justice and Social Democracy* 2, no. 3 (2014): 105–119.

Patman, Robert G., and Laura Southgate. "National security and surveillance: the public impact of the GCSB Amendment Bill and the Snowden revelations in New Zealand." *Intelligence and National Security* 31, no. 6 (2016): 871–887.

Radio New Zealand. "Solomons officials 'suspected' NZ was spying." *Radio New Zealand*, 18 March 2015.

Redmond, Valarie. "I Spy with My Not So Little Eye: A Comparison of Surveillance law in the United States and New Zealand." *Fordham International Law Journal* 37, no. 3 (2014): 733–776.

Rogers, Damien. "Extraditing Kim Dotcom: A Case for Reforming New Zealand's Intelligence Community?" *Kotuitui: New Zealand Journal of Social Sciences Online* 10, no. 1 (2015): 46–57.

Rogers, Damien. "Snowden and GCSB: Illuminating neoliberal governmentality?" In *Cyber Security and Policy: A Substantive Dialogue*, edited byAndrew Colarick, Julian Jang-Jaccard and Anuranda Mathrani, 325–350. Auckland: Massey University Press, 2017.

Rogers, Damien. "Intelligence and Security Act 2017: A Preliminary Critique." *New Zealand Law Review* 4 (2018): 656–692.

Rogers, Damien. "Transversal Practices of Everyday Intelligence Work in New Zealand: Transnationalism, Commercialism, Diplomacy." In *Problematising Intelligence Studies: Towards a New Research Agenda*, edited byHager Ben Jaffel and Sebastian Larsson, 132–155. London / New York: Routledge, 2022.

Rogers, Damien and Shaun Mawdsley. *Turning the Dial from 'Social Licence' to 'Democratic Security': New Zealand's Intelligence and Security Agencies and the Case for an Informed Citizenry, Unpublished Report July 2021*, accessed 7 August 2022, http://www.damienrogers.ac.nz.

Rogers, Damien, and Shaun Mawdsley. "Reconfiguring the relationship between intelligence professionals and the public: A first step towards democratizing New Zealand's National Security?" *National Security Journal* (2021), 23 p. [online first September 2021. 10.36878/nsj20210929.02].

Rogers, Damien, and Shaun Mawdsley. "Restoring Public Trust and Confidence in New Zealand's intelligence and Security Agencies: Is a Parliamentary Commissioner for Security the missing key? *Policy Quarterly* 18, no. 1 (2022): 59–66.

Rolfe, Jim. "Intelligence, Accountability and New Zealand's National Security." In *New Zealand and the World: Past, Present and Future*, edited by Robert G. Patman, Iati Iati and Balazs Kiglics, 358–372. Singapore: World Scientific, 2018.

Seigal, Micol. *Violence Work: State Power and the Limits of Police*. Durham/London: Duke University Press, 2018.

Sluka, Jeffrey A. "The Ruatoki Valley 'Antiterrorism Police Raids: Losing 'Hearts and Minds' in Te Urewera." *Sites: New Series* 7, no. 1 (2010): 44–64.

Smith, Anthony L. "Informing the National Interest: The Role of Intelligence in New Zealand's Independent Foreign Policy." In *New Zealand and the World: Past, Present and Future*, edited byRobert G. Patman, Iati Iati and Balazs Kiglics, 343–358. Singapore: World Scientific, 2018.

United States Senate Select Committee on Intelligence, Committee Study of the Central Intelligence Agency's Detention and Interrogation Program. (December 2014). (Senate Report); Executive Summary, available at https://www.intelligence.senate.gov/sites/default/files/press/executive-summary_0.pdf

Weaver, R. Kent. "The Politics of Blame Avoidance," *Journal of Public Policy* 6, no. 4 (1986): 371–398.

Weller, Geoffrey R. "Change and Development in the New Zealand Security and Intelligence Services." *Journal of Conflict Studies* 21, no. 1 (2001).

Wharton, Mary. "The Development of Security Intelligence in New Zealand, 1945-1957." Master of Defence Studies Thesis, Massey University, 2012.

Whibley, James. "One Community, Many Agencies: Administrative Developments in New Zealand's Intelligence Services." *Intelligence and National Security* 29, no. 1 (2014): 122–135.

Wilson, David. "The Use of Secret Evidence in the New Zealand House of Representatives." *Australasian Parliamentary Review* 28, no. 2 (2013): 25–35.

Young, William, and Jacque Caine. *Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019*. https://christchurchattack.royalcommssion.nz/the-report/

Young, William, and Jacque Caine. *Summary of Submissions*, 28 November 2020.

8 Liberty, equality, and counter-terrorism in France[1]

François Thuillier

1 *Your personal career, in which you have been both in the active services (RG, DST), in coordination (UCLAT, French Embassy in London) and in places of strategic reflection (IHESI, DGPN Cabinet), has led you to produce several books (L'Europe du secret in 2000, La révolution antiterroriste in 2019, Homo Terrorismus in 2020) which develop a fundamental thesis on the originality of France's anti-terrorist policy in the mid-1980s and its transformation linked to the evolution of European anti-terrorist policies and the influence of modes of action and conceptions from across the Atlantic. Could you please outline for us what you think are the main characteristics of this French trajectory that have organised the counter-terrorism space?*

Everything indicates that a French model did indeed exist at one time, since the way in which each State contains political violence is the result of its history and institutional balance. In this respect, since the rebirth of modern terrorism at the end of the 1960s, France had built a doctrine that was unique to it. Within the framework of a State governed by the rule of law and under the supervision of the judicial and constitutional courts, the following principles seemed to apply:

- A permanent and indiscriminate state of vigilance over the entire spectrum, without any ideological preconceptions; the principle of secularism, for example, prevents any religious justification from being taken into account.

- Targeted intelligence placed as close to the ground as possible. Out of concern for efficiency, out of colonial heritage, and due to the lack of mass intelligence tools, the internal and external services were more particularly inclined to human intelligence, which was better able to grasp the nuances and the long timeframe of complexities. So-called "security" intelligence with a purely operational aim remained the poor relation of services jealous of their independence.

- The fragmentation and complementarity of specialised services. This legacy of the 1930s aimed to dilute the power that a single intelligence service could have had to hold the country together, and to enrich political

DOI: 10.4324/9781003354130-9

decision making with all the professional cultures and research angles of agencies of equal legitimacy and simply coordinate with one another.

- The fight against terrorism was a public policy steered like any other from Matignon in its inter-ministerial dimension and the Ministry of the Interior in its operational dimension. Its technical management prevailed over any desire for partisan instrumentalisation and its agencies were kept at a prudent distance from the places of power.

- Careful strategic independence was sought. The fight against terrorism remained a national prerogative, alien to the dynamics of integration (NATO, the European Union, various coalitions) and to strategies of influence from abroad.

This posture resembled a sort of "Latin intelligence model", insofar as it emanated from old Mediterranean countries that had been hit by terrorism from the outset and were subsequently coveted by numerous authoritarian regimes. The centuries had forged a kind of philosophy of political violence with the constant concern to de-ideologise it and to de-exceptionalise the response. Attacks were commonplace and rarely the pretext for partisan jousting and political recuperation. Without idealising the near past, it seems to me that, despite a level of threat much higher than what we know today, the fight against terrorism remained a matter for professionals preserved from power issues.

However, the French doctrine of counter-terrorism has not ceased to be radicalised for half a century, independently of the current state of political crime. After a brief attempt to reduce security with the abolition of the State Security Court in 1982/83, our posture was then mainly guided by the exception, the increased repression of the law, the specialisation and centralisation of actors, the use of mass intelligence, etc. This slope, which was supposed to respond to a supposed radicalisation of the threat, was not followed by a more radical approach. Instead, the approach remained faithful to our political traditions. The last trace of this can be found in the 2006 *White Paper on France's response to terrorism*, which rejected the terms "war" (in favour of an ordinary fight against a crime) and "Islamism" (out of respect for our Muslim population, our partner countries in the southern Mediterranean, and our secular principles).

Everything changed the following year with the election of Nicolas Sarkozy and the alignment of our counter-terrorism policy with Anglo-Saxon principles: adoption of the controversial notion of "national security" (White Paper of 2008), return to NATO (2007/2009), importation of the concept of "radicalisation" (after the Merah affair in 2012) and of war rhetoric (Bataclan, 2015), the assumed recourse to counter-terrorism and targeted assassinations, etc. This return to the Western rule was coupled with a verticalisation and therefore a politicisation of the response: creation of the National Intelligence Advisor directly to the President of the Republic (2008, then CNRLT in 2017), of the DCRI (2008, then the monopoly of the DGSI in 2014/2018), of the National Anti-Terrorist Prosecutor's Office (2019); and

justification for the increase in means of surveillance of the population: explosion of the DGSE's technical capacities put at the service of domestic intelligence, expansion of the possibilities of filing (EDVIGE project, abandoned in 2008), challenge to European values in terms of civil liberties (on the generalised conservation of connection data for example), etc.

On examination, it becomes clear that this shift has been influenced in two ways that are quite revealing of the trajectory taken by France in other areas during the last three quinquennia:

First of all, that of Anglo-Saxon soft power, which has used anti-terrorist cooperation, especially since 1989 (fall of the Berlin Wall), and then 2001 ("war on terror"), to tighten the West's strategic ties when it was most needed. The war in Ukraine today provides the same arguments.

Secondly, that of the security lobby (surveillance capitalism, control industries, the new criminology, the conservative press, etc.), which has perceived the economic and symbolic interest of this shift by setting itself up as a merchant of fear and becoming the "secondary beneficiaries" of terrorist crime.

2 *Does this trajectory have to do with France's values, its positioning, or is it a more common trajectory of intelligence services in non-Anglo-Saxon countries, which can be found not only in southern Europe, but in fact just about everywhere, in Europe, in Latin America … ? Isn't the exception finally the choice of the British to recruit differently, to create different modes of coordination, to think of themselves as "intellectuals, as intelligent" and the Americans who add to this their financial and human superiority and their belief in maximum technology and security optimism. I'm thinking here of the trope of "refusing to negotiate with terrorists", which Thatcher proclaimed whilst simultaneously being engaged in discussions with the IRA, and above all, in the US, where the certainty that wars against terrorists can be won, which resulted in a general push of the autonomy of action of the services, the impetus to create fusion centres between services, demanding the circulation and sharing of information between agencies … This leads them to a very unfocused suspicion and to the development of discourses on (aggressive) prevention, as well as to a return to predictive intelligence (improved lie detection, facial recognition, artificial intelligence.)?*

As far as our country is concerned, I think it is important to understand that France was built on a paradox. It is not so much the republican hope and its mad hope of a society that is more just and more respectful of human rights that characterises it, but the constantly renewed failure to achieve it. Having caught a glimpse of the Enlightenment, we behave like a people who thought they saw their god but have since become convinced of their collective hallucination. We have measured the distance between us and the Republic (*res publica*) and this has discouraged us. And since then we have remained a reactionary, inegalitarian, counter-revolutionary society, with the only difference from our neighbours being that we are secretly ashamed of having betrayed our vocation.

All this undoubtedly explains the influence games, especially foreign ones, which are exercised and the sometimes disconcerting, often erratic ease with which they impose themselves on our soil in a few months after having come up against our mistrust and contempt. With each step backwards, we give the impression that we are falling from a greater height than our "allies" who appear, in comparison, to be more stable and constant, and above all more aware of their capacity to influence.

This is the case, for example, of everything concerning the "war on terrorism"; and the way in which we have adopted the Anglo-Saxon model of "fighting radicalisation" is the most edifying proof of this. Let us remember that this ideology, developed by and for countries with a communitarian tradition and a state religion, i.e. the exact opposite of our Republic, had always been kept at bay by our leaders and our specialised services until 2012. Apart from the fact that our secular tradition prevented us from venturing into the religious field in terms of crime prevention, sociology had long since shown us that, in terms of the act, violent intentionality preceded the passage through Islam. Islam was at best a facilitator, a pretext, and a justification, but in no way a significant determinant of crime. "Fighting against the deviations of a religion" thus appeared to us to be a dead end, a counter-productive and deleterious method, or even a disguised racism.

In 2012, the Merah affair (a young man from Toulouse, despite having been identified by local services, murdered seven people, including three children in a Jewish denominational school) seemed to call into question the French doctrine. The DCRI, criticised for having failed to evaluate the dangerousness of the criminal, was weakened. The political authorities, against the backdrop of the presidential elections, demanded announcements. The General Secretariat for Defence and National Security (SGDSN) took advantage of the situation to rush into the breach and propose a plan to fight radicalisation directly inspired by its meetings with London and the bilateral discussions on security held on a regular basis since the Saint-Malo agreements (1998).

A desperate Ministry of the Interior hastily seized on the project and imposed it, without an impact study, on the entire French anti-terrorist community. France was the last European country to fall into this ideology that the British had skilfully exported to the continent thanks to the empathy they had aroused in the Member States in July 2005 at the time of the London bombings, and above all thanks to their concurrent presidency of the Council of the European Union.

This episode says it all about our political lurch. We had developed a unique expertise and experience in Europe because of our long history of being a victim of political violence. As the country most affected by attacks for half a century, France had its own doctrine that regularly aroused the interest of its partners. And in a few months, foreign influences skilfully playing on the competition between agencies, the personal ambition of

their leaders and the ignorance of our long history by the political class have swept everything away, bringing us pitifully back into the rule of a West at war with terrorism.

3 *You have developed a thesis that distances itself from those of other analysts who claim to be very close to the services, even though their background is very far from yours. How would you characterise your intellectual approach and your reflection on your experience during your professional life and beyond? Can you explain to us what is lacking in these theses that only talk about the terrorist threat and the responses of the services, supposedly always in a hurry and ill-prepared, ill-equipped? What were the moments when events changed almost nothing? Or did the policy of the past become stronger? And what are the ones that in the short or medium term have affected all anti-terrorist policies?*

I have indeed been lucky enough to spend time – nearly 30 years – and to diversify my professional experience within the structures that develop and apply French anti-terrorist and intelligence policy. This inevitably forges an awareness of the issues involved in security. Albert Camus said that "in the randomness of the worlds and men we meet, it takes ten years to have an idea of one's own, of which one can speak". But it was a useful training period because it exonerates me today from the trials of angelism of naive idealism brought against researchers in my camp.

Indeed, we cannot limit our thinking about war (since that is what it is all about) to its ends without also reflecting on the means used: who calls for war, according to what arguments, who benefits from it, what changes does it bring about in our social organisation, etc. We cannot win a war without being clear about what we have to defend, without asking ourselves whether the way we behave "at the front" does not contradict what we are "at the back". Otherwise, we lose both the war and the peace. This is what could sum up my professional and civic career.

It therefore seemed to me that only critical security studies, through their effort to deconstruct, provided the theoretical means to understand what was really at stake around the notions of violence and order, and made it possible to mobilise the knowledge and energies necessary to rebuild what the ancients called the Republic. But above all, it became clear to me that the approximations and the obscurity maintained by the "security school" were weakening us in the face of the threat. Moreover, this school was made up of actors who, surprisingly, were linked to it because they derived economic, political, media, and academic benefits from it. They therefore had a vested interest in dramatising it and became somewhat complicit in it. These "secondary beneficiaries" of terrorist crime, these receivers of terror, combining suspicious partisan connivances and charlatanism, whom I have come into contact with during my professional career, have clearly acted as a repellent in my approach.

I have indeed kept, from my time in the services, the concern for operational efficiency. This is not achieved through bluster, overplayed

brutality, or declarations of war, but above all through clear-sightedness. It is this discernment that we lack today and which alone will enable us to win this battle. At a time when, for example, the last health crisis seemed to give voice to a scientific word that could guide public action and federate public opinion, the fight against terrorism still remains in the shadow of reason and a prisoner of bureaucratic inertia, electoral interests, and foreign influences. This is neither serious nor respectful of the past and future victims of terrorism.

