COGITATIO

Media and Communication (ISSN: 2183–2439)
2017, Volume 5, Issue 1, Pages 17–28
DOI: 10.17645/mac.v5i1.821

Article

Intelligence Reform and the Snowden Paradox: The Case of France

Félix Tréguer

Center for International Studies and Research, Sciences Po, 75006 Paris, France; E-Mail: felix.treguer@sciencespo.fr

Submitted: 10 November 2016 | Accepted: 26 January 2017 | Published: 22 March 2017

Abstract
Taking France as a case study, this article reflects on the ongoing legalisation strategies pursued by liberal states as they seek to secure and expand the Internet surveillance programs of their domestic and foreign intelligence agencies. Following the path to legalisation prior and after the Snowden disclosures of 2013, the article shows how post-Snowden controversies helped mobilise advocacy groups against the extra judicial surveillance of Internet communications, a policy area which had hitherto been overlooked by French human rights groups. It also points to the dilemma that post-Snowden contention created for governments. On the one hand, the disclosures helped document the growing gap between the existing legal framework and actual surveillance practices, exposing them to litigation and thereby reinforcing the rationale for legalisation. On the other hand, they made such a legislative reform politically risky and unpredictable. In France, policy-makers navigated these constraints through a cautious mix of silence, denials, and securitisation. After the Paris attacks of January 2015 and a hasty deliberation in Parliament, the Intelligence Act was passed, making it the most extensive piece of legislation ever adopted in France to regulate secret state surveillance. The article concludes by pointing to the paradoxical effect of post-Snowden contention: French law now provides for clear rules authorising large-scale surveillance, to a degree of detail that was hard to imagine just a few years ago.

Keywords
contentious politics; intelligence; internet; securitisation; Snowden; surveillance

Issue
This article is part of the issue “Post-Snowden Internet Policy”, edited by Julia Pohle (WZB Berlin Social Science Center, Germany) and Leo Van Audenhove (Vrije Universiteit Brussel, Belgium).

1. Introduction

In January 2008, a meeting took place in the office of then President of France, Nicolas Sarkozy, at the Élysée Palace. In front of him sat Prime Minister François Fillon and the Director of the *Direction Générale de la Sécurité Extérieure* (DGSE, France’s foreign intelligence agency) Pierre Brochand, as well as a few of their staff.

Brochand had come with a plea. France, he explained, was on the verge of losing the Internet surveillance arms race. From the 1980’s on, French intelligence services had managed to develop top notch communications intelligence (COMINT) capabilities, thanks to a network of intercept stations located across metropolitan France and overseas territories, sometimes in partnership with the German *Bundesnachrichtendienst*, or BND. But as almost all of the world’s communications were now travelling on IP based networks, the DGSE was losing ground on its main partners and competitors—in particular the National Security Agency (NSA) and the British Government Communications Headquarters (GCHQ)

France had some serious catching up to do, but it also had important assets. First, its geographic location, with almost two dozen submarine cables landing on its shores, both in Brittany, Normandy and the Marseilles area. Second, its engineering elite state schools and high tech firms—not least of which submarine cable operators Alcatel and Orange as well as surveillance technology provider Qosmos—, which could provide the technical know-how necessary to carry on this ambitious project.

Sarkozy was hesitant at first. The plan was very costly and its legality more than dubious. The French legal basis for communications surveillance dated back to 1991. Another issue was that of cost. At the time, the 2008 fi-

nancial crisis had yet to unleash, but the government was already facing recurring deficits and it needed to contain public spending.

But Pierre Brochand and its supporters in the President's staff turned out to be convincing. Sarkozy eventually agreed to move forward with the proposed plan: Over the course of the next five years, the DGSE would get the €700 million it needed to upgrade its surveillance capabilities and hire over 600 staff to work in its Technical Directorate (the number of DGSE employees was then 4,440). Only six months later, near Marseilles, the first of the new intercept stations was up and running, doubling up the traffic coming from international cables, filtering it and transmitting it to the DGSE's headquarters in Paris.

