Data localization as contested and narrated security in the age of digital sovereignty: the case of Switzerland

Samuele Fratini, Francesca Musiani

Data Localization as Contested and Narrated Security in the Age of Digital Sovereignty: The Case of Switzerland

Samuele Fratini[1,2] and Francesca Musiani[3]

[1] Department of Philosophy, Sociology, Education and Applied Psychology, University of Padua, Piazza Capitaniato 3, 35139, Padua, Italy

[2] Institute of Media and Journalism (IMeG), Università della Svizzera Italiana, Via Buffi 13, 6900, Lugano, Switzerland

[3] Centre Internet et Société, Centre national de la recherche scientifique, 59-61 rue Pouchet, 75017 Paris, France

Published online first on June 18, 2024 in *Information, Communication and Society*. https://doi.org/10.1080/1369118X.2024.2362302

Abstract

The construction and effects on national boundaries have become central topics in public and academic debates on digital sovereignty. Both state and non-state actors increasingly consider jurisdictions and traditional governing structures as means to capture and regulate digital data flows. This article delves into the intricate phenomenon of "data localization", conceptualizing it as a socio-technical assemblage reflecting the evolving expectations surrounding Internet architecture and national boundaries. Interviewing the users of Threema – a Swiss secure messaging app – this study unravels data localization practices as a hybrid black box, intertwining technical changes, political discourses, socio-technical imaginaries, and shifting social norms. Drawing on the field of Science and Technology Studies, we mobilize the analytical tools of *controversy* and *discourse* to highlight data localization as a locus of political contestation in Switzerland, where imaginaries of national boundaries are often mobilized to symbolize security and reliability. The article provides three key contributions to the discourse on digital sovereignty, fragmentation, and governance. Firstly, it argues for the usefulness of Science and Technology Studies in understanding Internet governance, emphasizing the need for analyses grounded in specific socio-technical contexts. Secondly, it advocates for a social perspective on digital sovereignty, emphasizing user agency, social movements, and collective action as crucial factors shaping the governance of data flows. Lastly, the article sheds light on users resorting to state jurisdictions as a means to reinforce control over data flows, exploring the discursive mobilization of national boundaries in the digital public sphere.

Keywords

Data localization, Digital infrastructures, Digital sovereignty, Secure Messaging, Science and Technology Studies, Switzerland

Introduction

In recent times, digital technologies have become the focal point of intense public scrutiny, as a series of disruptive events has ushered in a techno-pessimist era (Badouard, 2017). The techno-optimism of the last decades seems replaced by diffuse concerns about total surveillance (Véliz, 2021), democratic erosion (Zuboff, 2018), and foreign intrusion (Wylie, 2019). This skepticism has paralleled the rise of the concept of digital sovereignty, which gained momentum in the aftermath of the Snowden scandal in 2013 (Pohle & Audenhove, 2017). Even Western states have undertaken measures to fortify their control over digital technologies and to foster the autonomy of their national infrastructures (Thumfart, 2021; Farrand & Carrapico, 2022), with one significant component of digital sovereignty strategies being data localization—whereby states seek to regulate digital data flows by mandating their storage within national borders. However, the dominant narrative surrounding the resurgence of the nation-state and the academic preoccupation with digital sovereignty have too often coalesced into a monolithic account of data localization, depicted as a global rush toward the extension of state power over digital infrastructures. Moreover, scholarly attention has predominantly centered on nation-states as the primary actors, resulting in an institutional, linear, and top-down interpretation of data localization requirements (Hummel et al., 2021).

This paper seeks to contribute to the advancement of a nuanced understanding of data localization, by delving into a socio-political context where both public and private actors mobilize imaginaries of national boundaries as guarantees of security and reliability: Switzerland. We focus our attention to the users of Threema, a Swiss messaging application, as a crucial lens through which to explore the diverse imaginaries, hopes, and expectations associated with data localization. Addressing a specific context allows us to make general assumptions about the relationship between users and data sovereignty practices.

Employing Snowball Sampling Methods (SSM) and semi-structured interviews, we engage with users to elicit their perspectives. The paper draws on the concepts of *controversy* and *discourse* to develop a 'situated' understanding of data localization, in its different dimensions. Firstly, the concept of controversy allows us to investigate the meanings that actors attach to digital technology and the practices through which they embed it in their everyday lives (Latour, 2005). Secondly, the concept of discourse highlights the interplay of material, linguistic, social, and institutional interactions through which data localization acquires meaning (Edwards, 1996). Users share competing imaginaries of the digital public sphere whose performative character has material effects on the structure of the digital architecture. We find that, while all our respondents are willing to exert their control over their data, not everyone resorts to state jurisdiction as a means to capture data flows. Those who reject *Swissness* as a guarantee of security and reliability tend to trust technical features such as encryption, decentralization, and the minimization of data collection.

By interrogating the interplay of digital sovereignty, data localization, and user perspectives, this research contributes to a deeper understanding of the complex dynamics shaping the digital world. This study suggests considering user agency, social movements-born

claims, and other forms of collective action as fully capable of influencing how digital sovereignty is defined and shaped in practice.

The article is organized as follows. The first two sections are dedicated to introducing the two concepts that will guide our analysis; they are followed by a section introducing Switzerland as the legal and (geo-)political context of the research, before delving into the presentation of the empirical investigation and its results. A final section acts both as a discussion and a conclusion/overture.

Making Sense of Technology-related Controversies

Since at least the creation of the World Wide Web, a growing body of work – grounded in the Science & Technology Studies (STS) tradition that examines infrastructures and explores its contact points with Internet and platform studies – seeks to analyze the digital architectures subtending our social life. Digital platforms and infrastructures share the same distinctive features: they are deeply embedded into society, are usually taken for granted, and are endowed with extensive temporal and spatial reach (Plantin et al., 2018). Internet operators have become so necessary to people's everyday lives that they gained a status of invisibility, at least in the most developed countries (Star & Ruhleder, 1996). The dichotomy between offline and online settings stops making sense (Floridi, 2015).

However, digital artifacts are also lively questioned in the public discourse, with different communities questioning the future(s) of the digital society and proposed concurring visions. STS scholarship has contributed new ways of thinking about the relationship between digital media and society (Balbi & Magaudda, 2018), understanding the technical and the social as mutually constitutive and digital media as imbricated with social structures in a "seamless web" (Hughes, 1986).