All of this has undoubtedly encouraged an intellectual surge, almost a moral insurrection, on my part, which in effect sets me apart from the traditional positions of the academic world, which in my eyes is trapped in the quarrels of mandarinism and the deleterious effects of the precariousness of public research, and from those of the security world, which is partly bogged down in the ideology of identity. But it is of course a freedom that I pay dearly for by being kept away from these two fields that do not yet or no longer consider me to be one of them, and which forces me to find a more tenuous, more iconoclastic perhaps, more independent path on my own.

4 *How can we explain the fact that this French-style trajectory and its inflection towards American-style counter-terrorism is not really openly discussed, and is instead considered as a "natural" evolution? How can we analyse this confinement that always leads to continuing and expanding a policy that does not solve much and adds its own problems to the initial difficulties? Can we return to the initial model of the 1980s and still be effective in the fight, and if so, how? Under what conditions (and adaptations?)*

This evolution of our counter-terrorism policy, which has the support of a political arc ranging from the social democrats to the extreme right, has in fact met with no real opposition in principle, for several reasons. First of all, the political system of the Fifth Republic in France does not allow the expression of almost any counter-power. This is the case in particular for regalian activities and obviously for our intelligence policy. The majority in Parliament dissuades any public controversy in this area. And the bodies that monitor the activities of the French services are among the weakest in Europe, as we shall see later.

The apathy of public opinion is also carefully maintained by a whole network of actors who gravitate towards power and receive remuneration. It is worth noting, for our purposes here, that the security lobby has acquired majority positions in recent years. Media empires, built up by arms dealers and the big fortunes of finance and luxury goods, help to anaesthetise public opinion, which is invited to turn away from questions of social struggle and only to consume. These "new watchdogs" are largely financed in return by public aid to the press.

Security issues act here as a powerful diversion ("le fait-diversion", as Bourdieu used to say) or a kind of anaesthetic. The terrorist threat in particular requires the population to "rally" around the government in

order to better defend itself. Various social psychological processes are also at play here:

First, causal attribution theory demonstrates our need to attribute the crime to an objective reason in order to be able to process it. In the state of shock that follows the attack, we often unthinkingly seize on the first explanation given by the loudest media in an attempt to evacuate the overflow of emotions and cling to tangible justifications. We think we have a sense of reason, but we are often a long way from the truth.

The phenomena of conformism then invite us to adopt the opinion of the majority, as revealed by the Asch experiment. A fragmented society, such as ours today, particularly in the event of danger, will favour what brings its members together, even if artificially, over what drives them apart. Free will is seen here as divisive.

Terror Management Theory is particularly relevant to the threat of terrorism. It invites us to overplay our adherence to the beliefs that seem to hold the community together, to accentuate our prejudices against outsiders, and to ignore cases that fall outside the prevailing stereotypes (e.g. Muslims condemning the attacks).

Finally, let us note the seductive character of the "fight against radicalisation", which allows a lazy distancing of an "other", who is neither guilty nor really innocent, but objectively different, whose individual drift (the famous "process" of radicalisation) exonerates the community of any fault, but still leaves the possibility of his return to "normality" and de-escalation via "de-radicalisation". Between the essentialization of Islam and good feelings, this ideology has spread widely in our country since 2013, after an executive power in need of announcement effects has, as we have seen, unwisely opened the door to it.

In order to emerge from this mortifying and demobilising apathy, it seems to me, however, to answer your question as well, that not all the battles have yet been fought. Three of them seem to me to be indispensable today in order to find the voice of a more just and effective anti-terrorist policy:

First and foremost, the battle of words: we have unwisely given the terrorist everything they asked of us, i.e. to be seen as the fighter of an enemy army and the vanguard of a world Ummah. We must urgently stop using the language of the enemy, which is that of war and religion. There is a whole semantic terrain to be regained in order to deprive terrorism of its emotional charge. For we have known since Victor Klemperer and his *Language of the Third Reich* (1947) that it is above all in words that defeat is permanently established.

Secondly, the battle of intelligence: the services must be intellectually rearmed with greater recourse to the human and social sciences and must begin to educate public opinion about the threat by trying to objectify the real danger that terrorism represents today in relation to the other perils that surround us. This concern for clear-sightedness is the mother of all battles.

Finally, and this is what best responds to the concerns you express in this book, the battle of suspicion: we must find ways to strengthen the support of

the whole of society (including Muslims) for our anti-terrorist policy; stop playing on divisions by invoking "separatism" for example. We must also develop our vigilance on the positions of authority in the war against terrorism: who calls for war? on what terms? who benefits from it? etc. Finally, we need to make some institutional changes to de-exceptionalise our response, such as bringing our counter-terrorism coordination back to the level of the Prime Minister, and depoliticising our communication on the subject wherever possible. This is how we will deprive terrorist crime of its emotional charge.

But before embarking on these three battles requiring endurance and pugnacity, we should start with a simpler, more immediate and undoubtedly more fruitful exercise: to evaluate our anti-terrorist policy, to finally measure what this turning point in the "war on terror" has cost us. An interdisciplinary mission could do this in a few months, made up of the major inspection bodies and academics (sociologists, psychologists, anthropologists, etc.), possibly assisted by representatives of the services, elected officials, etc. There are two main reasons for this:

First of all, of course, the change in doctrine that took place about ten years ago (2012: Merah affair and importation of the Anglo-Saxon model of the fight against radicalisation) and on which we now have the necessary hindsight to measure its effects.

Secondly, the costly nature of this public policy: a report by the Court of Auditors two years ago already put the extra cost of this shift at 9 billion, the DGSI has doubled its budget in five years, the state's intelligence mission has increased by 11% in the same period, etc. At a time when money seems to be lacking for many social programmes, such budgetary arbitrations would require a little more transparency and debate.

There is indeed too much at stake in terms of public liberties (even if our fellow citizens have been easily persuaded to renounce them), strategic independence (and the risk of alignment with the diplomatic agenda of foreign countries), the trivialisation of the discourse of identity (at a time when the far right is gaining in power), and finally operational efficiency to continue to blindly apply a model that may well have become obsolete after having been counter-productive for several years.

5 *Counter-terrorism, with its "fusion centres" and data interoperability, has presented itself as a global tool (more or less well shared) and more open to institutional communication, abandoning the "no comment" policy. One could say that secret service officials now have communications officers who are quite talkative. Is this a positive aspect that gives the public a better understanding of the issues or a policy that aims to feign openness and in the worst case use methods of influence against its own citizens? How can we distinguish between transparency displayed through realistic fiction, testimony of the past making the services more "human", respect for secrecy on operational needs, and the intoxication of a false transparency aiming on the contrary to obscure the opponents, and the population?*

Much more than predicting, governing means hiding. Concealing from the eyes of the majority what constitutes the very mainspring of power, and ultimately the scandal of its fragility and illegitimacy. In this respect, intelligence is the keystone of this political comedy. But the war on terror has upset the relationship between intelligence and the fight against terrorism which, due to the decrease in state terrorism and the massification of low-intensity attacks, should have remained a matter of "low-level policing". Instead, the cop and the spy have been invited to come closer together, upsetting professional cultures and working methods, and leading to a confusion that is detrimental to both functions, and probably even to the information of the population as you suggest.

For the pre-eminence of intelligence has first of all removed the fight against terrorism from the view of the citizen. It is now hidden behind high walls of secrecy, preventing any support from the population, which is kept out of the definition of the threat and the choice of the means devoted to it. By entrusting the monopoly of the fight against terrorism to a service capable of classifying all of its activities (DGSI), the government has closed off all debate on the issue, thereby weakening the democratic vitality that is necessary for our collective resilience. As you say, although the services communicate more – and they have been asked to do so for the past 15 years – they inform less.

Secondly, the almost unlimited means available to intelligence since the 2008 White Paper may have led to an overestimation of the threat. I recall the words of Joseph Conrad in *The Secret Agent*: "The existence of secret agents should not be tolerated, because they tend to increase the immediate risks of the scourges against which they are employed". A service whose task it is to define and produce otherness in proportion to its means and thus risks obscuring our view of the reality of threats. Especially since, with Daech's terrorism for all, the border between "them" and "us" now runs through the middle of the population. Thus, never before have the services risked dividing us to such an extent.

These are two examples of how the fight against terrorism has suffered from the stranglehold of intelligence in our democracy of opinion. But the latter has not emerged unscathed from this forced marriage either. Thus, counter-terrorism has disrupted the work cycle of the services, notably by favouring "security" intelligence. This is operational intelligence, immediately usable in the field by the action service, the special forces or drone strikes, and whose life span is limited to one-off hits. Time and intelligence have thus been diverted to short-sighted intelligence, to the detriment of long-term analysis and complexities.

The fight against terrorism has also weakened our national sovereignty by marginalising counter-intelligence missions, which have been forced to take a back seat to the demands of counter-terrorist cooperation. In so doing, our security services have been reduced to the status of almost provincial auxiliary forces of a global grand design. Increasingly integrated

data exchange systems and the moral pressure of terrorised Western public opinion have accentuated inter-service suggestions and our strategic dependence on some of our allies.

The fight against terrorism has also modified the image of the services by forcing them to publicly assume illegal actions, such as targeted assassinations or collective punishments (such as the administrative closure of places of worship). While the infringements of the law of counter-espionage remained confidential, the counter-terrorism trumpeted by a political class giving in to the virilisation of its discourse risks casting a veil of suspicion over the activity of our services and delegitimising their action in the eyes of a part of the population.

Finally, the fight against terrorism has refocused the services in the institutional landscape. Once cautiously kept at the margins of the palace, they are now invited (the DGSI and the DGSE, for example, now participate in the national defence and security councils) and consulted by leaders seduced by their capacity to control the population. As the only bodies that have not suffered from the general disengagement of the state by neo-liberal regimes, the intelligence services have, under cover of the increasing terrorist threat, made themselves indispensable and now have a weight and influence that was previously only known to them in authoritarian regimes.

6 *One of the criticisms of the former French anti-terrorist policies was its rigidity in terms of data exchange between services and internationally, as well as a strong home-grown spirit between services, do the services that form the DGSI collaborate better than before with each other, and with the DGSE, or is the relationship purely transactional (including at the financial level) in each case?*

The DGSI was designated as the *lead agency* for counter-terrorism in 2018, four years after its consecration as a general directorate. But it had long been preparing the ground by gradually emancipating itself from the national police directorate general, by placing relays, i.e. permanent liaison offices and dedicated executives, within partner services (the intelligence directorate of the Paris police headquarters, the central territorial intelligence service, etc.), by claiming a quasi-monopoly of judicial investigations and by consolidating an exclusive and informal European network of cooperation between similar agencies.

The DGSE, which had previously been designated as the *lead agency* for SIGINT, willingly accepted this designation and has been visibly loyal ever since. We do not know if we should see this as the heritage of military righteousness or the relief of being rid of a politically sensitive file, but the DGSE seems to behave in an irreproachable manner towards its partner. To the point of sometimes letting the latter be overly masterful in the way, it deals with terrorist targets.

However, by conveniently taking a back seat to the DGSI, the foreign service is undoubtedly depriving our counter-terrorism policy of its professional culture, traditionally based on the long term and knowledge of human

geography (particularly in countries that are part of our former zones of influence), to give free rein to a police culture more eager to fabricate otherness and to legalise it. This impoverishment of our intellectual capacity to embrace all the dimensions of the terrorist phenomenon is one of the perverse effects of the hegemony now exercised by the DGSI.

It is true that the French counter-terrorism services communicate better with each other than before. The permanent staff created by the DGSI brings together representatives of each specialised service who exchange in real time on all objectives. The mobility of senior managers between the different services, as well as the joint initial and ongoing training sessions organised by the Intelligence Academy, allows for cross-fertilisation of professional cultures and human contact between agents.

Not to mention, of course, the fear, fostered by the political authorities, of underestimating sensitive information, which leads to the unrestricted transmission of the information gathered. It is now accepted in the counter-terrorism services that a career is no longer built on solitary successes, but that it can be shattered by the slightest withholding of information that proves fatal. Since the attacks of 2015, a director will be blamed less for having had a dull and lacklustre administrative career than for having been, through negligence or ambition, the indirect cause of an attack.

As a result, more is exchanged, but less is understood. Intelligence and personal and metadata circulate more rapidly within the first intelligence circle, but the capacity to analyse them, to put them into perspective, and to perceive the complexities and nuances that precede the dangers is diminishing in proportion to the increasingly narrow base that produces it. In the past, a "counter-terrorism community" offered a mosaic of professional cultures, means of investigation, and access to power, which resonated more accurately with the world around it. And there were not many more misses than today. If one department missed an event or analysed it falsely, the neighbouring department remedied it, and the political authorities had the full range of viewpoints at their disposal to form an opinion and decide on their action.

This is no longer the case today, behind the economies of scale, we have gained in coherence what we have lost in knowledge. The government is now pleased to have better control over an intelligence apparatus that is more vertical, less diverse, and better gathered around it, notably via the coordinator of intelligence and the fight against terrorism (CNRLT) placed under the President of the Republic. This allows him, for example, to use consolidated statistics to his advantage, without any contradiction, such as the famous number of "foiled attacks", while maintaining discretion about his functioning. But this cleverly staged facility could be deceptive. The authorities have reassured themselves at the expense of our freedoms, but no doubt also of their own efficiency.

7 *There has been much criticism of the ineffective parliamentary control over the action of the services and much hope has been placed on a tighter political and technical control around the executive (and the president). Is this related*

to the institutions of the Fifth Republic or to more general features of a model that rejects control and considers the secret services as having absolute delegation over means, including criminal means, as long as they fight for what they consider to be the interest of France or of the coalitions in which it engages? What reforms are possible to introduce more self-control and democratic control within the services? Could we envisage a status equivalent to that of whistleblowers when employees consider that orders covered by secrecy are illegitimate and do not fall within the framework of the national security of the state but within that of personal interests or acts that endanger the democratic framework of the country?

It is clear that the increase since 2008 in the means of surveillance of the population under the guise of the fight against terrorism has now exceeded the control capacities available to any counter-power. An imbalance has been created in favour of the intelligence services and their political sponsors. This new economy of control entails many dangers that go far beyond the mere infringement of individual liberties, which has been conscientiously documented by human rights organisations.

The main risk lies in the possible diversion of the services' resources to the benefit of the "legal country", outside the general interest. In the past, the answers to the question of whether the internal and external security services should primarily protect the government in power or the country and its population varied according to the interests and positions of authority of those interviewed but were always based on a kind of democratic wisdom that seemed to ignore the possibilities of manipulating public opinion. However, these have never been so present, constituting today a determining part of the polemological landscape. In this respect, the "war on terror" that concerns us here has presented a formidable opportunity to redistribute the powers of influence within the Western world.

The very essence of the intelligence services, as well as their working methods, has been affected, and the intelligence services, which have never been the spearhead in the history of the last two centuries, have moved even further away from the republican ambition, taking refuge in a kind of security separatism. The operating principles of democracy and the rule of law, such as publicity, representativeness, and legality, to which we could add sovereignty and secularism since the French Revolution, are being overturned by this "war on terror". Each of these notions would nevertheless constitute a relevant entry point for strengthening the democratic control of intelligence.

Let's take legality as the first possible avenue for reform. We could indeed start with the question of whistleblowers. Long excluded from the world of intelligence by the criminal sanction of any disclosure of a national defence secret, this possibility now exists through direct referral to the National Commission for the Control of Intelligence Techniques (CNCTR – created in 2015) which informs the Council of State and the Prime Minister. If the facts reported appear to be illegal, it also refers the matter to the public prosecutor

and the Commission on National Defence Secrecy for possible declassification of information.

