



HAL
open science

The French Intelligence Act : “The French Surveillance State?”

Wanda Mastor

► **To cite this version:**

Wanda Mastor. The French Intelligence Act : “The French Surveillance State?”: A comparison with the USA PATRIOT Act and FREEDOM Act. *European Public Law*, 2017, vol.23 (n°4), pp.707-722. hal-03678119

HAL Id: hal-03678119

<https://hal.science/hal-03678119>

Submitted on 25 May 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Scrutiny

The French Intelligence Act: ‘The French Surveillance State?’

A Comparison with the USA PATRIOT Act and FREEDOM Act

Wanda MASTOR^{*}

Key words: Terrorism; Counterterrorism; State of emergency; Surveillance; Bulk data collection; Intelligence; PATRIOT Act; FREEDOM Act; Judicial review; Administrative authorization

1 INTRODUCTION

The Intelligence Act of 24 July 2015, judged mostly compatible with the Constitution by the Constitutional Council (*Conseil Constitutionnel*), has been dubbed the ‘French PATRIOT Act’ by its critics. The aim of this article is to dispel this comparison, along with the claim that France would authorize mass surveillance at the same time as the United States is set to prohibit it with the recent FREEDOM Act. The legislation, essential in principle, is nevertheless not exempt from criticism: opting for extremely broad and vague objectives, as well as ‘eliminating’ the issue of international surveillance and the choice of prior authorization by a non-jurisdictional authority are less than convincing. A focus on counterterrorism would have resulted in the involvement of a specialized judge, a more effective guarantee than a merely consultative opinion from yet another new independent administrative authority.

After all the violent attacks that France has undergone in the recent past, it is more than ever necessary to reaffirm the importance of the surveillance. Only the preventive and not repressive tools are convenient to fight against the jihadists who are not afraid of suicide mission.

^{*} Professor of Public Law, Director of the Center of Comparative Law, Director of the European School of Law, University of Toulouse Capitole. Email: w.mastor@free.fr

2 THE FRENCH SURVEILLANCE STATE

If the context was not so serious, the title of the New York Times editorial of 1 April 2015, *The French Surveillance State*, would be considered ironic, so reminiscent it is of the language used by French observers when a traumatized United States was adopting the anti-terrorist act. The author reminds us that Manuel Valls ‘has assured the nation that the bill is not a French Patriot Act’, furthermore contending that parliamentarians should not approve the bill until this surveillance is authorized by a judge, since it appears to concentrate all power in the office of the Prime Minister. There is obviously no question of giving credibility to this press article, any more than there is to the French media who, following adoption of the Intelligence Act on 24 July 2015,¹ and without necessarily making the effort to read either the law carefully, systematically compared it to American Acts, mostly claiming that it went further. But, well-informed or not, this media coverage is emblematic of a particular point of view. Just following the example of the parliamentary debates and early academic comments, journalists failed to move away from the dual approach to the anti-terrorism debate: the choice between security and freedom. Regardless of the language or style used, the issue seems trapped in an impasse, caricatured by the introduction of ideological arguments. There is the impression that in France the left promotes the expression of freedom and the right issues of security. In this respect, it is disappointing to note that during the parliamentary readings, our representatives did not avoid this Manicheistic vision of the world.² As far back as the bill’s general presentation, the Prime Minister warned against all the ‘fantasies’ surrounding surveillance, emphasizing from the outset that there are many safeguards, including prior authorization, oversight and the right to effective judicial review. Misconceptions, misinterpretations and confusion cloud a clear vision of the American laws, from the 2001 USA PATRIOT Act,³ to the USA FREEDOM Act,⁴ while the French Intelligence Act is received with doubts and fears. The decision of the *Conseil constitutionnel* failed to dispel this haze of uncertainty, and nor did the new independent administrative authority established by the Law. The composition of the Commission was announced by Presidential Decree of 1 October (JORF

¹ N°2015-912 of 24 July, Journal Officiel de la République Française n°0171 of 26 July 2015, at 12735.

² Perhaps more than any other legislation, the Intelligence Act raises the difficult question of balance between the respect for freedom and safeguarding public order. French people are divided into two camps: a pro-security camp and a pro-freedom camp, unaware of the reality of the threat.

³ *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*, Pub. L. 107–156.

⁴ *Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act*, Pub. L. 114–123.

no. 0228 of 2 October 2015, page 17882).⁵ Pursuant to the organic law on the nomination of the President of the *Commission nationale de contrôle des techniques de renseignement* (National Commission for the Control of Intelligence Techniques⁶), validated by the *Conseil constitutionnel*,⁷ nomination of the Commission President by the President of the Republic has been confirmed by the relevant Standing Committees of each assembly.