A research tradition known as "controversy mapping" (e.g., Latour, 2005; Marres, 2015) has taken as subject of study the so-called "socio-technical controversies", i.e. those debates and discussions that address particular sets of scientific and technical knowledge, often embedded in artifacts, that is not stabilized; this instability is due to the fact that, in order to reach social acceptability, decision-making (or both), actors need to address juridical, economic, ethical, political and social considerations as well as the technical ones. This body of research has explored how controversies are opportunities to study how different social groups build conflicting social worlds where notions of technology acquire different meanings, and how they are performative, as they shape both the construction of technological artifacts and their subsequent regulation (Callon et al., 2011; Venturini & Munk, 2021). When it comes to digital platforms, public controversies often originate from 'public shocks', i.e., those moments that highlight technological 'infrastructural inequalities and call it to account for its public implications' (Ananny & Gillespie, 2017). Public shocks have the effect of nullifying the ontological invisibility of digital infrastructures by putting them under public scrutiny.

In the last decade, an impactful series of public shocks contributed to this shift. The most prominent events are the 2013 Snowden revelations (Pohle & Audenhove, 2017; Snowden,

2019), the 2018 Cambridge Analytica Scandal (Bennett & Lyon, 2019; Wylie, 2019), and the 2020 Covid Pandemic (Lyon, 2021). As a result of these landmark moments, the prominent public perception of digital technologies is what Romain Badouard (2017) has defined as the 'disenchantment of the Internet': technologies as the primary instrument of total surveillance, foreign invasion, democratic erosion, and social turmoil. In the field of Internet Governance (IG), scholars have highlighted the salience of technology-related controversies for decision-making processes. In recognizing that 'governance is collectively enacted by the design of technology' (DeNardis & Musiani, 2016), digital-related disputes become significant at different levels. Firstly, via the 'turn to infrastructure' (Musiani et al., 2016), the cooptation of technology for political objectives unrelated to their original aim. Secondly, they affect the crafting and enacting of Internet-related policy (Epstein et al., 2016). Finally, controversies also affect the norms and standards underpinning the functioning of the Internet infrastructure (DeNardis, 2014).

This article analyzes the implications of a neo-statist imaginary in the social (re-)ordering of the cybersphere. To do so, we adopt as a case study a socio-technical assemblage (a heterogeneous system composed of elements that are both material and immaterial, both physical and textual; see Bellanova & Duez, 2012) that effectively embodies the expectations of the re-structuration of Internet architecture along national boundaries: data localization.

Data Localization as Discursive Support

Nation-states attach increasing importance to having digital critical resources and data under their direct control and/or stored in their jurisdiction (Fratini et al., 2024). Data localization is broadly defined as the set of provisions that specifically 'encumber the transfer of data across national borders' (Chander & Lê, 2015).

Illustrations of this phenomenon may be found, e.g., in the European Union's attempts to force Big Tech companies to store their data within EU boundaries. The largest data protection fine in EU history ($1.3 billion) was issued in May 2023 against Meta, and it was just about data transfer from the EU to the US[1]. On its hand, Russia has enforced the so-called 'Yarovaya' Law since 2016, mandating every Internet operator to record and store the data and metadata they collect within the territory of the Russian Federation, and make them available to public authorities upon request. Furthermore, the latest 2022 amendments to the Data Privacy Law introduced strict data localization laws with enhanced adequacy tests for cross-border data flows. Even several countries in the Anglosphere that have historically applied a loose approach to digital governance are now debating or enforcing the in-home storage of digital data. In Canada (Government of Canada, 2018) and Australia,[2] data localization laws are already enforced. In the UK,[3] stringent requirements for international data transfer are put in place. These initiatives can all be linked to the state's attempt to increase its control over critical digital infrastructures.

[1] See: https://www.nytimes.com/2023/05/22/business/meta-facebook-eu-privacy-fine.html.
[2] Available at: https://www.aspistrategist.org.au/a-sovereign-australian-government-data-framework/.
[3] An overview is available at. https://www.dataguidance.com/notes/uk-data-protection-overview.

Through the internalization of the data chain and strict export control policies, states aim to counter corporate and foreign influences over digital ICTs and to encode their sovereignty. Labeled as national digital security or self-determination (Bradford, 2023), the underlying principle is the perceived necessity for the state to regulate the otherwise chaotic digital environment and the frequent legal controversies on data ownership. The present work aims to analyze technical and geopolitical nuances in the understanding of this seemingly monolithic rush to internalization and fragmentation (Pohle, 2023). Indeed, data localization practices can be analyzed as hybrid black boxes, as the term usually subtends intricate and opaque combinations of technical and non-technical changes, competing political discourses, diverging socio-technical imaginaries, and shifting social norms and practices – debated, negotiated, and understood by a wider variety of social actors.

We adopt Edwards' concept of *discourse* (1996) to account for the understandings, imaginaries, and perceptions that expert and non-expert communities link with data localization. Discourses are:

> '[…] a way of knowledge, a background of assumptions and agreements about how reality is to be interpreted and expressed, supported by paradigmatic metaphors, techniques, and technologies and potentially embodied in social institutions' (Edwards, 1996: 34).

The distinctive value of discourses is their power to signify, i.e. to give meaning to the interplay of material, linguistic, social, and institutional interactions through which human 'knowledge is produced and reproduced'. According to Rao (2023), discourses that redefine the role of technology infrastructures have the power to steer and shape technological development to such an extent that they should be regarded as infrastructures themselves. Discourses materialize both in the form of regulatory structures and institutional bodies (Pohle et al., 2016) and in the contestation of existing political agendas and decision-making processes (Aspria et al., 2016). For the present purpose, data localization requirements are assumed as the central support to the whole digital neo-statist discourse.

Storing and securing data within national boundaries is not new in the Western history of Internet Governance (Goldsmith & Wu, 2008). Nevertheless, the data localization discourse is today growingly loaded with political expectations, and increasingly regarded as a 'panacea to many concerns' (De La Chapelle & Porciuncula, 2021). This is not only true in the case of authoritarian states, e.g. China and Russia, but a rising standard also supported by the EU and several countries of the Anglosphere. In this regard, adopting the concept of discourse instead of that of socio-technical imaginaries (Jasanoff & Kim, 2015) is useful to account for the supra-national scope of social expectations connected with data localization.