In theory, compliance with this procedure spares the staff member concerned, who then benefits from the protection granted to whistleblowers. However, in addition to the complexity of the process, it requires great temerity on the part of the agent … Moreover, there is no public example of whistleblowing since this possibility was created. While the procedure has existed since 1998 in the United States and has already made it possible to reveal affairs of state, we had to wait for the 2015 intelligence law to allow French service agents to report breaches of the law of which they were aware, and then only with regard to the use of intelligence techniques. We could also think about adapting to the world of intelligence Article 40 of the Code of Criminal Procedure, which obliges any civil servant who has knowledge of a crime or an offence to inform the public prosecutor.

It should be added, however, that in this field, respect for legality is a necessary but probably insufficient criterion. In addition to the fact that it is accepted that the services sometimes resort to illegal methods, as they are the only ones authorised by custom to get their hands dirty for the collective interest, and that the law is not legitimate in any case, the vigilance of whistleblowers could be extended to all issues relating to the fundamental interests of the nation, according to Article L.811–1 of the Internal Security Code. A biased threat definition process, a diversion of resources to private or partisan interests, or the placing of a foreign service under trusteeship should thus also be able to give rise to alerts emanating from within the services, which would not otherwise be known.

It would then be necessary to define the most appropriate point of arrival for this type of information. At this stage, the Parliamentary Intelligence Delegation (DPR – created in 2007) would probably be the most appropriate, subject to strengthening the confidentiality of such exchanges, as well as its representativeness vis-à-vis the entire political landscape, by integrating more members of the opposition in the framework of a broad reform of its functioning.

In the second example, we could address the question of sovereignty by making public the degree of subordination of our services to their foreign partners. It would undoubtedly be interesting for the national representation to know our level of integration in various coalitions or even the suggestion that certain powers exert on our intelligence apparatus by providing it with information and hence avenues for work.

This point could be the subject of an annual communication from the CNRLT to the DPR in the form of percentages of data exchanges, incoming and outgoing flows, broken down by country. This is a recurrent request of the CNCTR, which is based on the *Big Brother Watch v. United Kingdom* ruling of 25 May 2021, while France is the last EU member to have no legal framework in the field of international cooperation, creating a legitimate suspicion.

Beyond these two atypical examples of reform projects, some existing control bodies would already benefit from being strengthened, as France, despite some improvements since 2017, has not yet caught up with its neighbouring democracies. While the list of structures supposed to oversee intelligence is impressive, the examination of each of them, taken in isolation, puts the effectiveness of the whole into perspective.

We will pass quickly over the internal hierarchical control, which is not really relevant to this question, and also over the Intelligence Services Inspectorate (ISR – created on 24 July 2014) which, in order to be credible, should be able to count on a permanent body of executives from all the major inspectorates, which can intervene on its own initiative and no longer only in the event of a referral from the government, and which should be able to rely on independent external expertise.

As regards the legal review itself, the law created a specialised chamber within the Council of State (litigation section) whose members are authorised to maintain secrecy but may only communicate to an applicant who has a complaint about an infringement of their privacy or an error of assessment, part of the investigation file, which contravenes the requirements of adversarial debate. The administrative judge limits himself here to noting the possible illegality of an investigation act.

Particular mention should also be made here of the way in which the government, and sometimes this same Council of State, disregard the case law of the European Court of Human Rights (ECHR) and certain rulings of the Court of Justice of the European Union (CJEU – *Télé2* ruling of 2016 for example) to justify mass intelligence. This is the case with the generalised retention of connection data for one year and the use of "black boxes" under the guise of a permanent "state of security emergency", which placed France on the margins of European rules.

External administrative control is also supplemented by the CNIL for data protection. In this context, it is time, for example, to give the CNCTR the right to check the legality of intelligence files. The last time a file of this type was submitted to the administrative judge, it failed to be validated (EDVIGE file in 2008). It would no doubt be useful to ensure that the individual data collected today are proportionate and reliable.

As I briefly mentioned before, parliamentary oversight was indeed added by the law of 9 October 2007, reinforced by the law of 18 December 2013, creating a parliamentary delegation for intelligence (DPR) which has moved from the "monitoring" of intelligence activity to its theoretical "control" and even "evaluation". But its limited resources make its mission dependent on the relationships of trust it builds with the services concerned. Thus, while the British *Intelligence and Security Committee* can count on a team of 14 people and a budget of 1.3 million pounds (excluding operations), while the Belgian *Permanent Committee R* has an investigation department of 5 people, the French DPR has no full-time administrator. This makes all the difference. Yet it is the DPR that should be the first to ensure that the battles waged on

behalf of the French people are correct. But the increase in its powers is systematically refused by the executive. This is what happened, for example, on 11 May 2018 with a bill from the chairman of the Senate's law commission aimed at strengthening this control. It happened again in 2023 with the new Military Programming Law (LPM).

In the end, therefore, it is the CNCTR that exercises the most vigilant control. It ensures that requests for authorisation of an intelligence technique scrupulously respect the principles of proportionality and subsidiarity, and only infringe on privacy in cases of absolute necessity. Its annual report is also the only real public document that slightly lifts the veil on the activity of the services. It is notably through it that we now know how much the surveillance of social movements (under the guise of "prevention of collective violence") has increased in recent years to the detriment of counter-espionage and economic intelligence.

However, the comparison with the major Western democracies is instructive. To take the British example again, the Intelligence Service Act of 1994 (MI6) and the Security Service Act of 1989 (MI5), reinforced by the Regulation of Investigatory Powers Act of 2000 and supplemented in 2016, allow for much more in-depth specialised control than in the French context. Even if the example of the Iraq war showed how easily London could still manipulate the activity of the services. And how thin the line between the intelligence services and partisan interests still is.

Beyond all the possible avenues of reform in order to introduce a little democratic control into the intelligence function, it would be appropriate to question the interest of the Republic in offering its most sensitive services to the inquisitorial gaze of the general public. Indeed, if tomorrow a more progressive and republican regime, convinced of the need for control, were to come to power, it would come up against a wall of opposition in the country that would show its distrust in the media, on the stock exchange, and certainly in the streets. A period of great disorder would set in, probably for a long time.

It is to be feared that the services themselves, by their sociological composition and their political positioning, would contribute to this, at least through bureaucratic inertia. And taking them over would be a first test of strength for a young, untested regime that lacks specialised managers. Moreover, until now, and with rare exceptions, the Republic has always accommodated security services reputed to be unfavourable to it, provided that they remain in their barracks and police stations, that they do not bite the hand that feeds them and that they carry out their tasks as correctly as possible, without causing opprobrium. From the "100 days" of Napoleon's return to power to the 1981/1983 period when the socialists came to power, the services always got away with the mere symbolic replacement of a few directors, without changing anything in their operating methods and their institutional isolation.

This undoubtedly explains the longevity of these citadels of the Ancien Régime which, enjoying a form of political impunity, only open up in their

own interest, as in 2015 and 2017 when the law came to legally validate practices that were previously illegal. Consequently, it is less a question today of finding tools likely to democratise and better control intelligence – these exist if a democratic will or scandal so requires – than of proving to political personnel the advantage that they would have in opening a few breaches in the wall of secrecy in order to ensure that our agents are indeed working for the sole benefit of the general interest (provided that this is correctly defined), without damaging it, and that republican principles no longer stop at the door of the services.

Note

1 An Interview with François Thuillier by Didier Bigo.

9 Intelligence oversight collaboration in Europe[1]

Thorsten Wetzling

1 *You are heading the research unit "Digital Rights, Surveillance and Democracy" of the Stiftung Neue Verantwortung (SNV) and you have been the head of the German team of our common Research Project GUARDINT. Your current work focuses on the practice, the legal basis, and effective independent oversight with respect to different modes of access and subsequent processing of personal data by security and intelligence agencies. You have already published different papers on the methodology to construct an index allowing to compare different forms of oversight structures in Europe, and their relative qualities. Could you give us an idea of the key differences existing in terms of oversight of intelligence services between Germany, France, and the UK, and what are the results if we want to judge their independence and efficiency?*

I will mostly draw on recent work related to GUARDINT as well as to the European Intelligence Oversight Network (EION). As regards the former, we collaborated with researchers from Sciences Po, King's College London, Université de Lyon, Wissenschaftszentrum Berlin (WZB) over the course of three years to shed light on international intelligence cooperation and accountability. GUARDINT produced a range of different outputs and I would encourage interested readers to consult the project website for detailed information on each of them. With regard to EION, this is a project where SNV regularly invites selected members of intelligence oversight bodies from ten European countries to collaborative workshops in Berlin. These events provide unique opportunities to discuss pressing themes of intelligence governance and to engage, where possible, in good practice sharing and other types of capacity-building deemed necessary to strengthen rights-based surveillance practices and effective accountability. Where suitable, I will draw on both projects in my responses to your questions.

Coming back to your first question regarding the intelligence oversight index and our findings with regard to Germany, France, and the UK, this relates to one guardian.org output, namely, the conceptual design and partial implementation of a composite index on intelligence oversight. This was

DOI: 10.4324/9781003354130-10

administered jointly by the SNV (Thorsten Wetzling, Kilian Vieth Ditlmann and Felix Richter) and WZB (Ronja Kniep and Sarah Naima Roller). Let me establish first the basic rationale for the index and its basic functionality before elaborating on some of our findings with regard to the three countries you have mentioned.

The revelations of Edward Snowden and subsequent parliamentary and media investigations as well as successful litigation in various courts have put democracies under pressure to establish, adjust, or – depending on your perspective – retro-fit their legal frameworks so as to better account for their large-scale, digital surveillance practices and to initiate more rigorous oversight reforms. Despite these developments, there still remains a notable dearth of comparative research on intelligence oversight, however. To help fill this gap, we designed and then partly implemented the *Intelligence Oversight Index* (IOI). Our aim was to measure and compare a variety of oversight practices of democratic countries. More specifically, we saw the IOI as a tool for the systematic mapping of emerging practices of oversight and to expose oversight gaps across countries and over time. By uncovering cross-country variances, we wanted the IOI to help illustrate the scope of actual activities in an area which is often dominated by politics of security, exceptionalism and secrecy and a supposed lack of alternatives. With the help of a composite index, we wanted to show that it is possible to identify common threads, criteria, and objectives for oversight in democratic countries and compare how these are implemented, despite many socio-legal differences that obviously exist between different political systems.

For this, we adopted a broad definition of intelligence oversight as a set of practices that scrutinise, evaluate, contest, and sanction as well as publicise the activities of intelligence agencies with the goal of preventing future misconduct or discovering past misconduct. We also decided to speak of oversight practices rather than mechanisms, systems, or institutions because we felt the need to compare not only a formal set of laws or the institutional designs of oversight. The goal was, rather, to observe how different actors *do* oversight, including the structural and institutional conditions these practices are embedded in (as much as the practices are producing these structures). The focus on practices was important to us because there tends to be a significant gap between the written rules governing surveillance on the one hand and their implementation on the other. For instance, as part of the index, we inquire about instances where oversight bodies actually make use of their data access rights.

Importantly, given the widely shared observation that "accountability now seems to flow from globalised network of activists and journalists, not from parliamentary oversight committees" (Richard Aldrich), our IOI distinguishes between two primary subsets of oversight practice, namely, *delegated* and *civic* oversight. *Delegated oversight* is exercised by external bodies bestowed with legal oversight mandates and powers by the state. We thus define oversight as external forms of scrutiny, from outside the government, that include parliamentary, expert, and judicial scrutiny and exclude internal control within intelligence or steering by ministries. *Civic*

oversight, by contrast, refers to the scrutinising practices by the media, CSOs, and citizens who complement *delegated oversight* through an oftentimes more adversarial and more public mode of oversight.

Having tried and tested various iterations of our conceptual framework for the assessment of intelligence oversight, we designed and conducted practitioner surveys, expert questionnaires, and desk research on civic intelligence oversight as a pilot study in Germany, France, and the UK. In addition, we conducted qualitative interviews with selected practitioners for the re-evaluation of concepts and a "thicker" understanding of civic oversight practices. In order to be transparent about our findings and to enable future generations of researchers to benefit from, build upon, or challenge our work on the potential and limitations of civic intelligence oversight, we published a website that provides open access to the anonymized data we gathered from our surveys.

With our descriptive empirical analysis of the modalities of civic oversight, we were able to present data from surveys with practitioners of civic oversight in the UK, France, and Germany and to compare their resources, activities and their transnational scope, their perceived impact, as well as protection and constraints of the often-sensitive work.[2] For example, we found that while there is little lack of expertise in civic oversight professionals, only a minority of practitioners report sufficient funding across all three countries. Furthermore, we identified a common predicament of civic intelligence oversight practitioners who are at a particular risk of becoming the subject of surveillance themselves. Our data shows that widespread distrust in the legal and technical safeguards against intelligence surveillance is seen as the main constraint for civic intelligence oversight in all three European democracies, even more so than a lack of financial resources. This is particularly the case for respondents from Germany and France, who expressed not only a much higher dissatisfaction with the status quo than their colleagues from the UK but also indicated relatively often that they either suspected or have evidence for their surveillance. Additionally, we provided new insights on the attitudes of civic intelligence practitioners towards intelligence agencies and state-mandated oversight in their respective countries.

These were just a few of our findings with regard to civic intelligence oversight in those three countries. With regard to delegated oversight, our team deviated from our original plan and decided to postpone the implementation of the IOI to delegated oversight in those three countries. We did this primarily because the actors and activities of delegated intelligence oversight we were supposed to assess were themselves in a fundamental state of flux during the time of the research project. This is because the norms, legal standards, and oversight of government access to and subsequent processing of personal data (often held by the private sector) have attracted unprecedented policy attention in the wake of landmark decisions handed down by the European Court of Justice (ECJ), the

European Court of Human Rights (ECtHR), and national courts, such as the German Federal Constitutional Court (BVerfG) between 2020 and 2021. Central elements of national intelligence legislation were deemed inadequate for the protection of fundamental rights and freedoms and this triggered new debates on intelligence governance and effective oversight. In turn, this brought momentum to new international debates on good standards and norms in forums such as the Council of Europe as well as the Organisation for Economic Cooperation and Development (OECD). Given government secrecy and the insistence by many governments that these matters are the sole prerogative of national security decisions, it is noteworthy that this subject became the subject of international negotiations. We have seen greater preparedness by national governments to discuss matters of intelligence governance and we have seen the instalment of new forms of oversight, notably judicial review mechanisms, that were not possible in some countries, such as Germany, a few years ago.

Generally, as regards delegated oversight, Germany to date has still the most fragmented landscape for intelligence oversight by comparison with France and the UK. Not only does Germany support two different legal regimes for bulk collection (Art. 10 Act for bulk collection of foreign-domestic communication data; BND Act for bulk collection of foreign-foreign communication data) but it also has two different entities that perform (quasi-)judicial oversight (i.e. prior approval of surveillance warrants and ex-post review of data processing), the G10 Commission and the Independent Control Council (Unabhängiger Kontrollrat, hereafter UKR), respectively. In addition, the German Data Protection Authority is also mandated by law to perform data protection reviews which look into the data processing and the establishment of databases and where there is considerable overlap with the mandate of the UKR. Moreover, due to the restricted remits (or limited catalogue of control competence) for each oversight body, there is a notable risk that a holistic understanding of the totality of surveillance activities is not available to the oversight bodies. This, however, is necessary to assess the necessity and not just the legality of additional surveillance applications. In addition, given the overlaps in control competences, one can observe unhelpful "turf wars" instead of systematic oversight cooperation among the various bodies.