The Law may be criticized for the content, even for its omissions, but the claim that it is a French clone of the US PATRIOT Act must be vigorously – and scientifically – rejected. This criticism, which has received ample coverage in parts of the media, was also a focal point of some of the speeches made by our parliamentary representatives (from the first day of debates⁸ to the last⁹). That opponents regret the bill was adopted at the same time the United States were reconsidering – in reaction to the Edward Snowden revelations – reigning in the most contentious provisions of the PATRIOT Act is one thing. But comparing it to the latter is another matter altogether. The fact it was the Socialists that brought forward and supported the bill did not reassure many parliamentarians, voters, left-wing supporters or civil liberties organizations. Deep misgivings were expressed by the French data protection authority, the *Commission nationale de l'informatique et des libertés*¹⁰ (CNIL), by the Defender of Rights,¹¹ by the National Assembly Committee on Rights and Freedoms in the Digital Age and even by the UN Human Rights Committee.¹² The former considers that ‘the provisions will allow the implementation of broader and more intrusive surveillance measures than permitted by the current legal intelligence framework’; the second ‘regrets that the National Assembly debates did not result in a better balance between public security imperatives and the protection of rights and freedoms’. The United Nations Committee stated, just a few hours before the decision of the *Conseil*

⁵ Francis Delon (nominated by the Vice-President of the *Conseil D’Etat* (Council of State) is President of the *Commission nationale de contrôle des techniques de renseignement* (National Commission for the Control of Intelligence Techniques); Patrick Puges is appointed member of the Commission as technical expert specialized in electronic communications. Also appointed are Jacqueline de Guillenchmidt (by the Vice-President of the *Conseil d’Etat*; Franck Terrier and Christine Penichon (jointly by the First President and the Attorney General of the Court of Cassation; Pascal Popelin and Catherine Vautrin (by the National Assembly); Michel Boutant and Catherine Troendle (by the Senate).

⁶ N°2015-911 du 24 juillet 2015, JORF n°0171 of 26 July 2015, at 12735.

⁷ Decision n°2015-714 of 23 July 2015.

⁸ ‘This text closely resembles a French PATRIOT Act, whatever the government claims to the contrary, and even if we do not go as far as the Americans’. National Assembly, Hervé Morin, session of Monday 13 Apr. 2015.

⁹ ‘The Intelligence Bill, despite all the denials, is clearly the PATRIOT Act 14 years on’, National Assembly, Jean-Jacques Candelier, session of Wednesday 24 June 2015.

¹⁰ Deliberation no. 2015-078 of 5 Mar. 2015 concerning an opinion on the intelligence bill.

¹¹ Opinion no. 15-09 of 29 Apr. 2015.

¹² Observations of 21 July 2015-CCPR/C/SR.3193.

constitutionnel, that the text ‘grants excessively broad and intrusive surveillance powers to intelligence agencies’.

Seeking balance, reconciliation, and respect for the lack of disproportionality are central to the deliberative actions of the executive, legislature and judiciary. These are delicate operations where the notion of threshold, even if not explicitly acknowledged, is omnipresent. To what extent can freedoms be curtailed for a higher interest? When does the just cause allowing these restrictions become unlawful? At what precise point does the preventive phase of intelligence seeking give way to the investigative stage and judicial process? What is the criteria for an emergency to become an ‘absolute’ emergency? Perhaps more than any other legislation, the Intelligence Act raises the difficult question of balance between the respect for freedom and safeguarding public order.

In the summer of 2016, after the terrible attacks of Nice and Saint-Etienne of Rouvray, this question arises more than ever and divides not only the political class but also the French people.

No one disputes that intercepting correspondence, collecting metadata and using algorithms, International Mobile Subscriber Identity- Catcher (IMSI-catcher) and spyware programmes infringe upon the right to privacy and freedom of communication. But neither does anyone question the need to combat terrorism in all its forms. The starting point is therefore to find a way out of the Manichean impasse explained above (*security vs freedom*) and address the concept that the French are divided into two camps: a pro-security camp, which as Article 1 of the French Internal Security Code (*Code de la sécurité intérieure*) states, is ‘a fundamental right and one of the conditions for the exercise of individual and collective freedom’, and a pro-freedom camp, unaware of the reality of the threat. Or to put it another way, the parliamentarians behind the referral to the *Conseil constitutionnel* explained that: ‘There is not one side determined to defend the Republic and another whose members are naïve or unpatriotic.’ Although the political community has generally highlighted the need for the principle of such legislation, which addresses the ‘shortcomings’, the ‘gaps’ and the ‘fragmented approach’ of the previous legal framework, to borrow words from the bill’s explanatory statement, the bill received a lukewarm welcome accompanied by fears and uncertainties.