The rise of data localization requirements constitutes an alternative way of structuring the global Internet, which by nature tilts the infrastructurally inscribed power relationships toward a new centrality of state jurisdictions. This affects the geographical circulation of data, their legal regulation, and their economic patterns of profitability. This implies that data localization is a *locus* of political contestation, as it embodies a radical reconfiguration of existing power balances.

By understanding the controversy around data localization through the lens of discourse, we aim to make sense of data sovereignty from an STS perspective. While localization and internalization seem to represent a global tendency, it is interesting to enlarge the scope beyond state and corporate discourses. On the one hand, an institutional approach is unable, on its own, to account for complex technological developments and fails 'to sufficiently open up the black-box of technology' (Pinch, 2008). On the other hand, governance is a distributed process, and users – whose agency is visible, especially during controversies and contestations – can contest and negotiate regulatory processes (Epstein et al., 2016). This paper will focus on a socio-political context where imaginaries of national boundaries are mobilized by both public and private actors as a guarantee of security and reliability: Switzerland.

Creating Trustworthy Data Spaces in Switzerland: The Double Safe Haven Narrative

When it comes to digital sovereignty, a large majority of academic publications have addressed influential geopolitical actors, e.g. China, the EU, Russia, and the US, other state entities have been overlooked. We argue that comprehending the mechanisms underpinning the co-constitution of society and technology requires attention to sociologically relevant case studies, regardless of their geopolitical size. When it comes to the data localization discourse and its relation to how digital sovereignty is defined and implemented, Switzerland is a discreet but extremely fruitful analytical opportunity.

For the purpose of this article, the most relevant aspect of Switzerland is not the already enforced data localization laws[4], but rather the dominant narrative on data governance, which is deeply rooted at public as well as corporate levels. We call this peculiar discourse the *Double Safe Haven* narrative, as multiple Swiss public and private bodies rhetorically harness their third-party position concerning the US and the EU, which are identified as the two main actors to interact. The major strength of this narrative is that, while the Swiss identity is associated with qualities that are traditionally representative of the US (e.g. harnessing the economic value of data through loose regulatory policies) and the EU (e.g. digital regulation style based on fundamental values), Swiss entities can waive their autonomy from those two digital spheres at any time. This happens especially when US or EU authorities are publicly blamed for eroding privacy values, such as the signing of the US CLOUD Act and the EU's proposal on E-evidence. Historically speaking, Switzerland managed to harness neutrality and federalism (Bory & Zetti, 2022) to play key historical roles, e.g., in the establishment of the International Telegraph Union (Balbi et al., 2014).

[4] The most relevant provision concerning data localization in Switzerland is the Swiss Federal Ordinance to the Federal Act on Data Protection of 31 August 2022 (DPO), whose Annex 1 enlists all those countries providing adequate data protection levels. It represents an extension of data localization requirements compared to previous provisions, as data transfers to non-adequate countries is only permitted if data protection is safeguarded by other means, e.g., international treaties, or in extremely exceptional cases, e.g., overriding public interests. The adoption of this EU-like evaluation of privacy adequacy offers legal support to substantiate the Swiss privacy narrative.

Political authorities are aware of the ability of Switzerland to be perceived as a safe harbor. This is explicitly declared in the Swiss Digital Foreign Policy Strategy 2021-2024[5] published by the Federal Council:

'Thanks to its neutrality and good offices, Switzerland is able to build confidence. This makes it easier for Switzerland to position itself as a bridge-builder in difficult, fragmented environments, including in the digital space.'

In almost every relevant public document, the Swiss digital strategy is to carve out an 'open and safe' as well as 'trustworthy digital space' (Report from the DETEC and FDFA to the Federal Council, 2022) between the EU and the US. In the Swiss Digital Strategy,[6] efforts to 'position Switzerland as a host state in the digital space' are outlined as one of the main components of the Swiss Digital Sovereignty strategy. This objective is regarded as feasible by the members of Digital Switzerland, who agreed that 'Switzerland can play a special role in the field of data sovereignty due to its strengths in research and development and its role as a host country of major international organizations'.

On the other hand, the Double Safe Haven narrative is widely employed for commercial purposes. Several Swiss tech companies try to market their services and products by harnessing values of safety and security that are traditionally associated with Switzerland as a neutral and independent country. 'Precision, reliability, and discretion are typical Swiss characteristics, and as a true Swiss company, Threema lives these values every day' is what is claimed on Threema's website (fig. 1).

Fig.1 - Fig.2

References to Switzerland in Threema's official website.

Threema is a Swiss messaging application founded in 2012 and adopted by 11 million individual users and more than 7000 corporate and institutional users (Fratini, 2024). The company is almost exclusively spread in the German-speaking area of Europe, usually labeled as DACH[7]. Threema is currently adopted by the Swiss army, some Swiss Cantons and municipalities, some German cities and Länder, as well as by Olaf Scholz, the Chancellor of Germany, himself[8]. Although its adoption is limited, Threema is the largest European messaging application and is in open competition with other secure messaging platforms, with regard to Signal and Telegram. Especially to compete with the former, Threema constantly boasts its *Swissness* and the two proprietary data centers located in the Zurich area (fig. 2). On its website, Threema markets the high level of security it offers by claiming to be free from the

[5] Available at: https://www.eda.admin.ch/missions/mission-onu-geneve/en/home/news/publications.html/content/publikationen/en/eda/schweizer-aussenpolitik/Digitalaussenpolitik_2021-2024.
[6] Available at: https://digital.swiss/en/action-plan/measures/operational-work-streams-on-digital-sovereignty.
[7] Shorthand for Germany, Austria, Switzerland.
[8] Available at: https://www.faz.net/aktuell/wirtschaft/unternehmen/threema-was-russland-stoert-ueberzeugt-olaf-scholz-18248712.html.

US CLOUD Act, GDPR-compliant while being autonomous from EU authorities at the same time.

Another representative example is Proton, a provider of a wide variety of encrypted and secure services, such as mail communication, VPN, data cloud, calendar, and others. Although it is more diversely widespread than Threema, Proton does not give up the chance to market its Swissness. On its website[9], Proton affirms that:

'Proton is based in Switzerland. This means all user data is protected by strict Swiss privacy laws. We are a neutral and safe haven for your personal data, committed to defending your freedom.'