The UK, unlike Germany or France, has gone at far greater length to streamline and simplify its legal framework for intelligence with the help of the Investigatory Powers Act. By contrast, Germany sports more than 30 individual Acts of Parliament and several by-laws with many cross-references to individual laws that obfuscate a dense web of provision from too much external scrutiny. More importantly, whereas the UK legal framework defines what counts as investigatory powers and establishes a review mandate for the oversight body IPCO over every public body that uses such powers, Germany still defies such functional logic. Instead, each intelligence actor has its own legal framework and the oversight bodies are

limited in as much as they can only assess the legality of the three federal intelligence agencies data collection or processing, not the very similar activities by actors within the defense or law enforcement sector. This is anachronistic and not in keeping with the Council of Europe's modernised Convention 108.

France, too, has many deficits still to overcome, notably the formal extension of the CNCTR's oversight remit to foreign intelligence collection and OSINT to give just two examples. Whereas all three countries have made significant improvements when it comes to the public reporting of oversight activities, many additional aspects would need still to be covered going forward. Interesting in this regard is also the use of supervisory technology. Many oversight bodies have recently received significantly better access to the IT systems and the various databases used by the services. Access by itself is not enough, however, to guarantee effective oversight. In order to implement what the ECtHR has called end-to-end safeguards, oversight bodies need to significantly up the ante when it comes to the development of control programs and automation in audits.

2 *German oversight authorities are regarded by many as more powerful than their counterparts in other democratic countries (in Europe and among the five eyes). Recent reforms of the German legislation that you have analysed and comment in the blog about-intel seem to give the right to the supervisors to have access to foreign data, giving them a better understanding of the scale of an operation, especially when we know that more than a half of data are coming from these foreign sources. Could you explain briefly the reform, (DPA, creation of a different supervisory authority for foreign sources …) and do you consider that it was a useful one, or do you consider that it is a reform "on paper" that is masking the practices more than revealing them?*

I think it is necessary to distinguish between different types of intelligence oversight bodies in the response to your question. This is because for the majority of German intelligence oversight bodies, notably the parliamentary intelligence oversight committee and the German Data Protection Authority, access to non-German intelligence service data remains severely restricted or non-existent. Only the newly established UKR can no longer be treated as a "third party" in international intelligence cooperation that involves the German foreign intelligence service (BND).

This needs further unpacking. I will briefly lay out the essence of the 2021 reform of German foreign intelligence induced by the landmark decision of the German Federal Constitutional Court which had found several provisions in the previous legal framework unconstitutional. Among other requirements, the court demanded that the amended legal framework for foreign intelligence collection must provide for two distinct types of oversight for the BND's SIGINT activities: judicial and administrative control. It did not prescribe, however, whether these separate oversight functions should be performed by one or several bodies. The lawmakers decided to combine both tasks within just one new oversight

institution, the UKR. The Federal Government and the majority in parliament saw in a unitary body a better precondition for successful international cooperation. They warned that, if too many oversight or review agencies would be involved, say a separate court for judicial review and a separate administrative control body, which might have involved the Federal Commissioner for Data Protection, and each entity exempt from the third party rule, foreign intelligence agencies might shy away from sharing information because of a fear that their data might not remain confidential.

The UKR, which is in operation since January 2022, enjoys comprehensive access to all BND premises and to all its IT systems as long as they are under the sole direction of the BND. If the UKR requests access to data that is not under the BND's sole direction, the BND shall "take appropriate measures" to facilitate access. However, the law does neither include specifications of what such "appropriate measures" shall be nor does it entail a duty to proactively inform the UKR about all operational systems and jointly administered databases with foreign services. Moreover, the BND is not obliged to provide a comprehensive overview over the complex systems used to collect and process foreign intelligence.

It was a firm requirement by the Constitutional Court that the "third party rule" may no longer undermine the effective and comprehensive oversight by the UKR. In its judgement the Court referred explicitly to the third party rule as a "rule of conduct that is based on agreements with foreign intelligence services and generally recognised by all intelligence services; according to this rule, based on informal arrangements, intelligence obtained from foreign intelligence services may not be shared with third parties without the consent of the intelligence service in question". It also held that "The third party rule is an administrative practice that is not legally binding, but is merely based on agreements with other intelligence services; it is thus flexible and the Federal Government can influence its practical significance ([…])". The Federal Government and the Federal Intelligence Service remain bound by the assurances they have given. However, in the future, it must be ensured, through the way the oversight bodies are designed and through changes in agreements with foreign services, that the bodies conducting legal oversight are no longer considered "third parties".[3]

The Court did not, however, specify who this general finding should be implemented in actual practice and the government and the ruling majority in the Bundestag in the end agreed on an institutional solution whereby only the UKR was rendered in a position to access information stemming from foreign agencies and not the other German oversight bodies. Yet, even the UKR is still not rendered in a position to have universal access to all information in the possession of the German foreign service. Its review mandate is limited to only some of the intelligence methods, and not others (such as HUMINT or the use and processing of data acquired through

non-compulsory means). In addition, the mandatory logging of informational activities for audit purposes is only required for a few selected cases of data deletion and purpose changes, but the law does not foresee the mandatory recording of comprehensive audit trails. Plus, the limited audit logs that are required – for example if the confidential communications of a journalist that were unlawfully collected in a hacking operation are deleted – appear to be only accessible for review by the internal data protection and compliance unit of the BND. The same is the case, for instance, if unevaluated bulk data is shared with a foreign intelligence service. The automated transfer must be logged, but only internal BND inspections may access these audit logs.

The work of the UKR ought to remain strictly confidential and the BND Act does not impose a public reporting obligation upon the UKR. Instead, it must report to the parliamentary oversight committee every six months, but the content of these reports is not specified in the law. While the UKR is, at least formally, exempt from the third party rule, the Federal Government continues to regard the parliamentary oversight committee as a third party in the context of information sharing. This has consequences for the UKR's reporting to the parliamentary committee: Only information that is under the exclusive control of the BND may be included. The UKR must consult the Federal Chancellery before reporting to the parliamentary committee, to ensure that the report does not comprise third party information. The UKR may exchange views and compare notes with other domestic oversight bodies, namely, the Federal Commissioner for Data Protection, the G10 Commission, and the parliamentary oversight committee about oversight-related matters. In doing so, it must comply with the respective obligations to protect secrecy. There is no analogue reference to international oversight cooperation, for example in the context of the European intelligence oversight working group.

In response to your question, I would thus say that, in my view, the 2021 reform of the BND Act contained both positive and negative aspects. On the one hand, when compared to previous intelligence reforms but also with a view to how other democracies have codified (or not) foreign intelligence collection in their respective laws, Germany has undoubtedly come a long way. With this reform, it cements its position among the few democracies in the world that offer comprehensive legislation and important safeguards regarding the use of bulk powers for foreign intelligence collection. Yet, together with my colleague Kilian Vieth, I drew a sober conclusion when reviewing the 2021 reform: we deplored a fragmented legal framework, a disconnect with recent European jurisprudence, significant gaps in comparison to ECtHR standards and the fact that data purchases remain insufficiently regulated. Further criticism is due because of the reform's ineffective data volume limitation and the fact that it does not offer a redress mechanism for

foreigners. What is more, many legal protections are restricted to personal data and by and large the reform does not provide enough value for compliance and transparency.

Thus, despite noticeable improvements, the reform has failed to address a number of known deficits and creates new accountability gaps. By international comparison, the BND Act now features an important high water mark: it no longer restricts the German Constitution's guarantee of the privacy of telecommunications and the right to press freedom to citizens and residents of Germany. Instead, these fundamental rights against state interference "also protect foreigners in other countries". At least de jure. In practice, however, non-nationals might not benefit much from their rights when confronted with surveillance by German intelligence. This is because the BND Act also does not incorporate the standard for effective remedy that the ECJ found missing in US intelligence legislation in its Schrems II decision. At long last, the reform established genuine independent judicial oversight for some of the BND's key collection and processing practices. Still, the legal framework remains replete with too many ambiguities and omissions. Our report further highlighted the UKR's vague mandate for administrative oversight and deplored broad exemptions from the warrant requirement and cautioned against accountability gaps tied to suitability testing and data transfers between the BND and the German Armed Forces.

3 *In Europe, some supervisory authorities have tried to build a network to exchange good practices concerning their work and thought to build, beyond that, regular exchanges on analyses and even collaboration for some specific cases which were transfrontiers. Could you resume the role of the ENIR and EGIO networks, and their current legacy (including your EION)? Don't you think that their efforts to join come from the fact that they are countries with small resources and no willingness to have a regional role on their own, but only through a reinforced Europe? On the contrary countries like France or the UK are less keen to have a non-exclusively national (multi-national) network judging the legitimacy and necessity of their activities?*

I would like to answer your multi-tiered question by first focusing on the genesis and the role of the different fora for intelligence oversight cooperation that are known to me. Afterwards, I will try to address the question about variations in European delegations' keenness to genuinely invest resources and commitment to international intelligence oversight cooperation.

At the beginning of a brief historical trajectory of international intelligence, oversight cooperation should be the acknowledgement of a mismatch, namely, that intelligence agencies have worked very closely together for more than 70 years while oversight bodies have only begun to increase cooperation among each other. Several developments in recent five years point to the direction that there now is genuine and more sustainable momentum for more international oversight collaboration. This collaboration takes, as indicated below, several forms which may include work on common

standards for oversight and audit practice as well as capacity-building exchanges on good practice in response to common problems or challenges.

Intelligence oversight cooperation is practiced beyond Europe, of course, so the historical trajectory has to be a bit broader. Among the fora that predominantly involve the review bodies of Five Eyes countries, one can list the International Intelligence Review Agencies Conference (IIRAC) which, for example, took place in 2002 in London. Interestingly, it involved all kinds of different oversight bodies, parliamentary oversight committee, such as the British ISC, but also expert bodies such as the Belgian Vast Committee and also oversight bodies more closely tied to the executive branch, such as Inspector-General type review bodies from Australia and the US. Since 2017, the review bodies of Five Eyes member countries also come together in a more structured forum, called the Five Eyes Intelligence Oversight and Review Council (FIORC) whose basic terms and objectives were laid down in a publicly available charter.[4]

Also at the international level, the former UN Special Rapporteur on the Right to Privacy, Prof. Joe Cannataci, has launched the International Intelligence Oversight Forum (IIOF) in 2016 which brought intelligence policy makers and intelligence oversight bodies from several UN Member States together to 2-day conferences which were held, thus far, in Bucharest, Brussels, Valletta, London, and Strasbourg.[5] Unlike the more close-knit Five Eyes or European Intelligence Oversight Fora, the IIOF has an important mandate to promote discussions and knowledge on intelligence oversight at a time of democratic back-sliding in several UN Member States.

In Europe, different oversight bodies came together, for example, as part of the Conference of the Parliamentary Committees for the Oversight of Intelligence and Security Services of the European Union Member States. This conference has had several iterations, notably in Brussels, Rome, and Berlin. The sixth instalment in Brussels was co-organised by the Belgian Vast Committee and the Belgian parliament. On that occasion, the member delegation of the conference collectively launched what would later be known as the ENNIR project, a European Intelligence Review Agencies Knowledge Network. ENNIR, in the words of now retired and long-term advocate of intelligence oversight cooperation, Wouter de Ridder, was "a database mapping the different intelligence authorities in Europe and a platform for information sharing between them". Unfortunately, in his words, "as promising as these meetings (of the Conference) and the ENNIR project were, the Berlin conference in 2011 was the last of its kind". De Ridder also deplored the fact that the ENNIR website had to be closed for lack of staff and, even more, enthusiasm generated by this initiative among the European delegations who were part of this conference.

Individually, some European oversight bodies have organised conferences for continued oversight body dialogues, notably the French

CNCTR and the Belgian Vast Committee in 2018 in Paris, which was followed up in December 2019 with a gathering in The Hague organised by the Dutch oversight body CTIVD.

More potent, perhaps, was the initiative launched by oversight bodies from the Netherlands, Belgium, Switzerland, Denmark, and Norway, called the European Working Group on Intelligence Oversight. In October 2018, representatives from oversight bodies of these five countries signed "the Common Statement of Bern".[6] The declaration revealed that these bodies had "begun a new form of cooperation" in the form of a "joint project to exchange experiences and methods" particularly on "the development of oversight and audit standards and oversight innovation". In 2019, the UK oversight body IPCO joined the group which "convened at board level in Brussels and at staff level in Copenhagen. Observer delegations from Germany and Sweden were present as well".[7]

In addition, and less formally, one may add that SNV, a civil society organisation in Berlin has launched a process in 2018 called the EION. Its approach is notably different in that individual members of different judicial and administrative intelligence oversight bodies from ten different democracies are regularly invited to collaborative workshops in Berlin. At those workshops, the small group of oversight practitioners is invited to discuss thorny themes and questions on the basis of a paper and in the presence of a few academic and private sector experts who can help shed different light on things.

Now, obviously they are remarkably obstacles to international oversight cooperation. Notably, as mentioned in my previous answer, government secrets may not be shared by oversight practitioners with their foreign colleagues – even though the services themselves might have very well shared such information with their foreign counterparts. This is a mismatch and Prof. Cannataci has often called for a new international standard along the way of "what is shareable is overseeable". To date, though, this call for action has not been met with much legislative reform, except perhaps in Germany but also only with regards to a fraction of the intelligence service activity and with significant curtailments on the part of the UKR to inform its oversight colleagues in Parliament about it. Apart from secrecy, though, more mundane factors also play an important role in holding back the advancement of genuine oversight cooperation. Here, one can point to the increasing workload of oversight bodies at the national level as well as the lack of ambition by some oversight bodies to take on additional tasks.

What is interesting, I think, is that the UK joined the European Working Group as a sixth member, and this may have prevented France from joining this group. There is, of course, no official documentation for the reason why France did not join the European Working Group to which they were invited, so I need to preface that this is solely my

assumption: It may be that the French oversight body, and possibly by extension the French government as this decision may not have been solely for the oversight body to take, felt that joining a forum for increasing international oversight cooperation where an oversight body from the Five Eye intelligence alliance Country (in this case IPCO from the UK) was also a member would present too much of an undesired proximity or risk that they may prefer to avoid so as to remain more autonomous or to prevent inadvertent intelligence sharing. This said, maybe the French oversight body also had similar reservations with regard to the other continental European members of the European working group and it was more a general precautionary measure not particularly directed at an oversight body from the Five Eyes alliance. Alternatively, it may have also been that the French delegation may have tried to establish a separate other oversight cooperation forum and was perhaps not prepared to accept that another forum was already gaining traction. I can really only speculate about this in the absence of further official information on this. What is clear, however, is that an oversight body from the UK did not seem to have such reservations. The French body CNCTR has, arguably, tried to set up an alternative to the European Working Group or, more accurately, invested in ad-hoc conferences with different European partner bodies (such as the Vast Committee) because it may have been critical of the fact that the UK IPCO body joined the European Working Group. Why Sweden and Germany have not joined the club formally, is also not exactly clear. It may quite simply also have to do with the fact that due to the fragmented landscape of oversight in Germany, it was not quite sure whether the G10 Committee, the Independent Council (until 2021), or the UKR should represent Germany in this forum.