How do we even know about this meeting? We owe this account to journalist Vincent Jauvert, who revealed its existence in a French weekly magazine on July 1st 2015, at the very end of the parliamentary debate on the 2015 Intelligence Bill (Jauvert, 2015). According to former high ranking officials quoted by Jauvert, these efforts paid off: "When we turned on the faucet, it was a shock! All this information, it was unbelievable!" All of sudden, France was back in the game. To such an extent that, a few months later, in 2009, the NSA even offered to make the DGSE a member of the exclusive Five Eyes club.

Apparently, the "Sixth Eye" deal failed over the Central Intelligence Agency's (CIA) refusal to conclude a no-spy agreement with France, and in 2011, a more modest cooperation was eventually signed between the NSA and the DGSE under the form of a memorandum—most likely the so-called LUSTRE agreement revealed in 2013 by NSA whistleblower Edward Snowden (Follorou, 2013). Another agreement was struck in November 2010 with the British GCHQ.

Jauvert's report connected many pieces of information of what was—and still remains—a puzzle. By then, a few public statements by intelligence officials had already hinted at the formidable growth of the DGSE's Internet surveillance capabilities. The Snowden documents and a handful of investigative reports had also given evidence of France's rank in the world of COMINT. However, for the first time, we were able to get a sense of some of the political intricacies and secret negotiations that presided over the rise of the most significant Internet surveillance program developed by French agencies, as well as their geopolitical outcomes.

But his report also raised questions: If the plan agreed upon at the Élysée Palace in January 2008 was so successful, why did the new French administration wait until the Spring of 2015 to "go public" by presenting the Intelligence Bill aimed at legalising this large-scale surveillance program?

The goal of this paper—adapted from a longer research report (Tréguer, 2016a)—is to study the process of legalisation of Internet surveillance capabilities, taking France as a case study to analyse the impact of post-Snowden contention on the techno-legal apparatus of surveillance, one that has become deeply embedded in the daily routine of security professionals in domestic and transnational security fields.

To provide an empirical analysis of this process of legalisation, the article uses the methodological toolbox of contentious politics, a sub-field of political sociology (Tilly & Tarrow, 2015). It first looks at historical antecedents of legalisation and contention around communications surveillance in France. By providing a content analysis of recent investigative reports and policy documents to shed light on a policy domain veiled in secrecy, the paper points to the growing gap between secret surveillance practices and the law prior to the Snowden disclosures of 2013. It then turns to the impact of these leaks and the resulting episodes of contention for the strengthening of privacy advocacy in France, its chilling effect on legalisation, as well as the role of the terrorist threat and associated processes of securitisation in the adoption of the Intelligence Act of 2015.

While calling for cross-country comparisons of intelligence reforms passed by liberal regimes since 2013, this case study concludes by suggesting that, rather than helping restore the rule of law, post-Snowden contention might paradoxically contribute to reinforcing illiberal trends towards the circumvention of procedural and substantive human rights safeguards, while strengthening the executive power's ability to "rule by law" (Tarrow, 2015, p. 162).

2. Before Snowden, Legalisation Was Underway

As many of its counterparts, France has a record of surveillance scandals. In 1974, a project by the Interior Ministry—aimed at building a huge database gathering as much information as possible on its citizens—sparked a huge outcry, after an unidentified engineer working on the project blew the whistle by speaking to the press (Joinet, 2013). The "SAFARI affair", named after the codename of the project, played an important role in the adoption of the French personal data protection framework in 1978 (Fuster, 2014).

2.1. The Wiretapping Act of 1991: An Antecedent of Legalisation

In 1991, following two condemnations by the European Court of Human Rights (ECHR) pointing to the lack of detailed provision surrounding both judicial and administrative wiretaps, the government rushed to Parliament to pass the Wiretapping Act, which provided the first comprehensive legal framework regulating the surveillance of telephone communications (Errera, 2003).