Also in this case, the Swiss territory is charged with expectations of technical and legal privacy and filled with political values of freedom. Switzerland's alterity is again expressed through the opposition to the US and the EU[10]:

'Switzerland, being outside of US and EU jurisdiction, has the advantage of being a neutral location. [...] In the US and EU, gag orders can be issued to prevent an individual from knowing they are being investigated or under surveillance'.

Two major aspects emerge from these public and corporate communications. Firstly, through constant resorting to neutrality, discretion, and safety, Swiss institutions attempt to reproduce traditional Swiss cultural constructs in the digital dimension. Swissness is conveyed through the commercialization of 'national historical narratives, symbols, and motifs' to the extent to which 'outdated views are perpetuated, [and] stereotypes are exacerbated' (Clarke, 2023). Secondly, employed metaphors suggest a spatial understanding of digital governance that brings to the utilization of offline geographical borders as a guarantee of a safe space. Swiss stereotypical values are digitally remediated[11] and geographically enclosed.

Yet, this narrative is complexified by how strategies have been implemented. While the creation of a Swiss National Cloud has been regarded as a milestone in the establishment of a Swiss trustworthy data space since 2020, the project was outsourced in 2022 to five big foreign providers, i.e., Alibaba, Amazon, IBM, Microsoft, and Oracle[12]. It happened despite the Swiss Federal Council pointing out the lack of transparency in those companies' decision-making structures[13]. This raised great concern, especially in the French-speaking Cantons. In Geneva, for example, a referendum on the constitutional introduction of the right to 'digital integrity' was held on June 18, 2023. Another example is offered by a quite famous episode where French police needed to obtain the email address of the founder of an anti-capitalist website called Paris-luttes.info. Even though ProtonMail is not subject to French or European jurisdiction, Swiss authorities forced the company to provide the required information upon request of

[9] Available at: https://proton.me.
[10] See: https://proton.me/blog/switzerland.
[11] By 'remediation', we mean the term used by Bolter & Grusin to indicate 'the formal logic by which new media refashion prior media forms' (1999: 273).
[12] Available at: https://www.republik.ch/2023/06/08/die-neue-cloud-des-bundes-oder-das-wolkenkuckucksheim.
[13] See: https://digitale-selbstbestimmung.swiss/wp-content/uploads/2022/05/Beilage-01-Bericht_EN-zu-BRA-UVEK-EDA.pdf.

Europol[14]. While the dominant narrative depicts Switzerland as a safe haven, history shows the relevance of existing power relationships, international obligations, and technological features in determining data flows.

The strength of the dominant narrative despite the existence of the aforementioned contradictions requires an in-depth analysis of the way the Swiss data localization discourse is perceived among average citizens and users.

Into the Wild: The Double Safe Haven Among Users

To understand technology as a social process means to account for the constellation of controversies, practices, and representations that contribute to its construction. While Swiss state and corporate actors seem to accept and reinforce the Double Safe Haven narrative, no academic contribution exists insofar as documenting the position of end users, regardless of their degree of technical expertise. Furthermore, a recent academic literature review of the data sovereignty concept showed that citizens, users, and consumers have received little attention compared with state and governmental entities (Hummel et al., 2021). The main related shortcoming is the impossibility of detecting negotiations, reappropriations, and rejection of the outlined narrative by users, understanding them as active agents of change in technological development. Consumption and utilization are to be understood as active processes of appropriation and redefinition of cultural products (e.g. Oudshoorn & Pinch, 2008) where users confer new meaning and attach new fears and expectations to technologies (Silverstone, 1994). Bypassing users reinforce the illusion that data localization practices are a monolithic driver of epochal change by excluding alternative understandings and narratives. This is detrimental to the academic debate and to an informed policy-making process.

To fill this gap, we decided to interview 17 users of Threema in the age group between 19 and 63 years (see Appendix for a full overview of informants). As previously observed, the company has been making intense use of the Swiss narrative to market its products and services. Addressing its users represents a good opportunity to follow the unfolding of the Double Safe Haven narrative 'into the wild', while it must be acknowledged that users of Threema may be inherently more conscious of data security than the average citizen. Furthermore, it also allows us to explore in detail a facet of the relationship between messaging applications and data sovereignty. While Threema is the selected application for internal communication in the Swiss army and the federal administration, other countries are now following the same trend. In France, for example, Prime Minister Élisabeth Borne requested all government employees to uninstall foreign communication apps (e.g., Signal, WhatsApp, and Telegram) in favor of a French application called Olvid by December 8, 2023[15]. Some branches of the German government are now using Threema, while the German army adopted the Matrix protocol[16], which is also relevant in France, where the government developed an in-house messaging

[14] See: https://www.vice.com/en/article/88njdg/protonmail-under-fire-for-sharing-clactivist-data-with-french-authorities.
[15] Available at: https://www.bleepingcomputer.com/news/security/french-government-recommends-against-using-foreign-chat-apps/.
[16] Available at: https://element.io/case-studies/bundeswehr.

system called Tchap in collaboration with Element[17]. Messaging applications have become a strategic control point for state authorities to exert their sovereignty over data flows. Yet, while several governments seem persuaded by data localization narratives, it remains to investigate the perceptions and values underlying users' adoption.

Participating users of Threema have been gathered through snowball sampling method (SSM). The core principle is '[...] identifying an initial set of relevant respondents, and then requesting that they suggest other potential subjects who share similar characteristics or who have relevance in some way to the object of study' (Tansey, 2007). Among the reasons to adopt this approach, we can claim it allows access to 'hard-to-reach or unknown populations when studying sensitive, controversial, and taboo topics' (Dosek, 2021), and this was the case, as we decided to address privacy-attentive users. Yet, SSM also has some weaknesses. Firstly, the sampling is non-probabilistic, thus not representative. Secondly, it tends to emphasize those actors with larger social networks, as they are more likely to be reached by researchers.

To overcome these limitations, we collected information about the most popular places of aggregation among Threema users in the digital space. Simply put, instead of relying on interviewees to reach other possible respondents, we drew on them to reach digital spaces where Threema is adopted. As previous contributions have shown, relying on social media and forums is effective in diversifying sources of information, offering an alternative channel to relevant actors, and thus bypassing powerful gatekeepers and including actors with less social ties (Dosek, 2021). Major places of aggregation where our informants have been found are the unofficial German-speaking 'Threema-Forum', Mastodon, Bluesky, and a Subreddit called 'Threema'.