To address such an extensive bill and the subsequent *Conseil constitutionnel* decision, the jurist must try to put aside all personal partisan, ideological and even philosophical opinions. She/He must try to avoid the classic divide, which inflames more than it informs the debate, by making his remarks laudatory and critical. Comparative law can eliminate any complacency in his argumentation – which would have the effect of minimizing the quality of our contribution (‘we are not going as far as the United States’) – and illustrate the similarities and divergences between the relevant laws to compare them most effectively. Adopting such a

methodological stance is particularly useful when reviewing three main points of the Law: the purpose of intelligence, the techniques used and oversight of implementation. In our view the Law is vital to combat a threat far more violent than the scope of the legislation, since it would totally take away our freedoms and not just infringe them. Thus we will primarily develop arguments which would have helped the law avoid the main criticisms aimed at it, often for legitimate reasons. For the three points we examined, there were alternatives to the provisions adopted, which we consider to be more appropriate.

3 THE PURPOSES OF INTELLIGENCE: MORE THAN JUST COUNTERTERRORISM

Before discussing the purposes of the recently adopted law, as set out in Article L 811-2 of the Internal Security Code which it amends, it is important to mention our main criticism. Restricting the scope to counterterrorism would have seemed more legitimate, as this is more urgent and specific. The majority of parliamentarians opposed to this first point, including the authors of the referral to the *Conseil constitutionnel* and those who participated in the debates, as well as bodies who issued an opinion prior to adoption, highlighted that the stated purposes are too broad, vague and unclear.

3.1 OPTING FOR A BROAD AND UNCLEAR SCOPE

As is convention, the Law begins by reminding us that ‘the public authority can undermine [the respect of privacy in all its forms] only in cases of necessity in the public interest provided for by law, within the limits fixed by it and in compliance with the principle of proportionality’. Then follows the list of cases justifying the infringement of freedom:

1. National independence, territorial integrity and national defense; 2. Major interests in foreign policy, performance of France’s European and international obligations and the prevention of all forms of foreign interference; 3. Major French economic, industrial and scientific interest; 4. Prevention of terrorism; 5. Prevention of: a) harm to the republican institutions; b) actions maintaining or reconstituting dissolved groups (...); c) collective violence likely to cause serious harm to the public peace; 6. Prevention of crime and organised crime; 7. Prevention of the proliferation of weapons of mass destruction.

There were good arguments for restricting this list. Firstly, the lack of clarity, which was also obvious to the authors of the referral to the *Conseil constitutionnel*, who emphasized the ‘loose semantics’, and wording so ‘vague’ that the guarantee of rights becomes ‘illusory’. It is difficult to precisely define what constitutes harm to the republican institutions, just as it is difficult to deny the over-inclusive nature of ‘collective violence likely to cause serious harm to the public peace’.

While the proponents of the Law defend themselves against the charge they were responding to current events – hence the accelerated parliamentary procedure – following the terrorist attacks on French soil, it is obvious that these attacks were one of the main driving forces behind the parliamentary work. It is nevertheless important to point out that the author of the substantial report for the National Assembly's Law Commission, Jean-Jacques Urvoas, was interested in the issue of intelligence and was determined to clarify the opaque situation before the so-called Charlie Hebdo and Hyper-Cacher attacks. But instead of basing the argument on the Law not having an exclusive focus on counterterrorism, and while maintaining the commitment to a clear legal framework for the work of the intelligence services, it would have perhaps been more appropriate to restrict the scope for a second reason: lessons drawn from the US experience.

3.2 LEARNING FROM THE US EXPERIENCE

When the PATRIOT Act, with its well thought-out acronym, was voted in the wake of the attacks of 11 September, foreign observers – including the author of this article¹³ – expressed outrage at the threats to freedom.

The sheer scale of this unprecedented event would serve to justify the war George W. Bush intended to wage against the 'Axis of Evil':¹⁴ on 14 September he declared a state of national emergency and signed a decree calling the reserve forces to active duty. In the days that followed, a 300 page act was adopted by a resounding majority, which in particular amended the 1978 Foreign Intelligence Surveillance Act – FISA. The provisions of the USA PATRIOT Act conflict with both substantive and procedural rights. In general terms, new surveillance tools were created; and communication interception measures, previously restricted for use in exceptional circumstances, were to become widespread. In total, six Amendments of the Constitution are undermined by the counterterrorist measures. In the interests of our argument, we should single out former section 802, which set out a particularly wide definition of the scope of the Act via the definition of terrorist activity. The notion of 'Domestic Terrorism' was linked to all activity which put lives in danger within the US territorial jurisdiction and was 'intended to intimidate the civilian population or affect the conduct of a government by mass destruction, assassination or kidnapping'. The vagueness of such a definition has the drawback of encompassing activity unrelated to terrorism in the conventional sense. This ambiguous wording, which was undoubtedly intentional,

¹³ *The State of Emergency in the United States: The USA PATRIOT Act and Other 'Legitimate' Violations of the Constitution*, XXIV *Annuaire International de Justice constitutionnelle* 461–475 (2008).