In the early 1990's, the prospect of Internet surveillance was of course still very distant, and the law was drafted with landline and wireless (satellite in particular) telephone communications in mind. So when tapping into Internet traffic became an operational necessity for intelligence agencies at the end of the 1990's, its

legal basis was progressively hinged on secret and extensive interpretations of existing provisions (one notable exception was a 2006 statute which authorised administrative access to metadata records for the sole purpose of anti-terrorism) (Tréguer, 2016b). Such was the case of the DGSE's large-scale Internet surveillance programme launched in 2008, and apparently backed by a provision of the 1991 Wiretapping Act that gave a blank check to the DGSE to conduct bulk interceptions of so-called "Hertzian transmissions" without any oversight.

French officials looking back at these developments have often resorted to euphemisms, talking about a zone of "a-legality" to describe this secret creep in surveillance capabilities (e.g. Follorou & Johannès, 2013). Although "a-legality" may be used to characterise the legal grey areas in which citizens operate to exert and claim new rights that have yet to be sanctioned by either the parliament or the courts—for instance the disclosure of huge swathes of digital documents (Tréguer, 2015)—it cannot adequately qualify these instances of legal tinkering by secret bureaucracies that seek to escape the safeguards associated with the rule of law. Indeed, when the state interferes with civil rights like privacy and freedom of communication, a detailed, public and proportionate legal basis authorising them to do so is required by supranational courts like the ECHR. Otherwise, such interferences are, quite plainly, illegal.

2.2. Legal Insecurity as a Driver for Legalisation

Secret legal interpretations are, of course, a common feature in the field of surveillance (Rubinstein, Nojeim, & Lee, 2014), and the extralegal regulation of Internet communications has become increasingly common among liberal regimes (Benkler, 2011; Tréguer, 2015). In France, as we will see, they could prosper all the more easily given the shortcomings of human rights advocacy against Internet surveillance. But even so, French national security policy-makers began to worry that the existing framework failed to comply with the standards of the ECHR.

In July 2008, six months after the launch of the DGSE's large-scale Internet surveillance program, the government released the *White Paper of Defence and National Security*—a major effort of strategic planning conducted under Sarkozy's presidency. This official policy document claimed, for what appears to be the first time, that intelligence legislation would soon be presented to Parliament:

> Intelligence activities do not have the benefit of a clear and sufficient legal framework. This shortcoming must be corrected. A new legal architecture will define the duties of intelligence agencies, safeguards for both their personnel and human sources, as well as overarching rules for the protection of classified information. Legislative amendments will be provided, while respecting the balance between the protection of civil rights, the effectiveness of judicial proceedings and the protection of secrecy. (French Government, 2008, p. 142)

The document added that "the consultation of metadata and administrative databases…will be enlarged".

But the following September, a major scandal erupted around the adoption of a decree authorising a very broad intelligence database—named EDVIGE—for domestic surveillance purposes. Within a few weeks, a widespread civil society mobilisation against the decree led the government to backtrack (Marzouki, 2009). It marked one of the biggest episodes of human rights contention under Sarkozy's presidency and was apparently enough to put the government's broader plans for modernising intelligence law to rest until the end of its mandate.

What a conservative, "tough-on-security" government could not achieve would eventually be pursued and carried out by a left-of-center, supposedly pro civil rights party. By the time the Socialist Party returned to power in 2012, its officials in charge of security affairs were the ones pushing for a sweeping reform that would legally secure the work of people in the intelligence community and, incidentally, put France in line with democratic standards (which require a public and detailed legal basis for the surveillance activities of intelligence agencies).