We conducted 17 narrative semi-structured interviews in English and in German between October and December 2023. Through an immersive configuration, we aimed to delve into users' understanding and usage of Threema, while asking about their perceptions of surveillance and privacy topics. In particular, we investigated what main risks they relate to digital surveillance, how they consider underpinning dangers, and how they perceive nation-states in the clash between privacy and surveillance. Every informant was also asked about their perception of Threema's Swiss identity and their in-home data centers. Interviews have been held exclusively through calls with or without video.

In 14 cases, we used Threema itself as an interviewing platform. This allowed us to account for a broader geographical distribution of users and fostered more honest conversations (Mann & Stewart, 2000: 153) while preserving the advantages of synchronous interviews (Chen & Hinton, 1999). Furthermore, it was useful to gain access to the most privacy-attentive informants by adopting the messaging application we knew they rely on (O'Connor & Madge, 2017). Finally, we attempted to reach a fair balance regarding the overall distribution of Threema. As a result, 10 users reside in Germany and 14 of them in German-speaking countries.

[17] Available at: https://joinup.ec.europa.eu/collection/open-source-observatory-osor/document/french-government-launches-house-developed-messaging-service-tchap.

'It is important to be in a neutral country like Switzerland'

According to much of the aforementioned literature on data sovereignty, state entities demand the storage of data within their jurisdiction for security, economic, and geopolitical reasons. In the case of Threema, in-home data centers are clearly marketed as an advantage in terms of privacy, security, and reliability. Then, we interrogated users on this topic. Among 17 interviewees, 11 of them confirmed that in-home data centers and the Swiss identity counted as an advantage at the moment of choosing the application.

The most cited advantage of choosing a Swiss messaging application is often found in the historical Swiss neutrality and the Swiss privacy laws, which are regarded as 'inclined to safety'. It is also important to highlight the relevance of the Swiss banking system in constructing security perceptions. Several users equate financial services with data security. User 17 affirms to be 'pretty sure that Switzerland is very good at data protection' because 'Switzerland is known for bank security and anonymous… things'. According to User 10, Swissness and Swiss data centers count as the main reasons to choose Threema and, interestingly, he links the perception of safety with cultural representations of Switzerland among German people:

'But why did I decide to use Threema in the first place? Because it's from Switzerland. And German people always think that products from Switzerland are actually the best, especially in terms of security.'

Threema's attempt to connote its security expertise by continuously resorting to a Swiss cultural myth of 'discretion, precision, and reliability' is particularly effective among these users. Also User 8 accords a positive role to Swissness in his choice of using Threema, while he confirms the existence of a link between Switzerland and security as a cultural representation:

'And that led me to decide to use Threema because Switzerland has always been in fact inclined toward security and this kind of things'.[18]

In addition, he introduces a further theme that is extremely common in the vast majority of the interviews, i.e., the advantage of relying on non-American data centers:

'And in fact, it seemed to me that Threema's servers are not located in the USA, but rather in Europe. And since they are in Switzerland, this is even better!'[17]

We noticed that relative trust in EU and Swiss jurisdictions is present even among those libertarian users considering nation-states as inherently malicious. Nearly every interviewee has extremely negative opinions about how privacy is valued in the USA, despite his opinion on data localization. They put great significance on Threema's compliance with the GDPR and regard the Swiss jurisdiction just as safe as or safer than the EU's. User 4 got in touch with European governmental employees who prefer using Threema for professional communication instead of Signal because it is a European and GDPR-compliant application. User 3 reports that 'being based in Switzerland where you're outside the EU's jurisdiction is definitely important'

[18] These quotes have been translated from German.

especially when EU institutions debate about 'banning encryption' through Chat Control[19]. Yet, interviewees do sometimes recognize the relevance of 'emotional factors' in tying Switzerland and privacy. Just as User 1 admits:

'I would say it's an emotional factor. It's much easier to like something that is nearer from where you are. So a company that's based in Switzerland, whereas I live in Switzerland, for example, is just more attractive on an emotional level. From a technical standpoint, I don't think that there is any meaningful difference.'

These data seem to confirm the rising appreciation for data localization. Yet, there is a significant portion of users who do not consider Swiss identity and Swiss data centers as an advantage. It is interesting to understand how they counter the outlined narrative.

'You would be very stupid to trust anything just because it's from Switzerland'

There is a group of six users who do not consider Swissness and Swiss data centers as the main reasons behind their adoption of Threema. On average, they tend to be characterized by high technical and/or legal expertise and perceive that data flows are difficult to capture and control through state jurisdictions. They think that resorting to Swissness is just 'good marketing' (User 6). They seem to know what a threat model is and are aware that privacy and security must be implemented according to the targeted enemy and/or the projected adversary. In this regard, User 4 claims that laws and jurisdictions may represent protection only if you are not trying to shield yourself against intelligence agencies. Intelligence is often described as a field where the inter-state power balance cannot be changed through good policies:

'Switzerland is part of the intelligence community. So you can be fairly certain that they will cooperate with the people that they have cooperation with, which is, amongst others, the United States of America. So from that perspective, for me, it's the same: if I use Threema or if I use Signal, I'm fairly certain that if the Americans want to know who I talk to, they will know that.' (User 4)

While they reduce protection benefits connected with Switzerland, they tend to put their trust in the technical features of the application. User 6 invites not to 'rely on governments' to protect your privacy, but on 'the individual use of the right tools'. These users like Threema because of its end-to-end encryption and its data minimization approach. Above all, they appreciate that Threema does not require their phone number. In downsizing the relevance of nation-states, some of these users regard Signal as safe even though it is US-based, a country that is unanimously regarded as 'the most aggressive and punishing nation' regarding surveillance practices (User 16). User 6 states:

'You can see that Signal is a US application, it works on AWS Amazon Web Services, and that's not a problem because everything is protected on the layer and through end-to-end encryption of the content and the metadata. So, even if the data is going to the US, that's not a problem.'