¹⁴ State of the Union Address, 29 Dec. 2002.

has inevitably led to abuses in practice. Because of the language used, this supposedly specific provision could also be used in the framework of criminal law cases, and indeed it has been. Through a broad interpretation, all political protest could thus be considered ‘domestic terrorism’, whereas the First Amendment prohibits Congress from adopting laws ‘abridging the freedom of speech’. According to civil liberties organizations, in particular the powerful American Civil Liberties Union (ACLU), the FBI has overused the possibilities offered by section 802, without restricting it to cases of terrorism.

The grounds for fearing such a large definition of the scope of the French law are thus based on lessons from comparative law. And it would be naïve to respond that French intelligence services are not the FBI: even in France potentially dangerous provisions could one day elude the good intentions of its creators.¹⁵

4 INTELLIGENCE TECHNIQUES: SHOULD WE BE AFRAID OF MASS SURVEILLANCE?

The Interior Security Code now has a title V: ‘Intelligence Gathering Techniques Subject to Authorization’, used by the services to be appointed by decree of the *Conseil d’Etat* (Article L 811-2). It should be noted that Article L 821-7 excludes parliamentarians, magistrates, lawyers and journalists from being subject to intelligence activities. When the *Conseil constitutionnel* was asked to rule on the absence of lecturers-researchers from the list, it replied with the technical guidance of why? Because: ‘Considering (...) that the principle of lecturer-researcher independence does not imply that university professors and lecturers should benefit from special protection in the event of the implementation of intelligence gathering mechanisms conducted by the administrative police’ (recital 36). The public will have to accept this ‘motivation’, but it is worth noting that tenures and regulated professions exist for the important contribution they make to public debate. Professors do not lecture in restricted and secret closed sessions. Amphitheatres, as do lectures and conference speeches, make professors key players in transferring knowledge and shaping public opinion. Moreover, these professors were the experts the public authorities sought out to talk about integration in prefectures and laicity¹⁶ in schools, to train some Imams and develop university degree courses on religions. A comparative constitutional law researcher has to use search engines which could

¹⁵ This is one of the arguments in the reply submitted by the members of parliament behind the referral to the *Conseil constitutionnel*: ‘Nothing would be worse than the introduction, through a text whose aim is to combat terrorism, of algorithmic governance into the very heart of our democracy; everyone should be concerned about the risk that it one day eludes its developers.’

¹⁶ The principle of secularism is one of the major principles recognized by the French Republic. It means the separation of the Church and the State and more generally, the religious neutrality of the Republic.

now be regarded as 'suspicious'. It stands to reason that a counterterrorism expert browses those web sites where he will find information on the many diverse aspects his research requires.

4.1 SOPHISTICATED TECHNIQUES

These can be described more specifically as security interceptions (Article L. 852-1.-I), sound recordings in some places and vehicles, and image and computer data capture (Article L. 853-1.-I). On a wider scale it further includes the gathering of information and documents relating to electronic communication from operators and internet hosting providers (Articles L. 851-1 and L. 851-2). Article 5 of the Law adds Articles L851-1, L851-2, L851-3 et seq. to the Internal Security Code, which allow the gathering of what is referred to as 'metadata'. For critics of the Law, this is even more of an infringement on freedoms than the data itself. In short, it is not only the content of an email that is intercepted, but all the relative information too: the address, time, etc. Gathering metadata is in fact no more or no less intrusive than collecting the data itself, since it is difficult to separate the two. Furthermore, Article L 851-3 allows the installation of the infamous 'black boxes' which use algorithms (Article L. 851-3.-I), and Article L. 851-6-I permits the use of IMSI catchers, which are fake relay transmitters which intercept telephone conversations (Article L. 851-6.-I). Telephones in the vicinity of the target are obviously likely to connect to this 'decoy tower'. Citizens will be hard pressed to find explanations of these modern and sophisticated techniques. Black boxes were singled out for criticism during the parliamentary debates, with opponents arguing they would result in mass surveillance. This issue will be examined below, but opponents of the Law are confusing mass surveillance and bulk information gathering. Black boxes use the information flowing through electronic infrastructure to track terrorists, as well as their support structure, among the mass of internet users. In more technical language, the intelligence services can identify individuals who are concealed among the mass of internet users by analysing indiscriminately all internet traffic carried by operators. The parliamentarians who referred the bill to the *Conseil constitutionnel* pointed out that not only is such a technique unconstitutional in terms of the principle of proportionality, but that it is also inefficient. According to a number of experts quoted by the applicants, this practice gives rise to too many 'false-positives', in other words a high percentage of false suspects. This argument is well demonstrated by the example used earlier in this article of the comparative researcher who, for research purposes, regularly consults web sites considered suspicious.