One man played an important role in this process: Jean-Jacques Urvoas, a long-time proponent of intelligence reform in the Socialist Party, who became Minister of Justice in early 2016. After the 2012 elections, Urvoas was re-elected to the National Assembly and awarded with the prestigious position of President of the Committee on Legal Affairs. This also made him a de facto member of the Parliament's Committee on Intelligence, sealing his membership to the small circle of intelligence policymakers. Mid-May 2013—just two weeks before the first Guardian article based on the Snowden files—, Urvoas presented a 200-page-long bipartisan report on the "evolution of the legal framework of intelligence services" (Urvoas & Verchère, 2013). In one section entitled "Tomorrow, a Condemnation by the ECHR?", the report provided an overview of the court's case law and insisted that:

> In France, for lack of legislation adapted to certain aspects of their activities, intelligence services are forced to act outside of any legal framework…. The interception of communication, the listening of places and the tapping of images violate the right to private life, as do the geo-localisation of a phone or of a vehicle…. Concretely, France is risking a condemnation by the European Court of Human Rights for violating the European Convention on Human Rights. For the time being, no legal challenge has been introduced against intelligence-related activities, but there is a constant risk of condemnation. (p. 31)

Recalling the ECHR 1990 rulings against France, the section ended with an invitation to engage in an intelligence

reform based on a careful analysis of the ECHR case law in the field of secret surveillance. But despite this acknowledgement that intelligence agencies had been engaging in illegal surveillance, there was no reaction from human rights groups.

3. After Snowden, Legalisation Sparked Contention

While the global anti-surveillance contention unleashed by Snowden reinforced intelligence policy-makers' rationale for legalisation by documenting surveillance practices to litigation, it also made such reform more exposed to public scrutiny and therefore politically riskier. However, probably comforted by the fact that French privacy advocates had traditionally overlooked the issue of Internet surveillance, policy-makers nevertheless gave it a try. In late 2013, a first attempt at partial legalisation was introduced, eventually giving rise to new alliances among advocacy groups.

3.1. Initial (Lack of) Contention

Initially, the reaction of the French civil society to the Snowden disclosures—the first of which appeared in a Guardian article on June 5th 2013—was relatively mild.

Like in the US, the UK, Germany, and other countries, there was of course widespread media coverage of the Snowden affair in June, July and August of that year (see Figure 1).

Many French Non Governmental Organisations (NGOs) active in the field of human rights joined the media frenzy. Some international organisations with presence in France, like Amnesty or Human Rights Watch, were able to get traction from the initiatives launched elsewhere, occupying the French public sphere by translating press releases targeting the US and the UK agencies. Digital rights organisations working on the overhaul of the EU framework for data protection, like *La Quadrature du Net* (LQDN), mentioned Snowden in passing in their public communications on the matter, but because they were busy working on the proposed EU regulation on data protection, they targeted the data collection practices of Internet firms rather than state surveillance (LQDN, 2013). The only notable exception to this relative apathy was the *Fédération Internationale des Droits de l'Homme* (FIDH), the worldwide movement for human rights founded in 1922, which filed a criminal complaint against NSA's PRISM program and appealed to the UN Special Rapporteur for Freedom of Expression, calling for an investigation into the facts revealed by Snowden (FIDH, 2013).

However, despite the recent Urvoas report hinting at the discrepancy between surveillance practices of French agencies and the law, none of these groups sought to turn the Snowden scandal into an opportunity to call, say, for an independent review of the DGSE's capabilities, or bring new privacy safeguards to a legal framework that was visibly outdated. How can we explain such lack of substantive contention?

3.2. Denials as Legitimisation Strategies

For one, even in activist circles, there was a feeling that the whole affair was mostly related to the NSA and the GCHQ, not to French agencies. In this regard, the legitimation strategies of policy-makers, which denied that French agencies were engaging in the same practices as their Five Eyes counterparts—a strategy also observed in Germany (Schulze, 2015)—, were successful. But even more than denials, it was a no-comment policy that dominated the French government's response to the unfolding scandal.