4 *Do you see a possibility to have a transatlantic dialogue on the different supervisory authorities of the five eyes (FIORC) and an EU or multinational network to agree on the limits that secret services cannot cross in operations abroad, and which distinguish them from illiberal and authoritarian regimes? Is the context of Ukraine a way to clarify this major distinction, which was fuzzier during the mid-2000s?*

I do indeed believe, as argued already partly in my response to your first question, that international discussions on the norms and standards that democracies need to adopt when it comes to electronic surveillance for the purpose of national security have attracted unprecedented public attention in recent years. Following landmark decisions by major European courts, governments, and parliaments had to be far more explicit about the legal framework and oversight process when it comes to different modes of government access to personal data. Given that the ECJ has rejected two previous transatlantic frameworks for data sharing between the EU and the US due to its concerns that US national security legislation does not provide, in its view, adequate data protection for European Union citizens

and companies, the search for common standards regarding bulk collection and oversight and redress has reached key decision makers in Brussels and Washington, too. Interestingly, as shown by the OECD process, there is a simultaneous concern that in the absence of new common standards, democracies will resort to data localisation which is deemed detrimental to economic growth. Lastly, democracies need to show, now all the more in the face of Russian disrespect for national sovereignty and its war of aggression in Ukraine, that they are distinct from authoritarian regimes. And this needs to be documented by means of various safeguards and guardrails against executive overreach.[8] Much has been written on this declaration and the lengthy negotiation and wordsmithing process it entailed.[9] As a consultant to the OECD Secretariat for this process I cannot reveal specific insights from the process. However, what I can point you to is the observation that despite some commonality identified, quite a substantial area has been bracketed. For example, notice how the declaration merely notes "stakeholders' calls for additional work and engagement to identify existing common safeguards in OECD Member countries to protect privacy and freedom of expression, and therefore promote trust, in the context of purchasing commercially available personal data, accessing publicly available personal data, and receiving voluntary disclosures of personal data by law enforcement and national security authorities". Thus, the identified commonality does not yet extend to the important modes of government access mentioned in this citation. Also, given the focus on commonality among all OECD member states it is perhaps unsurprising that the attributes of each principle may not include what may be considered a standard in some countries. For example, we know that some oversight bodies now possess direct access to the IT databases and operational systems of the intelligence services of their countries. This allows for far more advanced auditing and the use of supervisory technology. Similarly, the ECJ requires independent and effective review bodies, the OECD declaration use the word impartial and effective instead.

What needs to be said also is that if international norms and rules for intelligence collection will be further developed (and trimmed), this will be done primarily by states, not the oversight bodies. Oversight bodies may be consulted but new international conventions and the like are matters of diplomacy and here auditors are rarely invited to participate in the wordsmithing that international negotiations often amount to.

5 *You have recently done research on the role of private data brokers which have specialised on dataset and algorithms for national security purposes. Do we know how far the private companies operate in "preparing" the dataset?*

This is indeed an interesting and multi-tiered phenomenon. There can be various forms of public–private co-productions of intelligence. What we learned is that intelligence services across Europe are increasingly processing commercially available data as well as a broad range of information they deem "publicly available". To gain access to such data, they can

purchase data(sets), either ad hoc – when specific information is needed – or on a rolling basis by means of subscription from various data brokers. They can also purchase data on the darknet (which may emanate from leaks or stolen customer data) or buy finished intelligence and thus outsourcing time and resources for the analysis to private actors. In addition, services can also purchase from various providers the tools needed for automated analysis of commercially and publicly available data. In addition, services can obtain large (bulk) datasets through voluntary submissions of private sector entities, courtesy requests, or gifts. Last, but by no means least, agencies can also purchase or otherwise acquire large datasets through the use of authorised undercover agents or covert human intelligence sources (CHIS).

What these types of access have in common is that they are *non-compelled*; that is, the entity which provides the intelligence service with access to such data is not obliged by law to do so. This distinguishes these practices from signals intelligence (SIGINT) and computer network exploitation (CNE, commonly known as government hacking), where data held by the private sector can be obtained through compulsion or penetration. Notably, whereas compelled and direct access have been subject to increasingly dense regulation and oversight in established democracies, governments' purchases of commercially available data or their acquisition and processing of publicly available data still face far fewer legal restrictions and less robust (if any) authorisation and oversight procedures. This deficiency erodes public trust in government and is at odds with the promotion of the rule of law and democracy in Europe. Vague or missing legal restrictions and insufficient oversight may also increase the risk of disproportionate access to personal data without sufficient accountability. In turn, this may increase risks that various rights will be infringed, notably those to privacy, informational self-determination, and freedom of expression.

6 *What are the justifications given by the services to do such a thing? Is it because of a technical gap in which the secret services of Europe are obliged to ask US providers to help them? Is it on the contrary only a way for secret services to delegate some of their work and to gain time for a quicker reaction?*

There are, I believe, several potential explanatory factors for this developments. First, the rapid spread of web-based services, mobile devices, sensor networks, and the "internet of things" have jointly propelled a sheer inexhaustible availability of data. Unsurprisingly, it did not take long for such data being for sale in a burgeoning data market. More than 4,000 brokers now cater to the various needs for raw and processed data of their clients. Apart from companies in marketing and risk assessment, these clients also include national security and intelligence services. Second, as indicated given the current loopholes in legal framework and oversight deficits regarding non-compulsory access to data, there are clearly autonomy gains for services that may help

explain a growing investment in these types of private-public cooproductions of intelligence. In fact, I believe that the quantity and broad availability of commercially available data is profoundly transforming the practice of intelligence and national security as we know it. Fuelled by an insatiable thirst for data, these new forms of public–private co-production of intelligence fuse surveillance capitalism and government surveillance. As indicated, this poses profound new challenges to our democracies and, to date, invites creative non-compliance or worse: collusive delegation.

Consider for further illustration of a future challenge the fact that several European legal frameworks for intelligence apply governance standards only to *acquired data*, i.e. data in the possession of the services. However, many forms of non-compulsory government access to data revolve around practices where data may conveniently be stored in a private sector cloud. Here, the services may still have access to such data but, technically and legally, they have not acquired the data. In turn, this often means that oversight and audit mechanisms are severely restricted if at all applicable. In other words, if an oversight body such as the UK IPCO has direct access to the IT systems and databases of the services that is great progress. However, the UK services may still access finished analysis products or have service members use the IT systems of private (cloud) providers without such operations being overseen, let alone logged in formal government IT systems. In such a situation, I see a great need for lawmakers across Europe to do more to ensure that their national intelligence community conduct regarding data that is not directly in their possession, such as data hosted by private cloud providers, is still lawful and proportionate. Similarly, there are many forms of HUMINT and SIGINT interactions not sufficiently regulated. Here, too, then is a risk that services might benefit from the fact that HUMINT activities or those of CHIS are less densely regulated. What is more, there are severe deficits as regards the regulation and oversight of military intelligence. Here, too, there may be non-benign incentives for civilian-military intelligence interaction and this might increasingly involve the private sector, too. What is more, there is a risk that if finished products are purchased from the private sector one may not sufficiently know what types of data and data collection methods were being used. Here too, there is a risk that services may obtain data via purchases that they would not have been allowed to collect and process themselves.

7 *It seems that some supervisors worry about this evolution and would like to have the possibility to check the contracts and the details of what is provided by these companies, with power of sanctions, if necessary, against them. Do you think it is a necessary move and that it is to them or to courts of auditors specialised in checking military budgets to intervene? What kind of structure or grouping of monitoring actors would be the most capable to intervene, nationally or at the EU, and/or transatlantic level?*

Yes, I think much more should be done to enable comprehensive oversight body access to procurement contracts. As many researchers interested in data purchases by national intelligence agencies can testify, it is very difficult to establish through freedom of information requests the precise nature of "bought intelligence" and contractual obligations relating to its use. One essential piece of information is the contracts between private sector entities and the government. Oversight bodies should be granted unfettered access to any procurement contract that the agencies under their remit have concluded with private sector entities. A good practice in this regard can be found in Canada. Its oversight body NSIRA has a statutory power that ensures this kind of access. According to the NSIRA Act, it is "entitled, in relation to its reviews, to have access in a timely manner to any information that is in the possession or under the control of any department". Importantly, NSIRA, and not other government departments, can decide whether or not the sought information relates to a review or complaint. NSIRA is also entitled to have access to any protected information, such as information "under the law of evidence, solicitor–client privilege or the professional secrecy of advocates and notaries or to litigation privilege".

Another interesting aspect of oversight innovation in this regard comes from Norway. Its EOS Committee can extend its review focus to private sector organisations that work for or with the security and intelligence sector. If the EOS Committee learns that a service uses information provided by a private actor, it can compel access to the information it needs for its investigation directly from the private actor entity.

More generally, there is indeed further international engagement necessary, I believe. European lawmakers, for example, ought to do much more to ensure that data brokers do not gain access to certain types of data in the first place. What is more, the limited interactions data brokers may still have with security agencies ought to be rule-based and independently overseen. A good milestone for this would be to refine and then adopt a "whole of privacy approach" as regards the future regulation and oversight practice of these currently non-compelled modes of intelligence collection. If such data are collected and processed for commercial purposes, they are still likely to be obtained by the IC, which will use them for secondary purposes. In order to make the private sector's initial collection of data and its subsequent data aggregation for security agencies more rule-based and restricted, the GDPR must be applied and enforced more strictly. Doing so requires further refinements to European data protection frameworks and a closer alignment and synchronisation with accountability mechanisms that are geared towards the public sector. More specifically, lawmakers and decision makers should improve the *de facto* effectiveness of the GDPR. This, obviously, is an enormous and pressing endeavour. Among the many steps necessary would be extending the remit of the EDPB to a wider range of cross-border cases. What is more, one should call on lawmakers to ratify their countries' membership of Convention 108+ of the Council of Europe, the only international

legal framework that does not waive safeguards when data processing takes place for security and defence purposes.

In addition, lawmakers ought to do more to adopt a comprehensive and sufficiently foreseeable legal basis when it comes to automated OSINT. More safeguards are clearly necessary with regard to the purchase and use of OSINT analysis tools, including requirements relating to the different data types that can be used to feed cross-system information analysis tools. Reformers should trim the working definition for publicly available information and establish clearer boundaries between systematic and non-systematic collection of "publicly available data". Furthermore, provisions in national intelligence law should be adopted on government access to personal data through data purchases, including better safeguards to ensure the legality of data purchases, data analysis tools, and the subsequent use of data from non-compelled access.

Notes

1 An interview with Thorsten Wetzling by Didier Bigo.
2 See Roller, Sarah Naima, Thorsten Wetzling, Ronja Kniep, and Felix Richter. 2023. Civic Intelligence Oversight: Practitioners' Perspectives in France, Germany, and the UK. Surveillance & Society21(2): 189–204. Available at https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/15217/10813
3 Federal Constitutional Court, BND Act Judgement, 19.05.2020, recitals 292–296, https://data.guardint.org/en/entity/neb3eo8hl9h?page=75
4 https://www.dni.gov/files/ICIG/Documents/Partnerships/FIORC/Signed%20FIORC%20Charter%20with%20Line.pdf
5 For a publicly available agenda of the 2022 IIOF in Strasbourg, see https://rm.coe.int/iiof-2022-agenda-2754–4529-9462-1/1680a9000c
6 https://www.comiteri.be/images/pdf/publicaties/Common_Statement_EN.pdf
7 All quotations provided in this answer refer to this publication by Wouter de Ridder: https://aboutintel.eu/simple-oversight-demands/
8 For a recent and unique articulation of those, see the December 2022 OECD Declaration on government access to personal data held by private sector entities. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487
9 See for example these two piece on Lawfare during and after the OECD negotiation process: https://www.lawfareblog.com/towards-oecd-principles-government-access-data and https://www.lawfareblog.com/gentlemens-rules-reading-each-others-mail-new-oecd-principles-government-access-personal-data-held.

10 Torture and Security Service Mass Surveillance

Elspeth Guild and Sophia Soares

Introduction

The exponential development of computing capacities and interconnectivity which have accompanied the arrival of the internet and social media into everyone's lives has raised profound issues regarding the right to privacy and the protection of personal data. On the one hand, the possibility of contact with other people anywhere on the globe in a matter of nanoseconds and at no (direct) cost has proven exceptionally attractive to people. And, this is only one of the promises of the Internet and social media. In the same regard, the chance to create and develop virtual spaces for all sorts of activities, scientific, artistic, educational, social as well as effect commercial (shopping) and mobility (travel) transactions has similarly attracted enormous numbers of people to these media. On the other hand, the price paid for these possibilities and opportunities can be measured in terms of the loss of privacy for individuals. Virtually every online activity is capable of being tracked, traced, recorded, copied, and shared. Even the best privacy technologies designed to diminish the risk of such interference have proven limited.

Two main sources of interference with privacy online exist. First, there is the private sector itself which collects information on its customers and their preferences. This is an activity which has become exceptionally profitable where data brokers buy massive amounts of personal (and other) data and treat it for use by their customers (or sell it on to them) to achieve greater profitability by reaching ever better-targeted markets. The regulation of these activities is outside the scope of this chapter but is also a challenge for the right to privacy as well as consumer protection.[1] The second source of interference is by states themselves eager to have ever more accurate information about people, their citizens, and others, in order to govern them better. Here states are in a privileged position as they are entitled to pass laws requiring people to hand over their personal data and do so in all sorts of fields of state activity, from tax collection to criminal justice to border control. While states engage in personal data collection of their own, acquiring data directly from people they encounter, they also engage with the private sector, requiring private bodies to hand over the personal data which they

DOI: 10.4324/9781003354130-11

have collected in the course of their commercial activities (such as passenger name records). It is this second area which is of interest to us here.

Our focus in this chapter is on states' claim to an entitlement to collect and process personal data, the justifications which are given for such activities and how to protect the right to privacy in the face of them. The tension which exists between state authorities and people regarding the protection of privacy and delivery of data protection is not new. The 19th-century development of the principle of privacy was codified in international law after World War II and is now contained in Article 17 of the International Covenant on Civil and Political Rights 1966 (ICCPR).[2] Already in 1988, the UN Human Rights Committee issued General Comment 16 clarifying the meaning of Article 17 with reference to developing mechanisms of mass surveillance.[3] It is also found in regional human rights instruments, EU law, and national constitutions in many countries around the world also protect privacy and its concurrent duty of data protection.[4] Social media and computing techniques for the fine-grained analysis of data and states use of these tools to obtain and use personal data became a matter of international politics when Edward Snowden revealed the extent of US NSA bulk personal data collection and use for surveillance purposes.[5] The UN reacted by defining the position in international law on the Right to Privacy in the Digital Age in 2014 (the Report).[6] This initial report has been followed by annual reports of the same title presented by the UN Commissioner for Human Rights to the Human Rights Council addressing challenges.

Since then, there has been a very substantial struggle surrounding the crystallisation of international standards of privacy set out in Article 17 ICCPR. As discussed elsewhere in this volume, among the state agencies most anxious to obtain, use, and control personal data on an industrial scale have been security services. As the NSA scandal revealed, these agencies have been the least hampered by legal constraints regarding privacy, frequently using national constitutional rules dividing the rights of citizens from those of aliens and focusing on aliens though "inadvertently" also collecting massive amounts of personal data from their own citizens. One might say that some security services have become addicted to personal data (SIGINT)[7] as opposed to human intelligence. But this debate is outside our scope. Instead, in this chapter we take as the state of international human rights law Article 17 ICCPR as applicable to all interferences with the right to privacy and data protection. Furthermore, we accept the UN 2014 report on The Right to Privacy in the Digital Age as representing the consensus of the international community regarding a correct interpretation of the right to privacy.

This means that the right to privacy applies to everyone irrespective of nationality or geography. The content of the right to privacy is that there must never be an arbitrary or unlawful interference with the right to privacy and the right must be protected by law. Unless there is a lawful ground for interference with an individual's right to privacy, a person's personal data can only be used by others if accompanied by valid consent for the specific

purpose which is clear and precise and limited strictly to that purpose. Once the extent of that consent has been extinguished, the personal data must be destroyed. The justification which security services generally use to dispense with the consent requirement (that is where they accept at all that their use of personal data is limited by international human rights law) is necessity for the purposes of the fight against terrorism, the protection of national security and stopping serious organised crime (this third ground is not used by all security services as it is often within the mandate of the criminal justice services alone).