Article L. 854-1 of the Internal Security Code initially also contained international surveillance techniques the French authorities would have been empowered to use for communications sent or received outside national territory. Everyone knows, or can well imagine, the importance of such surveillance in the fight against terrorism. This type of surveillance is still allowed under the current FREEDOM Act, which did not amend section 702 of the FISA. It still authorizes the National Security Agency – NSA – to eavesdrop communications entering or leaving US territory. Civil liberties organizations had hoped that the new intelligence act would repeal this provision, which expires at the end of 2017. These measures are particularly sensitive: contrary to the legislation for national surveillance, the French Law refers the conditions for the deployment of intelligence techniques to a decree by the *Conseil d'Etat*. The *Conseil constitutionnel* very logically struck down this provision, and the argument sometimes put forward that the public authorities would have worked with maximum urgency – that we moreover reject – does seem appropriate here. We find it quite simply incomprehensible that the definition of the operating conditions, conservation and destruction of the collected information, traceability and review by the Commission could have been decided by a simple decree in *Conseil d'Etat*. Lawmakers reacted rapidly by proposing a new text, which was recently adopted by the National Assembly at first reading (Draft Bill Regarding Surveillance Measures of International Electronic Communications), which totally integrates international surveillance, with no referral to a decree in the *Conseil d'Etat*.

The length of time this data and metadata can be retained has also been a key issue during preparatory work on the bill. As we will see later, their collection is under the authority of the Prime Minister who ‘organizes the traceability of execution of authorized intelligence techniques (...) and sets the terms of the centralisation of the collected information’ (Article L. 822-1 paragraph 2). In practice when an intelligence gathering measure is deployed there is a record of the start and end dates, together with the nature of the intelligence collected. The draft bill initially provided for the destruction of the collected data within a year from their collection, reduced to one month for security interceptions, and extended to five years for connection data. The work of the parliament on this issue was important, and time limits finally begin, not from the date of the collection of the information, but from the moment it is used. The limits will be thirty days for intercepted correspondence and conversation, ninety days for intelligence gathered from sound recordings, video images and data capture and five years for data connection.

During parliamentary discussions, it was often claimed that France was legalizing mass surveillance at the same time as the United States was prohibiting it. This is not only inaccurate, but also untrue.

4.2 MASS SURVEILLANCE OR BULK DATA COLLECTION?

Mass surveillance is not permitted under the FREEDOM Act and the French Intelligence Act, but they do provide for bulk data collection. The subtlety lies in how the data collected is used upstream by the various operators. But the authorities, whether it be the FBI and the NSA in the United States or the Prime Minister in France, will now only have access to this data if a targeted request has been made, and surrounded by a number of safeguards (authorization by a judge or an authority).

‘Adoption of the draft bill will contribute to advancing the rule of law. The text does not introduce mass surveillance of any kind. Indeed it even proposes the exact opposite as it only foresees targeted surveillance’, stated Philippe Bas, the Senate rapporteur for the Joint Parliamentary Committee (Senate, session of 23 June 2015). The Interior Minister strongly denied the introduction of mass surveillance: ‘I would like to state most emphatically that all the measures in the text, without exception, are based on targeted action, clearly demonstrated intention and never – and I mean never! – on mass surveillance (...). We are opposed to mass information gathering!’ Bernard Cazeneuve was obviously wanted to ward off Orwellian statements on the Intelligence Act. But it does indeed involve bulk collection, not by the office of the Prime Minister, but by intelligence operators. It is similar in the US, which banned the bulk collection carried out by the surveillance services.