One notable exception to this wall of communication was Urvoas. On June 12th, in *Le Monde*, the then-member of Parliament refuted that French agencies were conducting large-scale surveillance of Internet communications, claiming:

> I have never heard of tools that could be associated to what the Americans use, and every time I asked intelligence officials, I got a negative answer. (Chapuis, 2013)

But two weeks later, on July 4th, Le Monde ran a piece by reporter Jacques Follorou on the "French Big Brother", claiming that France was "doing the same thing" as the NSA:

> *Le Monde* is able to reveal the General Directorate for External Security (DGSE, special services) systematically collects electromagnetic signals coming from computers or telephones in France, as well as traffic between French and foreigners: the totality of our communications is being spied upon. All emails, SMS, telephone records, connections to Facebook, Twitter, are then stored for years. (Follorou & Johannès, 2013)

The report also quoted a high-ranking intelligence official arguing that these practices were "alegal" (i.e. in a legal

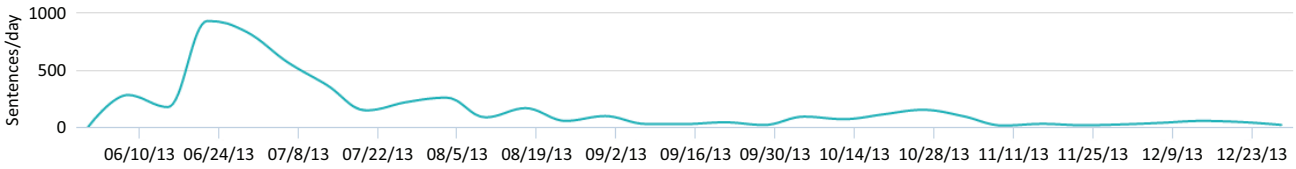

Figure 1. Number of sentences per day mentioning the term "Snowden" in national online news sources in France (based on 129 media sources) from June 2013 to January 2014. Source: MediaMeter.

grey area) rather than illegal (for lack of any public and detailed legal basis).

Considering what we now know about the DGSE's Internet surveillance programs and given also the provision of the 1991 Wiretapping Act allowing bulk collection of wireless communications, the article could have triggered a new scandal, directly aimed at French agencies. But because its sensationalist tone and several inaccuracies—most importantly the fact that it was technically infeasible for the DGSE to collect the "totality" of French communications—, it appeared overblown and was easily dismissed.

Once again, Urvoas was one of the only officials to comment. He immediately published a blog post refuting these allegations, using what would become a favoured metaphor in intelligence circles to distinguish French agencies from the NSA:

> In comparison to the NSA, a technical agency dedicated only to interceptions, the DGSE is a non-specialised agency collecting intelligence for the sole purpose of complying with its regulatory duties. We could thus say that, against the 'fishing trawls' that the NSA seems to be operating, the DGSE is conducting "harpoon fishing" as part of its prerogatives. (Urvoas, 2013a)

But the dismissal of *Le Monde*'s account did not only come from policy-makers. Jean Marc Manach, a journalist, surveillance expert and privacy advocate, also bemoaned the paranoid tone of *Le Monde*'s journalists (Manach, 2013). He also stressed that many of *Le Monde*'s claims, which quoted some of his own reports on the DGSE's so-called "Frenchelon" program, were in fact not new and had been documented before.

Manach was right. By then, officials from the DGSE had already hinted at the formidable growth of the agency's Internet surveillance capabilities. In 2010, its Chief Technology Officer, Bernard Barbier, who was then supervising the plan agreed upon in Sarkozy's office two years earlier, boasted during a public talk before the Cryptographers' Reserve that France was in the "first division" of communications intelligence. He also revealed that the Internet was now the DGSE's "main target" (Manach, 2010). Then, in March 2013, just a few weeks before the beginning of the Snowden disclosures, the head of the DGSE was even less equivocal, admitting before the National Assembly that, since 2008, "we have been able to develop a significant plan for the surveillance of Internet traffic" (French National Assembly, 2013).