Furthermore, while these users consider Threema's GDPR compliance as an advantage, they downsize the significance of being based in Switzerland when it comes to privacy and

[19] User 3 talks about a law enforcement proposal debated in the European Parliament the very same days the interview took place. If passed, the law would have allowed policing authorities to access private data to counter some criminal actions. This would have broken down end-to-end encryption.

security. In doing this, they often refer to Crypto AG[20], a Swiss company specialized in communication and information security working between 1952 and 2018. The company was harshly criticized for selling backdoored products to benefit American, British, and German signals intelligence agencies.

While they show a great appreciation for Threema, some of them think that the future of privacy is represented by decentralized and federated technology. In this regard, the Matrix protocol is sometimes cited as a good example of secure messaging:

'I think Matrix is the future in terms of that. I think decentralized networks are the future. They're also more robust and they're much harder to disrupt since they're not centralized. I mean, if we bombed the data centers where Threema has their servers [...] the whole service would go down. And since there are only ten servers, I mean, it's fairly easy to bomb them. You don't even have to be a nation-state for that. You could just be organized crime with a bunch of resources and people who don't care about law. Whereas if you take a decentralized network with Matrix, for example, you would have an endless amount of servers that you have to take down in order to actually take down the network. So I think the future for secure communication is decentralized [...].' (User 4)

Although not all these users could be defined as libertarians, they are united by the idea that any state authorities will, sooner or later, employ the information they have on private individuals for bad purposes. Therefore, relying on an application just for its citizenship is on average meaningless to them. User 15, for example, fears that collected personal data may be used to erode individual rights and harm democracy whereas the AFD[21] – or any other radical right-wing party – seized power in Germany. The most often cited solution is the radical reduction of data collection by corporations and governments.

Discussion and Conclusion

This article has argued that « data localization » — the set of measures that address the transfer of data across national borders — can be examined and understood as a socio-technical assemblage that embodies the expectations of the re-structuration of Internet architecture along national boundaries. Using the Swiss-based secure messaging application Threema as a case study, investigating the motivations behind user adoption of the tool, we have examined data localization practices as a hybrid black box of technical changes, competing political discourses, diverging socio-technical imaginaries, and shifting social norms and practices.

This article has sought to understand data localization through the double analytical tool of controversy and discourse. On one hand, it has analyzed localization as a *locus* of political contestation and examined how, in a context such as Switzerland where different actors mobilize imaginaries of national boundaries as a symbol and concrete embodiment of security and reliability, data localization comes to embody a set of reconfigurations of existing power balances around issues of digital sovereignty and Internet fragmentation. On the other hand, we

[20] A quick overview of the story is available here: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/.

[21] *Alternative Für Deutschland*, a German far-right party whose appreciation is rising, according to major survey agencies.

have shown how discourses on data localization give meaning to the interplay of material, linguistic, social, and institutional interactions through which data localization practices are (re-)produced. These reconfigurations of imaginaries and power balances take place not only around the technical features of the technologies and processes involved, but in a complex scenario including matters of legislation, of use (intended and sometimes unintended), of geopolitics, and even of morals and ethics, making the analytical lens of socio-technical controversy both appropriate and necessary. The prism of discourse, on its end, helps to flesh out the extent to which State-driven discourses about the alleged benefits of data localization in Switzerland clash and intersect with the standpoints of different involved actors – first and foremost, users – about what data localization does and does not do; furthermore, and perhaps more surprisingly, this analytical lens contributes to show how these discourses can be understood as becoming part of the infrastructure of data localization itself.

Beyond the specific case of Threema, Switzerland, and data localization practices, this article seeks to contribute three main points to current academic discussions of digital sovereignty, fragmentation, and governance.

First, this article seeks to emphasize, as a growing and recent body of literature does, the usefulness of STS-derived concepts and analytical tools to address oft-underexplored, yet central, dimensions of the study and the practice of Internet governance. In particular, we have leveraged here the study of socio-technical controversies as a powerful analytical tool to bring nuance to both technological innovation and governance strategies (see Musiani, 2020). While the extension of state authority over digital infrastructures is examined extensively today among both academic and non-academic publications, it is important to account for this complex process in a way that preserves nuance and accounts for its 'situated practices', grounded in socio-technical and geopolitical contexts (see e.g. Orlikowski, 2000). Conceptualizing this contestation of existing power relations as a socio-technical controversy permits to conduct in-depth analyses of the actors involved and confers renewed relevance to meanings attributed to, and encoded into, technology by different social groups.

This aspect is, indeed, directly related to the second point we wish to make in this conclusion. So far, a large majority of the existing literature attempts to understand data sovereignty from two main perspectives. The first perspective focuses on how institutional actors understand, enact, and contest digital sovereignty. A limited number of states and supra-national entities, most notably, China, Russia, the EU, and the US, have been traditionally adopted as the main unit of analysis to investigate data sovereignty (see e.g. Zeng et al., 2017; Litvinenko, 2021; Monsees & Lambach, 2022). A second, nascent approach emphasizes the materiality, the situatedness, and the embeddedness of data sovereignty: addressing corporations, producers, technologies themselves, and the nexus between the three, these approaches attempt to make sense of how data sovereignty strategies are infrastructured and materialized (see e.g. Möllers, 2021; Musiani, 2022).

While we recognize the usefulness and the centrality of both approaches – which, indeed, this very article also pays tribute to, and mobilizes – we wish to highlight here that a third entry point is necessary. As the return of the nation-state is, in many fields, an epochal

fact, future works should address the extent to which data sovereignty is, in many instances, a collective process. User agency, social movements-born claims, and other forms of collective action can usefully be operationalized as relevant *loci* where state sovereignty over data flows is reshaped and enacted. A nascent literature can be helpful in this regard, notably the body of work examining indigenous struggles for autonomy in contexts such as Canada or New Zealand, which have brought claims of data sovereignty (of marginalized groups) to the forefront (see respectively Couture et al., 2021; Kukutai & Taylor, 2016). The present article has shown that, beyond divergences in Swissness, almost every user is starkly willing to exert their personal control over produced data. When data sovereignty becomes a social request and claim, its collective manifestation should be considered of paramount importance in the restructuring of the digital sphere.