Adopted and promulgated by President Obama very shortly before the French Intelligence Act, the FREEDOM Act was positively received for one simple reason: in both theory and in practice, it is nigh impossible for it to be more prejudicial to freedom than the 2001 Act. By 67 votes to 32, the Senate thus adopted an act limiting NSA surveillance powers, with the symbolism of the search for the acronym ‘FREEDOM’ just as significant as ‘PATRIOT’ in a different context. Although the United States is still engaged in a war on terrorism, according to repeated statements by the Executive, the recent Act was actually more motivated by the Edward Snowden revelations, (even if, unlike the French Law, the US Act did not legalize the status of whistle blower). The assertion that the 2015 Act repeals and replaces the 2001 Act is untrue. Certain provisions have expired and have been replaced rather than extended; while others have been extended. By using the powers conferred by the PATRIOT Act as a legal basis, the United States had put in place a generalized surveillance system.

Indeed, section 215 of the 2001 Act, entitled ‘Access to certain business records for foreign intelligence and international terrorism investigation’, authorized the government to obtain from a secret court (the FISA Court) an order to seize databases from a wide range of institutions, including libraries. Also known as

the 'Library Provision', government authorities were able to intrude into an individual's private sphere with remarkable ease: FBI agents could obtain a warrant to secure medical and financial records, electronic (SMS, emails) and telephone communications, information about videos rented and books borrowed from libraries. In addition, section 215 included a so-called 'Gag order', prohibiting disclosure of the use by the FBI of this section. Not only does this conflict with the Fourth Amendment of the Constitution, which protects the 'right of citizens to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures (...)', section 215 is also in breach of a series of laws protecting the confidentiality of library records, adopted following abuse by the FBI.

Moreover, it was only recently that a warrant was necessary: the Protect America Act of 5 August 2007, ironically called the Police America Act by ACLU, had modified the FISA by giving new powers to the NSA. This agency was authorized to carry out surveillance without a warrant on all communications sent from or entering the United States and it made ample use of this possibility. The New York Times of 16 December 2005 reported that thousands of cases of extrajudicial eavesdropping were carried out after the 11 September attacks. As a result of this abuse, the FISA was once again amended by the FISA Amendments Act of 10 July 2008, restoring the need for a warrant and making authorization by the FISA Court mandatory to eavesdrop on an American abroad, whereas previously, approval by the Attorney General was sufficient.

The President and US legislators were therefore clearly motivated by the commitment to limit the powers of the NSA. Telecommunications operators will now themselves collect their clients' metadata (see in particular Title 1 of the Act, 'FISA Business Records Reforms'). Hence, the FREEDOM Act has not signed the death knell for the collection of data which could then be handed to the FBI or the NSA, subject to prior authorization by the FISA Court and identification of a clear target. It is therefore the end of bulk data collection, including of internet connection data, but only for Americans.

From bulk collection to mass surveillance, US and French legislators sought to move away from straying into the latter domain though the fundamental issue of safeguards.

5 SAFEGUARDS: ADMINISTRATIVE AUTHORIZATION AND JUDICIAL REVIEW

The French jurist is not alone in being accustomed to the familiar argument relating to freedoms: 'if and only if'. Intelligence mechanisms which clearly infringe on private life in all its forms should be accompanied by a range of safeguards, some of which have already been discussed, such as the reason and

length of time information can be retained. ‘The parliamentary debates sometimes resembled a constitutional law tutorial class (‘Have you already read article 66¹⁷?’, ‘Do you know the difference between preventive control and repressive action?’ ‘What is the role of a public prosecutor?’) and also, unsurprisingly, focused on the issue of safeguards and their jurisdiction. The Law introduces a new independent administrative authority to guide the Prime minister’s actions. In addition it also gives jurisdiction to the *Conseil d’Etat* to receive any appeals at first and last instances. We were personally in favour of the law falling under the jurisdiction of a single judicial authority.

5.1 THE FRENCH CHOICE FOR THE DUO OF INDEPENDENT ADMINISTRATIVE AUTHORITY AND *CONSEIL D’ETAT*

The jurisdiction of the National Commission for the Control of Intelligence Techniques (*Commission nationale de contrôle des techniques de renseignement*, CNCTR) stems from an inevitable a priori syllogism: the aim of intelligence is notably to maintain public order; therefore it falls within the scope of the administrative police; therefore administrative authorities and administrative judges have competence. Opponents of this specific point of the Law make another syllogism: given its purpose and techniques used, the law is a particularly brutal infringement of individual freedoms; therefore it falls within the scope of Article 66 of the Constitution; therefore it comes under the jurisdiction of a judicial judge. The *Conseil constitutionnel* ruled in favour of the former position, noting that ‘the legislator used article 21 of the Constitution as the basis for entrusting the Prime Minister with responsibility to authorize the deployment of intelligence measures in the framework of the administrative police’ (recital 18).