3.3. Advocacy Failure

This, in turn begs the question of why, in the immediate aftermath of the Snowden disclosures and even prior to that, it took so long for human rights groups in France to pick up on the pieces of information already available and go after these illegal surveillance operations, both in courts and in policy-making arenas.

The question is a complex one, and cannot be fully addressed here. But two aspects deserve to be mentioned. First, regarding strategic litigation, it is worth noting that in the French civil law system, legal opportunities have traditionally been lacking (Meili, 1998), especially in a field such as state surveillance covered by state secrets. Statements by officials are not enough to initiate legal action. In other countries like the US, they might help trigger successful "FOIA requests" (named after the 1966 Freedom of Information Act) (Schulhofer, 2015). In France however, the national "freedom of information" law adopted in 1978 has extremely broad national security exemptions and is generally much weaker (for instance, the request must specify the exact name of the documents sought after, which represents a formidable hurdle in policy areas covered by state secrets) (Chevallier, 1992).

Second, and more importantly, the lack of mobilisation prior and in the immediate aftermath of the first Snowden disclosures speaks about the structural weaknesses of online privacy advocacy in France, at least until late 2013. Even when in October 2013, thanks to the Snowden trove, *Le Monde* revealed the existence of the so-called LUSTRE data-sharing agreement between the NSA and the DGSE, showing that the latter sent millions of metadata records daily to the US agency (Follorou, 2013), human rights advocacy groups did not pick up on the issue.

A few hypotheses, based on observant-participation conducted in this advocacy field, can be offered to explain these structural weaknesses. Though there have been recent and successful episodes of contention against offline surveillance and intelligence files, Internet surveillance has mostly remained out of the focus of large human rights organisations and smaller digital rights groups in the past decade, which may be due to the particular interests of their staff and subsequent prioritisation in handling their limited resources. Also, a general knowledge of the field in the US, the UK or Germany suggests that historical factors, more recent legalisation processes and leaks regarding Internet surveillance programs likely played an important role in helping civil society groups in these countries maintain stronger networks and expertise.

One major moment of the transnational post-Snowden contention, for instance, was the release of the "International Principles on the Application of Human Rights to Communications Surveillance" in May 2014 (EFF, 2014). Although framed as a key response of the global civil society to the Snowden controversies, the work on this text started as early as 2012 and, as noted in the document, "more than 40 privacy and security experts participated in the drafting process". However, according to one interview conducted for this article with a lawyer who played a major role in the drafting of this document, there wasn't any French national among them. This tends to confirm that, until recently, French NGOs

had remained outside of these transnational networks working on state surveillance.

3.4. Legalisation of Metadata Access Sparks Contention

These structural weaknesses of anti-surveillance advocacy in France help explain why intelligence policymakers would try to legalise very intrusive metadata access powers as early as October 2013, in the midst of the Snowden scandal.

In 2006, a law had been adopted to give intelligence agencies access to metadata records held by access providers and hosting providers, but only for fighting terrorism. What is more, from 2009 on, intelligence agencies had apparently experimented with traffic-scanning devices provided by Qosmos and installed on the infrastructure of the few major telecom operators to monitor metadata in real-time (Hourdeaux, 2016; Reflets.info, 2016).

Already in late-2012, it was becoming clear to intelligence policy experts that—in line with what had already been alluded to in the 2008 White Paper of Defence—these crucial capabilities for expanded and real-time access to metadata needed to be secured. Despite public discussions on the matter in Parliament at the time, nobody in the advocacy sphere apparently took notice.