The problem then becomes how to enforce the right to privacy in international human rights law. It is apparent that under pressure from technological change, state capacities, and the demands of some state agencies, protecting the right to privacy needs new tools at the international level to prevent abuse and backsliding. As one scholar put it, we need to make the violation of the right to privacy as self-evidently wrong as engaging in torture.

In this chapter, we examine how the protection of another human right – the prohibition on torture – has given rise to new tools intersecting between the international, regional, and national frameworks to bring to the ground increasingly effective enforcement of the prohibition. The UN adopted a Convention against Torture in 1984 and it remains among the most widely ratified conventions in the human rights area. In 2002, in response to concerns about the correct implementation of the prohibition, the international community adopted a protocol (the Optional Protocol to the Convention against Torture) which requires states to create National Preventative Mechanisms (often a mandate given to national human rights institutions) whose job is to ensure the correct national implementation of the prohibition on torture. The protocol includes a sophisticated system of national and international cooperation and mutual reinforcement which has already delivered promising results on the ground. In the next two sections, we will explain this system and how it works before coming back, in our conclusions regarding the potential of such a system for the protection of the right to privacy.

The path to the optional protocol to the convention against torture

The prohibition on torture as we know it today only emerged in the post-World War II era with the development of international human rights law.[8] The prohibition was enshrined internationally in both "soft law" – including in Article 5 of the Universal Declaration of Human Rights 1948[9] – as well as in binding law, notably in Article 7 ICCPR.[10] The latter Article proclaims that "[n]o one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment" and is to be read in conjunction with the Covenant's Article 4 which explicitly proscribes any derogation from aforesaid prohibition.[11] Similar iterations of the prohibition have arisen over time in regional instruments including in Europe, the Americas, and Africa.[12] On each occasion, the prohibition was recognised as an "absolute" human right

in the sense that states were (and still are) bound to uphold it, even in times of public emergencies threatening the life of their nation.[13]

Notwithstanding such lofty intentions by the international community, torture was still only prohibited in theory. Torture continued to be systematically practiced around the world with particularly cruel practices observed in the Latin American context. In 1972, Amnesty International launched its worldwide campaign against torture followed two years later by the UN Human Rights Commission taking the unprecedented step to formally express its concerns to the Chilean government about the documented cruel torture methods practiced by its military junta, just one of a number of systematic torture practices from around the world. In 1975, the UN General Assembly adopted the Declaration on the Protection of All Persons from Being Subjected to Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment which would later serve as a model for the UN Convention against Torture (Torture Convention).[14]

During the drafting stages of the Torture Convention, which was formally commenced by a UN-designated working group in 1978, innovative approaches to fighting the phenomenon were put forward including entrusting the Human Rights Committee with such special tasks as examining state reports, deciding on individual and inter-state complaints, and conducting *ex officio* inquiries. In the end however states agreed instead on the proposal to establish a "Committee against Torture" consisting of independent experts entrusted with the task of monitoring compliance with the Torture Convention. Controversial issues in relation to matters such as the inquiry procedure under Article 20 were settled by compromises (including "opting-in" clauses, etc.) and the draft submitted by the working group and adopted by the UN Human Rights Commission in 1984 was transmitted to the UN General Assembly which forum adopted it unanimously on Human Rights Day of that same year, 10 December 1984, as the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment.[15] States parties to the Convention currently stand at 173 and universal ratification is actively being pursued by various actors including the "Convention against Torture Initiative".[16] In terms of content, the Convention provided the first ever international definition of torture – as any setting where state officials may be involved in inflicting "severe pain or suffering, whether physical or mental" on an individual – keeping its focus on the criminalisation of torture in national laws, ensuring remedies for victims whilst also placing certain torture prevention responsibilities on States parties.[17]

In addressing the phenomenon of torture historically, international human rights law thus, in the first instance, sought to criminalise acts of torture which can be seen as a "reactive" response to the problem. What the Torture Convention fell short of accommodating at the time of adoption however was the proposal by Costa Rica for an optional protocol (OP) to put in place a system of preventive and unannounced visits to places of detention. The

proposal was based on the idea by Jean-Jacques Gautier – founder of the Swiss Committee against Torture (now the Association for the Prevention of Torture) – to open up places of detention to outside scrutiny and create a system of unannounced visits. He was in turn inspired by the visits of the International Committee of the Red Cross to prisoners of war and believed that copying such preventive measures in peacetime, on a basis of cooperation and confidentiality, could render torture much less likely.[18]

An approach such as the above would have provided a truly preventive dimension – a more "pro-active" response to the problem – as well as a practical means for States parties to implement their prevention responsibilities under the Torture Convention and thereby reach compliance with the overall prohibition on torture. Post-adoption of the Torture Convention, the UN Human Rights Commission deferred consideration of the OP several times until 1991 by which time "much had changed" in terms of the Torture Convention having entered into force (in 1987), the mandate of the UN Special Rapporteur on Torture having been established[19] and the workability of a preventive visits system having been demonstrated within the Council of Europe setting.[20] In addition, the Cold War had ended, loosening political constraints to negotiations concerning sovereignty-related issues which the proposed system inevitably presented.

The realisation of the optional protocol gaining momentum in a changed environment

The necessity of a preventive dimension in the context of the prohibition on torture seemed to at least merit examination which was exactly what an NGO coalition expressed in its written statement submitted to the UN Human Rights Commission ahead of the latter's consideration of a re-worked Costa Rica draft of the OP in 1992. It seemed that the 11-year delay to considering the proposal ultimately led to the establishment by the Commission of an open-ended working group whose task it would be to draft the OP on the basis of the latest Costa Rica proposal. After meeting annually for the subsequent decade, negotiations nearly reached a deadlock and were only salvaged by late-in-the-day proposals of combining the creation for an international visiting committee with "National Preventive Mechanisms". This proposal, first submitted by the Mexican delegation and then, in a revised version, by the EU bloc, was to become the basis for the final text which was presented to the Commission.[21] Moreover, negotiators were also likely spurred on by the Vienna Declaration and Programme of Action 1993 unapologetically reaffirming that efforts to eradicate torture should primarily be concentrated on prevention and calling for the early adoption of an OP establishing preventive visits to places of detention.[22]

At the time of the OP working group negotiations and final proposal, many states already had a pre-existing commitment to the prohibition on torture as it was contained in both Article 7 ICCPR and the Torture Convention. The OP

proposed nothing additional to its parent treaty in terms of substantive articles, instead elaborating on its effective implementation through a purely preventive approach rather than an adjudicate one. It was (and is) due to the nature of torture taking place in secret[23] that the effective implementation of the Torture Convention necessitated a system of independent monitors with the authority to make unannounced visits. This view was in fact reflected explicitly in the Preamble to the proposed OP which stated that States parties are "[c]onvinced that further measures are necessary to achieve the purposes of the [Torture Convention] and to strengthen the protection of persons deprived of liberty against torture".[24] The proposed OP text was adopted by the UN Human Rights Commission by 27 votes to 10 with 14 abstentions in April 2002 (after having warded off a "no-action" motion challenge from the USA).[25] It gathered momentum while making its way through the UN system during the following months and was finally put to the UN General Assembly in December of 2002 at which venue it was adopted by 127 votes to 4, with 42 abstentions.[26]

The Optional Protocol to the Convention Against Torture (OPCAT) was thereby adopted and a string of ratifications by primarily Council of Europe Member States and Latin American states ensured its relatively swift entry into force on 22 June 2006.[27] The initial ten-member Subcommittee on Prevention of Torture (SPT or Subcommittee), the international element of the Optional Protocol, took up its work and embarked upon its first "programme of visits" one year later by which time it already self-identified as a "new type of United Nations treaty body".[28] By 2009, State party accession to OPCAT had reached the threshold of 50 to trigger the enlargement of the Subcommittee from 10 to 25 members. This in turn propelled it into becoming the largest sitting UN human rights treaty body which it still is to this day (Table 10.1).

The importance of a regional bloc, in this case the Council of Europe, in pushing ratification was significant. The Council of Europe's own European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment[29] (adopted in 1987) had already been ratified by all 46 Member States by the mid-noughties in addition to future Member State Montenegro by way of the 1993 protocol which opened it up to non-member states. The Convention is primarily devoted to creating an implementation and monitoring mechanism for preventing torture, inhuman and degrading treatment and punishment in the form of a committee with powers to visit places of detention and assess how persons deprived of their liberty are treated in order to strengthen their protection from torture and other ill-treatment. The strengths and weaknesses of this implementation approach were already becoming clear when OPCAT was adopted and its text thus addresses the limitations of a single committee charged with monitoring activities in multiple states. The need to develop capacity and mechanisms on the ground in Member States was already apparent to those seeking to implement the prohibition on torture within the Council of Europe. This led to substantial pressure in that

Table 10.1 OPCAT Timeline

OPCAT Timeline		
Year	*Event*	*Remarks*
1948	Universal Declaration of Human Rights adopted by UN General Assembly	Prohibition on torture in Article 5
1966	International Covenant on Civil and Political Rights 1966 adopted by UN General Assembly	Prohibition on torture in Article 7
1975	Declaration on the Protection of All Persons from Being Subjected to Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment adopted by UN General Assembly	
1976	Swiss banker Jean-Jacques Gautier launces idea of international visiting mechanism to places of detention	Idea based on visits to prisoners of war by the International Committee of the Red Cross; Jean-Jacques Gautier founds the Swiss Committee against Torture in 1977 (now the Association for the Prevention of Torture)
1978	UN Convention against Torture negotiations	Visiting mechanism idea first raised formally
1980	Costa Rica submits first draft OPCAT	Draft prepared by the Swiss Committee against Torture (now the Association for the Prevention) and the International Commission of Jurists
1984	UN Convention against Torture adopted	Comes into force in 1987 and establishes the Committee against Torture; Protocol omitted
1987	Council of Europe's European Convention for the Prevention of Torture adopted	Comes into force in 1989 and establishes the European Committee for the Prevention of Torture
1989	Fall of the Berlin wall and end of Cold War	Enables negotiations

(*Continued*)

Table 10.1 (Continued)

OPCAT Timeline		
Year	*Event*	*Remarks*
1992	UN Human Rights Commission considers re-worked Costa Rica draft backed by an NGO coalition; UN open-ended working group to draft OPCAT designated and starts work	Formal annual meetings take place over the following decade
1993	Vienna Declaration and Programme for Action calls for the early adoption of OPCAT	
2001	Mexico draft suggests NPMs; EU bloc reworks NPM suggestion and submits draft	
2002	OPCAT text adopted by the UN General Assembly	By this time, the International Covenant on Civil and Political Rights had been in forced for 26 years, the UN Convention against Torture had been in force for 15 years, and the European Convention for the Prevention of Torture (with its visiting Committee) had been in force for 13 years
2006	OPCAT enters into force	20 ratifications
2007	10-member OPCAT Subcommittee on Prevention of Torture takes up its work	
2009	OPCAT Subcommittee expands to 25 members	50 States parties; Largest UN human rights treaty body
2022	91 States parties and a further 25 States signatories; 77 States parties with designated NPMs	

region to ratify OPCAT with its more developed mechanisms linking the international monitoring body with national ones.

The political context is also one which must never be forgotten. The end of bipolarity symbolised by the fall of the Berlin wall in November 1989 led to substantial unrest in Europe, the creation of a number of new states, and civil war in the then Socialist Federal Republic of Yugoslavia. The extent of human rights abuses observed in that war shocked Europe out of its post-World War II complacency that torture was an exception in Europe and war unimaginable. A number of Council of Europe organs and instruments came into being as the details of the atrocities (some being classified as genocide by the International Criminal Tribunal for the Former Yugoslavia)[30] became known in Europe. The importance of enhancing monitoring mechanisms against torture was highlighted by these events.

The OPCAT framework

The framework of the Optional Protocol to the Convention Against Torture (OPCAT) encompasses a global mandate and an innovative manner of linking international and national torture prevention mechanisms to ensure a comprehensive approach to furthering the effective implementation of the prohibition on torture. As alluded to above, the introduction of the national mechanisms might have occurred to appease certain blocs of states during the drafting stages, but it is arguably this element of dual international-national implementation that ensures the effectiveness of the framework. The mechanisms under OPCAT thereby consist of the Subcommittee on Prevention of Torture along with the National Preventive Mechanisms (NPMs). This dual approach to torture prevention is ground breaking[31] – especially as the NPM element essentially domesticates international torture prevention[32] – and it has been praised widely.[33] The approach of using national independent bodies to form part of treaty implementation has since been duplicated in other fora such as in the frameworks of the Convention on the Rights of Persons with Disabilities and the International Convention for the Protection of All Persons from Enforced Disappearance, respectively.[34] It could in fact be claimed that OPCAT facilitated the coming into being of what was arguably the beginning of a transition time for the international human rights regime from an "era of declaration" to an "era of implementation".[35]

At the international level, the SPT has a three-pronged mandate, incorporating its three "Pillars" of work: visits to places of detention in States Parties; an advisory role vis-à-vis NPMs; and cooperation with other UN, international, regional, and national entities.[36] Other important factors which can impact on the Subcommittee's ability to fulfil its role with regards to the above activities include its membership[37] as well as the financial and human resources allocated to it.[38] At the national level, in turn, each State party's designated NPM must carry out regular detention visits[39] (a "continuation" of the SPT's much less frequent visits) while also working with government

and civil society partners to further the implementation of OPCAT.[40] Specifically, the NPMs are mandated to make recommendations to relevant authorities and submitting proposals and observations on legislation[41] as well as to carry out additional activities including awareness raising.[42] NPMs are independent bodies but part of state monitoring apparatuses. The independence of each NPM is particularly central to its effectiveness in fulfilling its role as is its membership and the availability of resources.[43] Of particular interest from an outside perspective, is perhaps the NPMs' accountability to and relationship with the SPT.[44] OPCAT Article 11(1)(b) mandates the SPT to advise on and assist with the establishment and evaluation of States Parties' NPMs as well as to offer training, technical assistance, recommendations, and observations with a view to strengthening the capacity and/or the mandate of the NPMs. Overall, out of the 78 visits ever conducted by the SPT, 10 have had a special NPM focus.[45]

OPCAT Article 4 authorises the SPT and NPMs to visit places of detention and assess the conditions of that detention with a view to strengthening the protection of detainees against incidences of torture and other ill-treatment.[46] As proclaimed by the Association for the Prevention of Torture, the OPCAT represents a paradigm shift in that it replaces the secrecy of detention by transparency in the form of these unannounced visits. The basic idea being that if it is the secrecy in places of detention that enables torture then by eliminating – or reducing – that secrecy element, the risk of torture will inevitably be reduced or eliminated altogether.[47] "Places of detention" in this context refers to all places where persons are or may be liberty deprived and thus fall under the OPCAT framework.[48] Article 4 cites that:

1 Each State Party shall allow visits […] to any place under its jurisdiction and control where persons are or may be deprived of their liberty […] These visits shall be undertaken with a view to strengthening, if necessary, the protection of these persons against torture and other cruel, inhuman or degrading treatment or punishment.
2 [D]eprivation of liberty means any form of detention or imprisonment or the placement of a person in a public or private custodial setting which that person is not permitted to leave at will by order of any judicial, administrative or other authority.[49]

The Article thus sets out an understanding of 'deprivation of liberty' as an umbrella-type term for a variety of confinement forms from which a person is not permitted to leave at will.[50] The SPT has noted on several occasions that the terms employed in Article 4 should be given a broad interpretation[51] and that the term "places of detention" is to be interpreted extensively to include multiple types of places[52] beyond the traditional, such as prisons and police cells, to inter alia closed psychiatric units, homes for the elderly and immigration detention which could all be described as "less traditional places of detention".[53]

As part of their mandated activities, the SPT and the NPMs thus conduct unannounced visits to places of detention but how does the larger framework of the OPCAT work in practice, of what does it consist, and which checks are in place to ensure its effectiveness? Rather than additional reporting requirements, the OPCAT establishes practical obligations on States parties to ensure that they are in a position to comply with their pre-existing normative obligations on the prohibition on and prevention of torture.[54] Bearing in mind the overarching aim of establishing cooperation and a triangular relationship between States parties, the SPT, and the NPMs, those state obligations can be classified into seven broad categories as follows:

1 to establish, designate, or maintain an NPM (or NPMs);
2 to open up all places of detention under its jurisdiction and control to external scrutiny by its NPM(s) and the SPT;
3 to facilitate contact between its NPM(s) and the SPT;
4 to provide information to its NPM(s) and the SPT on domestic detention procedures and preventive measures;
5 to consider the recommendations of its NPM(s) and the SPT;
6 to cooperate with its NPM(s) and the SPT; and
7 to publish the annual reports of its NPM(s).[55]

Thinking outside the box: The SPT and NPMs

Constituting the international element of the OPCAT framework, the Subcommittee on Prevention of Torture comprises 25 members who are all independent experts elected by and from within States parties.[56] As mentioned above, the SPT's mandated activities are essentially divided into three "Pillars", as per OPCAT Article 11, the first being[57] the Subcommittee's visits to places of detention – or "to any place under [a State party's] jurisdiction and control where persons are or may be deprived of their liberty"[58] – and making recommendations to States Parties concerning the protection of liberty deprived persons against torture and other ill-treatment by way of issuing confidential reports to States parties following such visits.[59] The reports will only ever be made public with the relevant State party's consent or, alternatively, as a consequence of non-cooperation.