Parliament has made the opinion of the CNCTR (which will comprise two members of the National Assembly, two senators, two members of the *Conseil d’Etat*, two senior ranking judges from the Cassation Court and a technical expert specialized in electronic communications) a safeguard of their deployment. However, opponents of the law have not failed tirelessly to raise the point that this prior opinion is only advisory. This did not ‘move’ the *Conseil constitutionnel*, which merely replied ‘that *in itself*, the prime ministerial authorization procedure, informed by the opinion of the National Commission for the Control of Intelligence Techniques, does not breach the right to respect of private life, nor the inviolability of the home or the secrecy of correspondence’ (recital 19, emphasis added).

¹⁷ The Art. 66 of the French Constitution: ‘No one shall be arbitrarily detained. The Judicial Authority, guardian of the freedom of the individual, shall ensure compliance with this principle in the conditions laid down by statute.’

Of course, the bill's advocates countered, just as tirelessly, that new Article L. 311-4-1 of the Administrative Justice Code conferred jurisdiction to the *Conseil d'Etat* to pass judgment on petitions concerning the use of intelligence techniques. Furthermore, any person wishing to check if they are or were subject to illegal surveillance or not can seek relief in the *Conseil d'Etat*, as can the CNCTR if it considers its advice or recommendations have not been followed up or that the actions taken were inadequate.

The argument of ex post judicial guarantee is undoubtedly legally admissible, but strategically very complicated. Recognizing that the case for the law's purposes outweighs the case for the extent to which freedoms are undermined – put another way, denying the judicial judge's jurisdiction – the merely optional nature of CNCTR advice is hard to accept. Beyond the logic and coherence of law, it casts strong and legitimate suspicion on the legislation: the most important say belongs to the Prime Minister. Pursuant to Article L. 821-1, intelligence gathering measures are subject to prior authorization from the Prime Minister, which is issued after receiving the opinion of the independent administrative authority. An unfavourable opinion must be reasoned, but it is not binding and does not necessarily affect the issuing of the authorization. On the other hand, the Commission can submit recommendations and seek assistance from the *Conseil d'Etat*.

In addition the Law provides that the Prime Minister does not need to request the opinion of the Commission 'in case of absolute emergency' (Article L. 821-5) – not to be confused with 'operational emergency' outlined in Article L. 821-6. An absolute emergency falls under the control of the *Conseil d'Etat*, with the CNCTR nevertheless 'informed without delay', and is restricted to the purpose of 'preventing serious breaches of public order'. It cannot involve the collection of data in real time on the networks of telecommunications operators or the controversial algorithms. These conditions meant that the *Conseil constitutionnel* did not strike down this emergency procedure, as requested by the parliamentarians in their application. Applicable in case of 'imminent threat' or 'extreme risk of not being able to carry out the operation later', the procedure for an operational emergency was even more derogatory than in the case of an absolute emergency, since it did not require authorization from the Prime Minister. Interestingly, it was not parliamentarians but the Prime Minister who requested that the *Conseil constitutionnel* review this procedure and, quite logically, the *Conseil* struck it down. With no procedural guarantee, in practice it handed excessive powers to the intelligence agencies, not least for the use of IMSI catchers,¹⁸ bringing 'a disproportionate breach of the right to respect of privacy and for the secrecy of correspondence' (recital 29).

¹⁸ *International Mobile Subscriber Identity*. It is an equipment of phone espionage used for the interception of the traffic of mobile telephony.

5.2 THE US CHOICE FOR A SPECIAL COURT

This decision to use a special court for security in the US predates the adoption of the FREEDOM Act, which seeks to increase the transparency of legal proceedings. The fact that overall we are favourable to the intervention of a judicial judge prior to all surveillance operations (and even if some members of parliament responded to this position with the retort ‘we don’t have time!’¹⁹), is not an issue here. In line with the disappointment we expressed earlier in this article that the law is not restricted to counterterrorist measures, we believe it is crucial to create a specific judge – which actually already exists – to prevent equally specific events in a changed world. This obviously does not imply a new and restrictive understanding of freedom, but a determined method of fighting terrorism in all its forms by including in this fight enhanced guarantees to protect freedoms. In our opinion, judicial protection is the strongest guarantee. In this field there is a line so fine between prevention and repression that the distinction between the administrative and judicial police²⁰ seems artificial to us. Acts of terrorism are autonomous offences punished with aggravated sentences (Article 421-1 of the Penal Code), regulated by a special procedural regime (centralized prosecution, investigation and trial by a court with specialized judges). The specific needs for a high level of specialization in this field were refined from 1986 to 2012 with each new step in the legislative process to suppress terrorism: specialization of the police and intelligence services, as well as the Parquet (the public prosecution service) with the establishment of the nationally competent counterterrorist section in the Parquet of Paris). Intelligence is not exempt from increasing specialization; on the contrary, an analysis of the methods for gathering intelligence reveal their sophistication. Thus it is a matter of serious concern that the 24 July Law only requires that one member of the independent administrative authority has technical competence, and this in a body supposed to be the custodian of freedoms. If the purposes of the law had not been so broad and unclear and had focused on counterterrorism, then the coherence would have enabled authorization by a judge specialized in intelligence matters and counterterrorism, rather than by a Commission. The argument raised during the parliamentary debates concerning response times (‘There is no time to call the prosecutor!’) is weak: how could an independent administrative authority composed of nine members, a number of whom have no experience in the matter, react more quickly and efficiently than a specialized judge? The current