In August 2013, Prime Minister Manuel Valls presented the 2014–2019 Military Planning Bill (*Loi de Programmation Militaire*, or LPM). Over the course of the parliamentary debate, and in particular when the Senate adopted amendments to the Bill in first reading in October 2013, the law became the vehicle for a partial legalisation of the new capabilities. We were just four months after the first Snowden disclosures, and again no human rights organisation reacted. Six weeks later however, an industry group representing online social services including Google France, AOL, eBay, Facebook, Microsoft, Skype and French companies like Deezer or Dailymotion published an article against the reform (*Association des Services Internet Communautaires*, 2013). It was only then that human rights groups understood the importance of this provision and mounted a last-minute effort to get the provision out of the bill.

Coming at a very late stage of the legislative procedure, the effort eventually failed to strike out the provision. But despite this failure and a somewhat exaggerated denunciation of "generalised surveillance," this first episode of post-Snowden contention had at last led to the mobilisation of civil society groups around Internet surveillance issues, one which benefited from widespread media coverage. Frustrated by their failure to react in time (*before* rather than *after* industry groups) and also finally realising the need to build and share expertise around Internet surveillance and digital rights in general, human rights groups created a new umbrella organisation. Announced on the international "data protection day" in January 2014, it was called the *Observatoire des Libertés et du Numérique* (OLN).

OLN's initial members included organisations that often worked together on non-Internet issues—including the Human Rights League, a lawyers' union (*Syndicat des Avocats de France*) and a judges' union (*Syndicat de la Magistrature*). They were joined by two smaller research organisations devoted to the interplay of the digital technologies and privacy (CECIL and CREIS-Terminal). A few days later, LQDN—with its already established expertise on digital rights, its singular Internet-inspired political culture as well as its own international networks (Breindl, 2011)—, asked to join the coalition.

This brokerage of new connections between French human rights NGOs would play a key role against the Intelligence Bill. But in the meantime, the government apparently slowed the path to legalisation set forth by Urvoas in its recent reports. Post-Snowden contention was finally under way in France, and it was likely perceived to make any significant intelligence reform much more politically risky. At least in the short term.

4. A Long-Awaited Legalisation: Passing the 2015 Intelligence Act

Soon, with the spectacular rise of the threat posed by the Islamic State (Giroux, 2014) and the Paris attacks of January 2015, "securitisation" discourses helped create the adequate political conditions for the passage of the Intelligence Act—the most extensive piece of legislation ever adopted in France to regulate the work of intelligence agencies.

Securitisation is understood in critical security studies as "speech acts through which an intersubjective understanding is constructed within a political community to treat something as an existential threat to a valued referent object, and to enable a call for urgent and exceptional measures to deal with the threat" (Buzan & Wæver, 2003, p. 491). In the field of terrorism, these are of course not new. And by the time the Intelligence Bill was introduced, anti-terrorism was already back on the top of the political agenda in France, with the looming threat coming from the Islamic State in Syria and Iraq.

In July 2014, just as the government was introducing a new anti-terrorism bill before the Parliament, President François Hollande convened a National Intelligence Council at the Élysée Palace. In the laconic press-release issued on that day, the Council claimed to have "determined the strategic priorities of [intelligence] services and approved the legal, technical and human resources necessary to carry on these priorities" (French Presidency, 2014). The debate on the anti-terrorism bill, finally adopted on November 2014, also gave an opportunity to OLN members to engage in their first coordinated action against the law's new restrictions on freedom of expression online.

But on January 25th 2015, then Prime Minister Manuel Valls turned the long-awaited intelligence reform into an essential part of the government's political response to the Paris attacks carried on earlier

that month. With the country under shock, Valls presented yet another package of "exceptional measures" that formed part of the government's proclaimed "general mobilisation against terrorism". (French Government, 2015). He announced his government would soon present a new bill, which he said was "necessary to strengthen the legal capacity of intelligence agencies to act," alluding to "Djihadist Internet communications".