Finally, our article shows that, among the ways users try to reinforce their control over data flows, we can observe how some of them resort to state jurisdictions, both as an idea and a concrete embodiment of constraints and opportunities, as a guarantee of (digital) security. The discursive mobilization of national boundaries' imaginaries in the digital public sphere acquires great relevance, yet it is so far an understudied topic in academic literature, even in those works that set out to analyze nation-states' discursive constructions of the Internet and digital technologies (Haggart et al., 2021). Indeed, in today's age of predominant techno-pessimism, our respondents, as users of the Internet faced with the necessity of choice among the many communication applications it supports, seem to resort to traditional governing structures – those very structures whose suitability to the Internet had been questioned in the early days of the network of networks[22] – to contain the backlashes of digitalization. The fears, hopes, and expectations they have shared with us, and which constitute the empirical backbone of this article, ultimately contribute to the re-assembling of the state and its role in the digital sphere and suggest new directions for thinking about the practices and the infrastructures of digital and data sovereignty.

Disclosure Statement

The authors report there are no competing interests to declare.

Funding

Samuele Fratini is supported by a PhD scholarship of Università degli Studi di Padova. Francesca Musiani is supported by the French National Agency for Research by means of the DIGISOV grant ("Gouvernance numérique et souveraineté dans un monde fracturé : états concurrents et circulation des normes", 2024-2027, ANR-23-CE53-0009-02).

Ethical Considerations

The first author followed the ethical principles described by the ethical committee of the 'Università degli Studi di Padova'. To ensure the right to privacy, individuals have been

[22] See Pohle & Thiel, 2020 for a brief discussion of 'cyber-exceptionalism' as it relates to digital sovereignty.

anonymized, and interviewees signed consent forms that allowed for the use of all materials gathered.

Notes on Contributors

Samuele Fratini is a PhD student at the University of Padua and the Università della Svizzera Italiana (USI). His research interests sit at the intersection of Science & Technology Studies, Media Studies, and Internet Governance, with a special focus on the German-speaking area. Major covered topics include privacy, sovereignty, and surveillance.

Francesca Musiani is Associate Research Professor at the French National Center for Scientific Research (CNRS), co-founder and deputy director of its Center for Internet and Society (CIS). Her interdisciplinary research explores Internet infrastructures as instruments of governance.

References

Ananny, M., & Gillespie, T. (2017). Public Platforms: Beyond the Cycle of Shocks and Exceptions. *The Platform Society*, 22.

Aspria, M., de Mul, M., Adams, S., & Bal, R. (2016). Of Blooming Flowers and Multiple Sockets: The Role of Metaphors in the Politics of Infrastructural Work. *Science & Technology Studies*, 29(3), 68-87. https://doi.org/10.23987/sts.59196

Balbi, G., Fari, S., Richeri, G., Calvo, S. (2014) *Network Neutrality: Switzerland's role in the genesis of the Telegraph Union, 1855–1875*. Peter Lang Verlag

Balbi, G., & Magaudda, P. (2018). *A history of digital media: An intermedia and global perspective*. Routledge.

Badouard, R. (2017) *Le désenchantement de l'internet. Rumeur, propagande et désinformation*. FYP éditions.

Bellanova, R. & Duez, D. (2012). A Different View on the 'Making' of European Security: The EU Passenger Name Record System as a Socio-Technical Assemblage. *European Foreign Affairs Review*, 17: 109–124.

Bennett, C. J., & Lyon, D. (2019). Data-driven elections: Implications and challenges for democratic societies. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1433

Bradford, A. (2023). *Digital Empires: The Global Battle to Regulate Technology*. Oxford University Press.

Bolter, J.D., & Grusin, R. (1999). *Remediation: Understanding New Media*. The MIT Press.

Bory, P., & Zetti, D. (2022). *Digital Federalism: Information, Institutions, Infrastructures (1950–2000)*. Schwabe Verlag.

Callon, M., Lascoumes, P., Barthe, Y., & Burchell, G. (2011). *Acting in an uncertain world: An essay on technical democracy*. MIT Press.

Chander, A., & Lê, U.P. (2015). Data Nationalism. *Emory Law Journal*, 64(3), 677-739.

Chen, P., & Hinton, S.M. (1999). Realtime interviewing using the world wide web. *Sociological research online*, 4(3), 63-81. https://doi.org/10.5153/sro.308

Clarke, A. (2023). Reflecting on nation image and perceptions of nation brand: Scottish-themed pubs, bars and restaurants outside of Scotland. *Journal of Consumer Culture*, 0(0), 1-18. https://doi.org/10.1177/14695405231207601

De La Chapelle, B., & Porciuncula, L. (2021). *We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty*. Internet and Jurisdiction Policy Network.

DeNardis, L. (2014). *The global war for Internet governance*. Yale University Press.

Dosek, T. (2021). Snowball Sampling and Facebook: How Social Media Can Help Access Hard-to-Reach Populations. *Political Science & Politics*, 54(4), 651-655. https://doi.org/10.1017/S104909652100041X

Edwards, P. N. (1996). *The closed world: Computers and the politics of discourse in Cold War America*. The MIT Press.

Epstein, D., Katzenbach, C., & Musiani, F. (2016). Doing internet governance: Practices, controversies, infrastructures, and institutions. *Internet Policy Review*, *5*(3). https://doi.org/10.14763/2016.3.435

Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, 31(3), 435-453. https://doi.org/10.1080/09662839.2022.2102896

Floridi, L. (Ed.). (2015). *The Onlife Manifesto*. Springer International Publishing.

Fratini, S. (2024). Performing Privacy Culture. The Platform Threema and the Contestation of Surveillance Made in Switzerland. Studi Culturali, 21(1), 3–26.

Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models. SSRN Electronic Journal, 87. https://doi.org/10.2139/ssrn.4816020

Goldsmith, J. L., & Wu, T. (2008). *Who controls the Internet? Illusions of a borderless world*. Oxford University Press.

Government of Canada (2018) *Government of Canada White Paper: Data Sovereignty and Public Cloud*. Treasury Board of Canada Secretariat.

Haggart, B., Tusikov, N., & Scholte, J.A. (2021). *Power and Authority in Internet Governance: Return of the State?* Routledge.

Hughes, T. P. (1986). The Seamless Web: Technology, Science, Etcetera, Etcetera. *Social Studies of Science*, *16*(2), 281–292. https://doi.org/10.1177/0306312786016002004

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data Sovereignty: A Review. *Big Data & Society*, 8(1), 1-17. https://doi.org/10.1177/2053951720982012

Jasanoff, S., & Kim, S.-H. (2015). *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power*. University of Chicago Press.