¹⁹ Reply to Claude Goasguen by Jean-Yves le Drian, National Assembly, session of 13 Apr. 2015, <http://www.assemblee-nationale.fr/14/cri/2014-2015/20150212.asp>.

²⁰ In France, we distinguish the administrative police of the judicial police. The first one has for mission the research for public order, the second has for mission to pursue the authors of breaches. It is one of the foundations of the distinction enter the competence of the administrative judge and the judicial judge.

discussion about the ‘non-nomination’ of Jean-Marie Delarue, the President of the National Commission for the Control of Security Interceptions, demonstrates the need to raise, above all other contingency, such fundamental – and vital – issues for our nation.

As such, the issuing of authorizations for the use of such sophisticated and intrusive surveillance techniques should lie, not with the executive, but with a judge with this exclusive jurisdiction. Or at the very least within the jurisdiction of the executive, but after receiving authorization, and not just an opinion, from this judge. This proposed model is clearly comparable to the surveillance warrant issued by the FISA Court in the United States. However, the FREEDOM Act will not succeed in overcoming – at least not for a while yet – the memories of recent events, which have not given this system a good reputation.

The FREEDOM Act attempts to introduce greater transparency into proceedings before the FISA Court (see in particular title IV, Foreign Intelligence Surveillance Court Reforms). Thus the Act establishes a panel of experts who will be heard by the Court on issues of rights and freedoms and new communication technologies. Furthermore, the main decisions of the Court will be pronounced in public, whereas previously, since its creation in 1978 following the Watergate crisis, proceedings were shrouded in secrecy. But while the principal of such a special court seems interesting to study with the view to developing something comparable or even duplicating, in practice it is a different matter. It will undoubtedly take some time for the FREEDOM Act’s new provisions concerning the FISA Court to shrug off the heavy burden of its secretive past, since the NSA carried out generalized surveillance without the normally required judicial warrant.

Practical application of the French Law will no doubt rapidly encounter difficulties. Do operators run the risk of being overwhelmed by the large amount of data collected? Will the police and intelligence services, often faced with emergencies, have the time to distinguish between a ‘regular’ and ‘absolute’ emergency? How will the Prime minister deal with the advice of the CNCTR? Does the *Conseil d’Etat* risk being inundated with paranoid applications? The final article of the Law states that the application of all provisions will be ‘reviewed by the Parliament within five years after entry into force’. The role of the researcher is not to be automatically critical of a law, but to shed light on any inaccurate comparisons and shortcomings. We remain unconvinced by the choice to adopt extremely broad and vague purposes, to jettison the issue of international surveillance and to use an independent administrative authority for prior authorization. But the role of the citizen is to wish and hope that the choices made by their representatives prove to be successful.

Unfortunately, the series of violent attacks which shook the world over the last two years, in particular France, invites in a certain form of pessimism. In

France, the debates on the extension of the state of emergency hid the necessity of strengthening the ways of the intelligence. Created by the law of 3 April 1955 for an initial time of twelve days, the state of emergency is in force since 14 November 2015 (the last continuation having been voted by the Parliament on 21 July 2016).

Definitively, the comparative law has to make us humble: the French comments often denounced the *PATRIOT Act* as being a temporary text which became definitive. It was an aberration for the defenders of the liberties. Today, in front of jihadist danger which does not last for days but for decades, the French people are confronted with the same reality and the state of emergency is not ready to be interrupted.

POSTSCRIPT

On 6 July 2017, the French parliament voted for the sixth continuation of the state of emergency (until 1 November), which should be the last one. The new president of the Republic, Emmanuel Macron, indeed announced that a new antiterrorist law would then be voted, with some dispositions regarding the state of emergency converting to *droit commun* i.e. ordinary law and not by exceptional provision. This 'normalization' of the exception is raising new controversies.