Visits to States parties fall under Pillar II of the SPT's activities when they are designated as having "a special NPM focus". In fact, all NPM-related activities of the Subcommittee, whether or not they form part of a country visit, fall under this Pillar. Specifically, the SPT is mandated to advise on and assist with the establishment and evaluation of States parties' NPMs as well as to offer training, technical assistance, recommendations and observations to NPMs with a view to strengthening their capacity and/or their mandate. NPMs should in turn cooperate with the SPT. The OPCAT principles of cooperation and constructive dialogue is reflected here and in practice translates into an expectation that the Subcommittee and the NPMs will

work in a complementary manner. To facilitate its Pillar II activities, the SPT is required to have direct contact, confidential if necessary, with the NPMs[60] and it is the obligation of States parties to allow such contact.[61] A former UN Human Rights Commissioner has referred to this "unique interplay" between NPMs and the SPT as reinforcing the "potential of both to spare countless human beings from the horrors of torture and other ill-treatment".[62]

Finally, the Pillar III mandate covers the Subcommittee's cooperation activities for the prevention of torture in general, with relevant UN, international, regional and national entities. Some relevant cooperation activities are reported in annual reports as well as in visiting reports while presumably an important extent of this work remains confidential.

Implementing torture prevention obligations at the national level

As the first exclusionary preventive international human rights treaty, OPCAT is also the first to entrust national bodies (i.e. NPMs) with its implementation. In order for the NPM system to work effectively however, the NPMs must be equipped with a strong legislative mandate as well as the necessary human and financial resources while their independence must be maintained.[63] It is only then, in combination with their day-to-day presence within and knowledge of the local context, that they can effectively fulfil their mandated role and hence the reason why the OPCAT framework insists on guaranteeing those conditions. Bearing in mind that the effective functioning of NPMs is a continuing obligation of States parties, key to meeting the requirements necessarily includes regular assessments by the respective State party as well as by the NPM itself, taking into account the SPT's views. Independence of the NPMs is likewise crucial - in terms of its mandate, operations and finances - alongside its ability to fulfil its key functions with the help of expert and independent members.[64]

As we have seen, the activities of NPMs reflect those of the Subcommittee with necessary variations and, of course, are restricted to the national level. In effect, NPMs' functions are four-fold, starting with their visiting mandate which is equally broad as that of the SPT under OPCAT Article 4. The places of detention that the NPMs should visit include both those located within the territory of the State party as well as those outside of it but within the State party's powers or effective controls. With the SPT having conducted periodic visits to States parties on average only every 5–6 years (which is to be the expected regularity of visits by an international body), the NPM element is vital in completing the preventive framework under the Optional Protocol.

Secondly, NPMs have a vast advisory function which entails them reviewing any relevant rules concerning matters such as detention or interrogation and treatment of persons deprived of their liberty; providing recommendations to State authorities on legislative proposals; and, providing input to States parties' reports as well as to other human rights mechanisms. Thirdly, the educational function of the NPMs include ensuring that relevant

professionals, such as civil and military personnel (but in effect anyone involved with liberty deprived persons), receive satisfactory education on torture prevention.

Fourthly, and finally, is the cooperative function of the NPMs, not just vis-à-vis the SPT, as highlighted above, but also entailing a meaningful dialogue with state authorities as well as with other relevant stakeholders involved with torture prevention. This in turn reinforces the triangular relationship between these bodies as envisaged under OPCAT. Cooperation between NPMs is also encouraged so that best practices and the like can be shared.

Adjusting to State Diversity without Sacrificing Effectiveness

OPCAT Articles 3 and 17 require that States parties establish, designate or maintain an NPM within a year of becoming party to OPCAT. If a declaration is made under Article 24, this period can be extended by three years with a further two-year extension requiring approval through consultations between the SPT and the State party.[65] In any case, once an NPM has been designated, the State party must promptly notify the SPT and publicly promulgate the NPM at the national level. Under the Optional Protocol, States parties are at liberty to establish new bodies or designate existing ones as their NPM as long as they are allowed to perform their functions in accordance with the required stipulations. From among the 91 States parties to the OPCAT, 77 have so far designated their NPMs.[66] The Association for the Prevention of Torture classifies each NPM as falling into one of the following categories:[67]

- Multiple Institutions (6)
- National Human Rights Commission (17)
- National Preventive System in Federal State (2)
- New Specialised Institution (13)
- Ombuds Institution (32)
- Ombuds Plus Institution (6)
- Other: Inter-Governmental Body (1)

The bracketed numbers show the occurrences of each NPM type on a global scale. It is immediately obvious that OPCAT States parties have taken a varied approach to the designation of NPMs which reflects the adaptability and suitability of the system to a variety of state structures.[68] While most NPMs are ombuds institutions or national human rights commissions, an important share (17%) are new institutions established with a specific NPM mandate. In terms of assistance to States parties, technical support is available vis-à-vis the establishment and effective functioning of their NPMs and can be sought from the OHCHR Treaty Body Capacity Building Programme which has provided national training courses on accession to the Optional Protocol and to the Torture Convention and on NPMs jointly with the

Subcommittee. OHCHR's field presences have inter alia provided advice on NPM establishment and collaboration with the authorities while the OPCAT Special Fund supports the implementation of publicly available SPT recommendations vis-à-vis the establishment or strengthening of NPMs.[69]

Cooperation, supervision, and consultation – the SPT and NPMs

As alluded to above, one of the triangular relationships under the OPCAT framework is that of the SPT and the NPMs. In fact, the coherency of the OPCAT framework is in effect premised on the Subcommittee – in its role as the international preventive mechanism – guiding and guarding the system as a whole.[70] Accordingly, upon establishment of an NPM, the SPT is to establish and maintain direct contact with the newly designated mechanism to facilitate collaboration and exchanges of information. Specifically, the Subcommittee supports and advises NPMs through: 1. Offering training and technical assistance, with a view to strengthening their capacities; 2. Assisting in the evaluation of their needs and the means necessary to strengthen the protection of persons deprived of their liberty against torture and other ill-treatment; and, 3. Making recommendations and observations to States parties, to strengthen the capacity and mandate of NPMs.[71]

In practice, it is reported that the SPT provides support to NPMs via regular e-mail correspondence amongst other forms of contact.[72] Furthermore, the SPT member assigned as rapporteur for a certain State party is responsible for liaising with its respective NPM. The SPT also issues general guidelines and assessment tools to NPMs as well as thematic advice such as how to carry on its preventive monitoring under COVID-19 times.[73]

The establishment and development of the SPT/NPM structure took time and dedication. The interlocking nature of the relationships at the international, regional, and national levels has made possible the delivery of real monitoring at the national level by independent bodies, assisted and advised by regional and international counterparts. The detail with which we have set out the development and operation of the OPCAT system is designed to encourage states and NGOs to reflect on how such a system could be envisaged and put into place as regards the right to privacy. The challenges which brought the OPCAT system into place were as enormous and apparently intractable as the challenges which are currently facing the right to privacy. It is to this aspect we will turn now.

A model for the right to privacy?

In 2013–14 at the UN, the pressure for action to control mass surveillance of personal data and its use came from two countries: Germany and Brazil. At the time there was some discussion of the possibility of an optional protocol to ICCPR on a monitoring mechanism for Article 17. The political impetus however was insufficient to take that idea forward, indeed even the UN Human Rights Committee's General Comment 16 was not updated as a

result of the pressure for better protection of privacy. However, in the European context, both the Council of Europe and the European Union adopted new instruments to protect privacy.[74] Yet, the international reach of privacy infringements made possible by new media and used by state authorities for security purposes far outstretches Europe.

To come back to the purpose of this chapter, can lessons be learned from the development of monitoring mechanisms against state use of torture[75] assist to develop mechanisms against infringements of privacy in the form of mass surveillance, the answer is clearly yes. The first step, if the model of OPCAT is to be followed is by preference the adoption of an optional protocol to ICCPR setting out a monitoring mechanism for Article 17. This would not be the first time since the adoption of OPCAT that pressure has mounted to use similar tools to protect other rights such as the rights of persons with disabilities and the protection of all persons from enforced disappearances as mentioned above. In relation to the former, national human rights institutions formed a prominent part of the lead up to the adoption of the relevant convention which includes a requirement for states parties to inter alia designate "one or more independent mechanism(s)" at the national level to facilitate the implementation of the convention.[76] In relation to the protection of all persons from enforced disappearances, the relevant convention requires the cooperation of its Committee with all relevant institutions, agencies, or offices of the States parties.[77]

An optional protocol along the lines of OPCAT creating an equivalent of the SPT and a duty of state parties to create NPMs (which are truly independent) would be an excellent approach. In fact, a number of national human rights institutions are already mandated to address privacy-related issues. According to our interlocutors, one of the keys to the success of OPCAT both in the development, design, and adoption stages has been the active participation of NGOs. One in particular, the Swiss NGO, the Association for the Prevention of Torture, was singled out as particularly important in bringing pressure to bear at the national level to ratify OPCAT. But it was also very important in bringing civil society pressure to the UN, convincing states in the UN General Assembly to support OPCAT.

There is no silver bullet to control and limit mass surveillance contrary to Article 17 ICCPR either by state or non-state bodies. But international legal frameworks are part of the solution. As the problem is an international one, with cross-border movement of personal data providing the source of mass surveillance, international tools to control it must be put into play. Of course, the right to privacy is a qualified right, unlike the prohibition on torture which is absolute. States' claim to the legitimacy of interferences with personal data and thus privacy is primarily based on the need to protect national security. This of course raises the question, how did states protect national security (encompassing action against terrorism, serious organised crime, trafficking in human beings, and the protection of state interests) before mass

surveillance through technological media was possible, however, we will leave that question aside.

We rather, ask the question: as there is a right to privacy to which mass surveillance is an interference as accepted by the international community embodied in the UN, what justifications do states provide for the interference on the grounds of national security? All too often the claim of necessity to protect national security goes unexplained and unchallenged. As soon as a state authority raises the claim of national security, the authority making the claim all too often expects that considerations of human rights and legality will fall away (in cases where the right in question is a qualified one). This must change. If a state claims national security, that claim must be justified on the basis of evidence and susceptible to judicial control. Within a multi-layered system of monitoring,[78] national claims must be justified not just to quasi-independent (or not even) bodies which have been established by executives convinced by their security services of the value of mass surveillance but also to international instances. A counterbalance needs to be created which can challenge the quasi-automaticity of rubber-stamping state claims to national security in the area of mass surveillance and purporting to justify national security as always trumping the right to privacy without any concrete evidence of necessity being produced against which a proportionality test could be applied. International and regional human rights pressure needs to be applied in addition to national willingness to change the balance of power around state mass surveillance and the right to privacy in the digital age.

Notes

1 Among areas of specific concern are the protection of minors, vulnerable persons (such as those with addictions), etc.
2 UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171: Article 17 "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks".
3 UN Human Rights Committee, *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988, available at https://www.refworld.org/docid/453883f922.html
4 Oliver Diggelmann and Maria Nicole Cleis, "How the right to privacy became a human right," *Human Rights Law Review,* 14.3 (2014): 441–458; Arianna Vedaschi and Valerio Lubello, "Data retention and its implications for the fundamental right to privacy: A European perspective," *Tilburg Law Review,* 20.1 (2015): 14–34.
5 Zygmunt Bauman et al., "After Snowden: Rethinking the impact of surveillance," *International political sociology*, 8.2 (2014): 121–144.
6 UN General Assembly, *The right to privacy in the digital age - Report of the Office of the United Nations High Commissioner for Human Rights*, (A/HRC/27/37), 30 June 2014.

7 Nicole Perlroth, Jeff Larson and Scott Shane, "NSA able to foil basic safeguards of privacy on web," *The New York Times*, 5 (2013): 1–8.
8 Manfred Nowak, Moritz Birk and Giuliana Monina, eds., *The United Nations Convention Against Torture and Its Optional Protocol - A Commentary*, 2nd ed., (Oxford: Oxford University Press, 2019), 2.
9 UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III), available at https://www.refworld.org/docid/3ae6b3712c.html
10 UN General Assembly, *International Covenant on Civil and Political Rights*.
11 Ibid: Article 4, especially Article 4(1)-(2).
12 Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5, available at https://www.refworld.org/docid/3ae6b3b04.html; Organization of American States, *American Convention on Human Rights ("Pact of San Jose")* Costa Rica, 22 November 1969, available at https://www.refworld.org/docid/3ae6b36510.html; Organization of African Unity, *African Charter on Human and Peoples' Rights ("Banjul Charter")*, 27 June 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), available at https://www.refworld.org/docid/3ae6b3630.html
13 UN General Assembly, *International Covenant on Civil and Political Rights*: Article 4(1).
14 Nowak et al, *Convention Against Torture – A Commentary*: 2–3.
15 UN General Assembly, *Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment,* 10 December 1984, United Nations, Treaty Series, vol. 1465, p. 85, available at https://www.refworld.org/docid/3ae6b3a94.html
16 See UN Treaty Collection for the status of ratifications of the Torture Convention (correct as at 20 September 2022), available at https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-9&chapter=4&clang=_en and the 'Convention against Torture Initiative' at https://cti2024.org
17 For torture prevention responsibilities, see particularly Articles 2 and 16 of the UN General Assembly, *Convention against Torture*.
18 See amongst many sources, Nowak et al, *Convention Against Torture - A Commentary*: 4; "The OPCAT: Torture prevention in practice," *Association for the Prevention of Torture*, http://www.apt.ch/en/what-we-do/achievements/opcat-torture-prevention-practice; Edouard Delaplace and Matt Pollard, "Visits by human rights mechanisms as a means of greater protection for persons deprived of their liberty," *International Review of the Red Cross*, 87.857 (2005): 69–82, 70).
19 See the website of the UN Special Rapporteur on Torture at https://www.ohchr.org/en/special-procedures/sr-torture
20 Rachel Murray et al., *The Optional Protocol to the UN Convention Against Torture*, (Oxford: Oxford University Press, 2011), 22.
21 Ibid: 23–26.
22 See UN General Assembly, *Vienna Declaration and Programme of Action*, 12 July 1993, A/CONF.157/23: paragraph 61, available at https://www.refworld.org/docid/3ae6b39ec.html
23 See "The OPCAT: Torture prevention in practice," *Association for the Prevention of Torture*, http://www.apt.ch/en/what-we-do/achievements/opcat-torture-prevention-practice
24 UN General Assembly, *Optional Protocol to the Convention Against Torture and other Cruel, Inhuman and Degrading Treatment or Punishment*, 9 January 2003, A/RES/57/199: Preamble, available at https://treaties.un.org/doc/source/docs/A_RES_57_199-E.pdf
25 The Economic and Social Council official records, Commission on Human Rights, *Report on the Fifty-Eighth Session,* 18 March - 25 April 2002, E/2002/23 E/CN.4/2002/200: 17.
26 UN General Assembly, *Optional Protocol to the Convention Against Torture.*