Kukutai, T., & Taylor, J. (2016). *Indigenous data sovereignty: Toward an agenda*. ANU Press.

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford University Press.

Litvinenko, A. (2021). Re-Defining Borders Online: Russia's Strategic Narrative on Internet Sovereignty. *Media and Communication*, 9(4), 5-15. http://dx.doi.org/10.17169/refubium-32268

Lyon, D. (2021). *Pandemic surveillance*. Polity.

Mann, C., & Stewart, F. (2000). *Internet Communication and Qualitative Research: A Handbook for Researching Online*. SAGE Publications Ltd

Marres, N. (2015). Why Map Issues? On Controversy Analysis as a Digital Method. *Science, Technology, & Human Values*, *40*(5), 655–686. https://doi.org/10.1177/0162243915574602

Möllers, N. (2021). Making digital territory: Cybersecurity, techno-nationalism, and the moral boundaries of the state. *Science, Technology, & Human Values*, *46*(1), 112-138. https://doi.org/10.1177/0162243920904436

Monsees, L., & Lambach, D. (2022). Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity. *European Security*, 31(3), 377–394. https://doi.org/10.1080/09662839.2022.2101883

Musiani, F. (2020). Science and Technology Studies Approaches to Internet Governance: Controversies and Infrastructures as Internet Politics. In L. DeNardis, D. Cogburn, N. Levinson, & F. Musiani (Eds.) *Researching Internet Governance: Methods, Frameworks, Futures*, (pp. 85-104). The MIT Press.

Musiani, F. (2022). Infrastructuring digital sovereignty: a research agenda for an infrastructure-based sociology of digital self-determination practices. *Information, Communication & Society, 25*(6), 785-800. https://doi.org/10.1080/1369118X.2022.2049850

Musiani, F., Cogburn, D. L., DeNardis, L., & Levinson, N. S. (Eds.). (2016). *The turn to infrastructure in Internet governance*. Palgrave Macmillan.

O'Connor, H., & Madge, C. (2017). Online Interviewing. In N.G. Fielding, R.M. Lee, G. Blank (Eds.), *The SAGE Handbook of Online Research Methods*, (pp. 416-434). Sage Publication Ltd.

Orlikowski, W.J. (2000). Using technology and constituting structures: a practice lens for studying technology in organizations. *Organization Science*, *11*(4), 404–428. https://doi.org/10.1287/orsc.11.4.404.14600

Oudshoorn, N., & Pinch, T. (2008). User-Technology Relationships: Some Recent Developments. Cambridge. In E. Hackett, O. Amsterdamska, M. Lynch, & J. Wajcman (Eds.), *The Handbook of Science and Technology Studies*, (pp. 541-567). The MIT Press.

Pinch, T. (2008). Technology and institutions: living in a material world. *Theory and Society*, 37, 461-483. https://doi.org/10.1007/s11186-008-9069-x

Plantin, J.-C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2018). Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society*, *20*(1), 293–310. https://doi.org/10.1177/1461444816661553

Pohle, J., Hösle, M., & Kniep, R. (2016). Analysing internet policy as a field of struggle. *Internet Policy Review*, 5(3). https://doi.org/10.14763/2016.3.412

Pohle, J., & Audenhove, L. V. (2017). Post-Snowden Internet Policy: Between Public Outrage, Resistance and Policy Change. *Media and Communication*, *5*(1), 1–6. https://doi.org/10.17645/mac.v5i1.932

Pohle, J. & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4), 1-19. https://doi.org/10.14763/2020.4.1532

Pohle, J. (2023). Vom Mythos der Zersplitterung: Das globale Netz zwischen Zentralisierung und Pluralisierung. *WZB Mitteilungen*, 180, 11–14.

Report from the DETEC and FDFA to the Federal Council on 30 March 2022 (2022) *Creating trustworthy data spaces based on digital self-determination*. Digital Self-Determination Network.

Silverstone, R. (1994). *Television and Everyday Life*. Routledge

Snowden, E. (2019). *Permanent Record: A Memoir of a Reluctant Whistleblower*. Macmillan

Star, S. L., & Ruhleder, K. (1996). Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces. *Information Systems Research*, *7*(1), 111–134. https://doi.org/10.1287/isre.7.1.111

Tansey, O. (2007). Process Tracing and Elite Interviewing: A Case for NonProbability Sampling. *Political Science & Politics*, 40(4), 765–772. https://doi.org/10.1017/S1049096507071211

Thumfart, J. (2021). The COVID-Crisis as Catalyst for the Norm Development of Digital Sovereignty. Building Barriers or Improving Digital Policies?, In D. Hallinan, P. de Hert, & R. Leenes (Eds.), *Enforcing Rights in a Changing World: Computers Privacy Data Protection (CPDP)*, (pp. 1-44). Hart Publishing.

Véliz, C. (2021). *Privacy is power*. Melville House.

Venturini, T., & Munk, A.K. (2021). *Controversy Mapping: A Field Guide*. John Wiley & Sons

Wylie, C. (2019). *Mindf*ck: Inside Cambridge Analytica's Plot to Break the World*. Random House

Zeng, J., Stevens, T., & Chen, Y. (2017). China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty'. *Politics & Policy*, *45*(3), 432–464. https://doi.org/10.1111/polp.12202

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Public Affairs

Appendix

ID	Gender	Country	Swissness	Duration
User 1	Male	Austria	1	30 min.
User 2	Male	Germany	1	25 min.
User 3	Male	USA	1	25 min.
User 4	Male	Sweden	0	70 min.
User 5	Male	Germany	1	30 min.
User 6	Male	France	0	30 min.
User 7	Male	Switzerland	1	15 min.
User 8	Male	Germany	1	15 min.
User 9	Male	Germany	1	30 min.
User 10	Male	Germany	1	25 min.
User 11	Male	Germany	0	30 min.
User 12	Male	Germany	0	20 min.
User 13	Male	Austria	1	70 min.
User 14	Male	Germany	1	30 min.
User 15	Male	Germany	1	30 min.
User 16	Male	UK	0	60 min.
User 17	Male	Germany	1	30 Min.