27 See further the UN Treaty Collection for the status of ratifications of the OPCAT, available at https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-9-b&chapter=4&clang=_en
28 UN Committee Against Torture, *1st annual report of the Subcommittee on Prevention of Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*, 14 May 2008, CAT/C/40/2, available at https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=12&DocTypeID=27
29 Council of Europe, *European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment*, 26 November 1987, ETS 126, available at https://www.refworld.org/docid/3ae6b36314.html
30 International Criminal Tribunal for the former Yugoslavia, *Prosecutor v. Radislav Krstic – Judgment*, August 2, 2001 (Krstic judgment).
31 Malcolm D. Evans and Claudine Haenni-Dale, "Preventing Torture? The Development of the Optional Protocol to the UN Convention Against Torture," *Human Rights Law Review,* 4 (2004): 19–55, 20.
32 See further Stéphanie Lagoutte, Sébastien Lorion and Steven L. B. Jensen, eds., *The domestic institutionalisation of human rights* (Abingdon: Routledge, 2021).
33 See for example Manfred Nowak, "What did OPCAT add to the existing mechanisms in the fight against torture?," *Subcommittee on Prevention of Torture - 10th Anniversary of the OPCAT Celebration Event - Speeches,* 2016, available at https://www.ohchr.org/EN/HRBodies/OPCAT/Pages/OPCAT10Speeches.aspx
34 Rachel Murray, "National Preventive Mechanisms under the Optional Protocol to the Torture Convention: One Size Does Not Fit All," *Netherlands Quarterly of Human Rights*, 26.4 (2008): 485–516, 486.
35 See further Sébastien Lorion, "A Model for National Human Rights Systems? New Governance and the Convention on the Rights of Persons with Disabilities," *Nordic Journal of Human Rights*, 37.3 (2019): 234–258.
36 UN General Assembly, *Optional Protocol to the Convention Against Torture*: Article 11(1)(a)-(c).
37 Ibid: Articles 5–10.
38 Ibid: Article 25.
39 Ibid: Article 19(a).
40 See "National Preventive Mechanisms - Subcommittee on Prevention of Torture," *UN Office of the High Commissioner for Human Rights*, https://www.ohchr.org/en/treaty-bodies/spt/national-preventive-mechanisms
41 UN General Assembly, *Optional Protocol to the Convention Against Torture*: Articles 19(b)–(c).
42 UN Subcommittee on Prevention of Torture, *Analytical assessment tool for national preventive mechanisms,* CAT/OP/1/Rev.1, 25 January 2016: section II, paragraph 9, available at https://www.ohchr.org/sites/default/files/Documents/HRBodies/OPCAT/CAT-OP-1-Rev-1_en.pdf
43 UN General Assembly, *Optional Protocol to the Convention Against Torture*: Article 18(1)–(3).
44 Ibid: Articles 18(4) and 20(f).
45 These numbers do not take into account suspended or terminated visits or visits not listed on the SPT's website (correct as at 20 September 2022). Chronological list of SPT visits available at https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/CountryVisits.aspx?SortOrder=Chronological
46 UN General Assembly, *Optional Protocol to the Convention Against Torture*: Article 4(1); "The term "ill-treatment" is used to refer to any form of cruel, inhuman or degrading treatment or punishment", see UN Subcommittee on Prevention of Torture, *Report on the visit made by the Subcommittee on Prevention of Torture to Italy*, 23 September 2016, CAT/OP/ITA/1: paragraph 4.

47 See "The OPCAT: Torture prevention in practice - What is the impact of the OPCAT," *Association for the Prevention of Torture*, http://www.apt.ch/en/what-we-do/achievements/opcat-torture-prevention-practice; Delaplace and Pollard, "Visits by human rights mechanisms as a means of greater protection for persons deprived of their liberty": 70.
48 Nowak et al, *Convention Against Torture - A Commentary*: 745, paragraph 19.
49 UN General Assembly, *Optional Protocol to the Convention Against Torture*: Article 4.
50 Ibid; See also UN High Commissioner for Refugees, *Guidelines on the Applicable Criteria and Standards relating to the Detention of Asylum-Seekers and Alternatives to Detention*, 2012: paragraph 5, available at https://www.refworld.org/docid/503489533b8.html; University of Bristol Human Rights Law Clinic, *'Deprivation of liberty' as per Article 4 of OPCAT: the scope*, October 2011, available at http://www.bris.ac.uk/media-library/sites/law/migrated/documents/deprivationofliberty.pdf
51 Nowak et al, *Convention Against Torture - A Commentary*: page 745.
52 Ibid: 747-8.
53 Association for the Prevention of Torture, *Optional Protocol to the UN Convention against Torture: Implementation Manual*, 2010 (revised edition): 50, available at https://www.apt.ch/sites/default/files/publications/opcat-manual-english-revised2010.pdf; See also Nowak et al, *Convention Against Torture - A Commentary*: 747-8; and, Antenor Hallo de Wolf, "Visits to Less Traditional Places of Detention: Challenges under the OPCAT," *Essex Human Rights Review*, 6.1 (2009): 73–97, 75.
54 That approach differs radically from 'traditional' international human rights treaties, whose modus operandi is based on a more classical cycle of reporting to UN treaty bodies and implementation of recommendations formulated by the treaty bodies.
55 Association for the Prevention of Torture, *Implementation Manual*: 22–23.
56 See further the "Membership" section of the website of the Subcommittee on Prevention of Torture, available at https://www.ohchr.org/en/treaty-bodies/spt/membership
57 UN General Assembly, *Optional Protocol to the Convention Against Torture*: Article 11(1)(a).
58 Ibid: Article 4.
59 Technically speaking, OPCAT Articles 12(a) and 14(1)(c) in conjunction with Article 4 grant the SPT unrestricted access to all places of detention, within each State Party's jurisdiction and control, where persons are or may be deprived of their liberty.
60 Association for the Prevention of Torture, *Implementation Manual*: 26.
61 OPCAT explicitly recognizes the obligation of States parties to grant NPMs the right to have contact with the Subcommittee, to send it information and to meet with it, see UN General Assembly, *Optional Protocol to the Convention Against Torture*: Article 20 (f).
62 UN Office of the High Commissioner for Human Rights, *Preventing Torture: The role of national preventive mechanisms – A practical guide,* 2018: iii, available at https://www.ohchr.org/sites/default/files/Documents/Publications/NPM_Guide_EN.pdf
63 "National Preventive Mechanisms - Subcommittee on Prevention of Torture," *UN Office of the High Commissioner for Human Rights*, https://www.ohchr.org/en/treaty-bodies/spt/national-preventive-mechanisms
64 UN, *Preventing Torture: The role of national preventive mechanisms – A practical guide*: 13–36.
65 UN General Assembly, *Optional Protocol to the Convention Against Torture*: Article 24(2).

66 Correct as at 20 September 2022.
67 "List of designated NPMs by regions and countries," *Association for the Prevention of Torture*, http://www.apt.ch/en/knowledge-hub/opcat-database/list-designated-npm-regions-countries
68 For an early appreciation of this fact, see Murray, "National Preventive Mechanisms under the Optional Protocol to the Torture Convention: One Size Does Not Fit All".
69 UN General Assembly, *Optional Protocol to the Convention Against Torture*: Article 26 - States and other entities are encouraged to financially contribute to the OPCAT Special Fund to support national torture prevention activities world-wide. The Fund relies entirely on voluntary contributions; See also "Special Fund of the OPCAT - How the Fund is managed," *UN Office of the High Commissioner for Human Rights*, https://www.ohchr.org/en/about-us/funding-budget/trust-funds/the-special-fund-focus-torture-prevention/how-fund-managed
70 UN, *Preventing Torture: The role of national preventive mechanisms – A practical guide*: iv.
71 Ibid: 11.
72 Ibid.
73 All documents can be found on the website of the Subcommittee on Prevention of Torture, available at https://www.ohchr.org/en/treaty-bodies/spt
74 European Union, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation) (Text with EEA relevance)*; Council of Europe, *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* CETS No. 223, Strasbourg, 10.X.2018.
75 Though it should be remembered that OPCAT also applies to private actors in some circumstances.
76 UN General Assembly, *Convention on the Rights of Persons with Disabilities: resolution / adopted by the General Assembly*, 24 January 2007, A/RES/61/106: Article 33, available at https://www.refworld.org/docid/45f973632.html
77 UN General Assembly, *International Convention for the Protection of All Persons from Enforced Disappearance*, 20 December 2006: Article 28, available at https://www.refworld.org/docid/47fdfaeb0.html
78 Such as OPCAT.

References

Books

Lagoutte, Stéphanie, Sébastien Lorion, and Steven L. B. Jensen, eds. *The domestic institutionalisation of human rights*. Abingdon: Routledge, 2021.

Murray, Rachel et al. *The Optional Protocol to the UN Convention Against Torture*. Oxford: Oxford University Press, 2011.

Nowak, Manfred, Moritz Birk, and Giuliana Monina, eds. *The United Nations Convention Against Torture and Its Optional Protocol – A Commentary*, 2nd ed. Oxford: Oxford University Press, 2019.

Journal and newspaper articles

Bauman, Zygmunt et al. "After Snowden: Rethinking the impact of surveillance." *International political sociology* 8.2 (2014): 121.

Delaplace, Edouard, and Matt Pollard. "Visits by human rights mechanisms as a means of greater protection for persons deprived of their liberty." *International Review of the Red Cross* 87.857 (2005): 69.

Diggelmann, Oliver, and Maria Nicole Cleis. "How the right to privacy became a human right." *Human Rights Law Review* 14.3 (2014): 441.

Evans, Malcolm D., and Claudine Haenni-Dale. "Preventing Torture? The Development of the Optional Protocol to the UN Convention Against Torture." *Human Rights Law Review* 4 (2004): 19.

Hallo de Wolf, Antenor. "Visits to Less Traditional Places of Detention: Challenges under the OPCAT." *Essex Human Rights Review* 6.1 (2009): 73.

Lorion, Sébastien. "A Model for National Human Rights Systems? New Governance and the Convention on the Rights of Persons with Disabilities." *Nordic Journal of Human Rights* 37.3 (2019): 234.

Murray, Rachel. "National Preventive Mechanisms under the Optional Protocol to the Torture Convention: One Size Does Not Fit All." *Netherlands Quarterly of Human Rights* 26.4 (2008): 485.

Perlroth, Nicole, Jeff Larson, and Scott Shane. "NSA able to foil basic safeguards of privacy on web." *The New York Times* 5 (2013): 1.

Vedaschi, Arianna, and Valerio Lubello. "Data retention and its implications for the fundamental right to privacy: A European perspective." *Tilburg Law Review* 20.1 (2015): 14.

Websites and newspapers

Association for the Prevention of Torture. "List of designated NPMs by regions and countries." *Association for the Prevention of Torture*. http://www.apt.ch/en/knowledge-hub/opcat-database/list-designated-npm-regions-countries

Association for the Prevention of Torture. "The OPCAT: Torture prevention in practice." *Association for the Prevention of Torture*. http://www.apt.ch/en/what-we-do/achievements/opcat-torture-prevention-practice

Association for the Prevention of Torture. "Torture prevention in practice." *Association for the Prevention of Torture*. http://www.apt.ch/en/what-we-do/achievements/opcat-torture-prevention-practice

UN Office of the High Commissioner for Human Rights. "National Preventive Mechanisms - Subcommittee on Prevention of Torture." *UN Office of the High Commissioner for Human Rights*. https://www.ohchr.org/en/treaty-bodies/spt/national-preventive-mechanisms

UN Office of the High Commissioner for Human Rights. "Special Fund of the OPCAT - How the Fund is managed." *UN Office of the High Commissioner for Human Rights*. https://www.ohchr.org/en/about-us/funding-budget/trust-funds/the-special-fund-focus-torture-prevention/how-fund-managed

International judgments, laws, reports, and speeches

Association for the Prevention of Torture. *Optional Protocol to the UN Convention against Torture: Implementation Manual*. 2010 (revised edition).

Council of Europe. *European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment*. 26 November 1987, ETS 126.

Council of Europe. *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*. 4 November 1950, ETS 5.

Council of Europe. *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. CETS No. 223, Strasbourg, 10.X.2018.

European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation) (Text with EEA relevance)*.

International Criminal Tribunal for the former Yugoslavia. *Prosecutor v. Radislav Krstic - Judgment*. August 2, 2001 (Krstic judgment).

Nowak, Manfred. "What did OPCAT add to the existing mechanisms in the fight against torture?" *Subcommittee on Prevention of Torture - 10th Anniversary of the OPCAT Celebration Event - Speeches*. 2016.

Organization of African Unity. *African Charter on Human and Peoples' Rights ("Banjul Charter")*. 27 June 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982).

Organization of American States. *American Convention on Human Rights ("Pact of San Jose") Costa Rica*. 22 November 1969.

The Economic and Social Council official records, Commission on Human Rights. *Report on the Fifty-Eighth Session*. 18 March - 25 April 2002, E/2002/23 E/CN.4/2002/200.

UN Committee Against Torture. *1st annual report of the Subcommittee on Prevention of Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*. 14 May 2008, CAT/C/40/2.

UN General Assembly. *Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*. 10 December 1984, United Nations, Treaty Series, vol. 1465, p. 85.

UN General Assembly. *Convention on the Rights of Persons with Disabilities: resolution/adopted by the General Assembly*. 24 January 2007, A/RES/61/106.

UN General Assembly. *International Convention for the Protection of All Persons from Enforced Disappearance*. 20 December 2006.

UN General Assembly. *International Covenant on Civil and Political Rights*. 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171.

UN General Assembly. *Optional Protocol to the Convention Against Torture and other Cruel, Inhuman and Degrading Treatment or Punishment*. 9 January 2003, A/RES/57/199.

UN General Assembly. *The right to privacy in the digital age - Report of the Office of the United Nations High Commissioner for Human Rights*. (A/HRC/27/37), 30 June 2014.

UN General Assembly. *Universal Declaration of Human Rights*. 10 December 1948, 217A (III).

UN General Assembly. *Vienna Declaration and Programme of Action*. 12 July 1993, A/CONF.157/2.

UN High Commissioner for Refugees. *Guidelines on the Applicable Criteria and Standards relating to the Detention of Asylum-Seekers and Alternatives to Detention*. 2012.

UN Human Rights Committee. *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*. 8 April 1988.

UN Office of the High Commissioner for Human Rights. *Preventing Torture: The role of national preventive mechanisms - A practical guide*. 2018.
UN Subcommittee on Prevention of Torture. *Analytical assessment tool for national preventive mechanisms*. CAT/OP/1/Rev.1, 25 January 2016.
UN Subcommittee on Prevention of Torture. *Report on the visit made by the Subcommittee on Prevention of Torture to Italy*. 23 September 2016, CAT/OP/ITA/1.
University of Bristol Human Rights Law Clinic. *'Deprivation of liberty' as per Article 4 of OPCAT: the scope*. October 2011.

Index

Note: *Italicized* and **bold** page numbers refer to figures and tables. Page numbers followed by "n" refer to notes.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com