The Paris attacks only reinforced the ongoing trend toward securitisation, helping to locate the fight against terrorism—and the instrumental role of communications surveillance in that respect—beyond the domain of normal, democratic politics. Securitisation would for instance justify the government's choice to present the bill to Parliament using a fast-track procedure, allowing only one ruling in each of the Parliament's chambers. In sum securitisation was effectively added to denials as rhetorical strategies aimed at dealing with post-Snowden contention, and finally pass a legal basis for what were until then illegal security practices.

4.1. The Intelligence Act's Main Provisions on Internet Surveillance

During the expeditious parliamentary debate that ensued (April–June 2015), the bill's proponents never missed an opportunity to stress, as Valls did while presenting the text to the National Assembly, that the new law had "nothing to do with the practices revealed by Edward Snowden". Distinction strategies notwithstanding, the Act's provisions actually demonstrate how important the sort of practices revealed by Snowden have become for the geopolitical "arms race" in communications intelligence.

The Intelligence Act creates whole new sections in the Code of Internal Security. It starts off by widening the scope of public-interest motives for which surveillance can be authorised. Besides terrorism, economic intelligence, organised crime and counter-espionage, it now includes vague notions such as the promotion of "major interests in foreign policy" or the prevention of "collective violence likely to cause serious harm to public peace". As for the number of agencies allowed to use this new legal basis for extra-judicial surveillance, it comprises the "second circle" of law enforcement agencies that are not part of the official "intelligence community" and whose combined staff is well over 45,000.

In terms of technical capabilities, the Act seeks to harmonise the range of tools that intelligence agencies can use on the regime applicable to judicial investigations. These include targeted telephone and Internet wiretaps, access to metadata and geotagging records as well as computer intrusion and exploitation (i.e. "hacking"). But the Act also authorises techniques that directly echo the large-scale surveillance practices at the heart of post-Snowden controversies. Such is the case of the so-called "black boxes", these scanning devices that will use Big Data techniques to sort through Internet traffic in order to detect "weak signals" of terrorism (intelligence officials have given the example of encryption as the sort of things these black boxes would be looking for).

Another provision limited to anti-terrorism allows for the real-time collection of metadata. Initially, the provision targeted only individuals "identified as a [terrorist] threat". After the 2016 Nice attack, it was extended to cover individuals "likely related to a threat" or who simply belong to "the entourage" of individuals "likely related to a threat". In theory, tens of thousands of people could fall under this definition, and have their metadata collected in real-time during a renewable period of four months.

Similarly, there is a whole chapter on "international surveillance", which legalises the massive programme deployed by the DGSE since 2008 to tap into international cables. Like in other countries, the underlying logic of this article breaches the universality of human rights: communications crossing French borders can be intercepted and analysed "in bulk" with lesser safeguards than those applicable to domestic surveillance. However, the transnational nature of the Internet makes it very likely that the communications of French citizens and residents massively end up in the DGSE's nets, despite a pledge for procedures of so-called "technical minimisation" aimed at protecting communications related to "French technical identifiers" (e.g. French IP addresses).

The Act also grants blanket immunity to intelligence officers who carry on computer crimes into computer systems located abroad, which again will directly affect many French Internet users. The provision may contravene Article 32(b) of the Budapest Convention on Cybercrime on the trans-border access to computer data (Cybercrime Convention Committee, 2014). This provision speaks to the fact that, with encryption on the rise since 2013, the capability to massively penetrate endpoints through hacking is becoming a focus point for intelligence agencies (e.g. UK Home Office, 2016).

As for oversight, as it has been the case since the 1991 Wiretapping Act, all national surveillance activities are authorised by the Prime Minister. A revamped oversight commission (the CNCTR) composed of judges and members of Parliament has 24 hours to issue non-binding opinions on authorisation requests. The main innovation of the Intelligence Act is the creation of a new redress mechanism before the *Conseil d'Etat* (France's Supreme Court for administrative law), but the procedure is veiled in secrecy and fails to respect defence rights, which again echoes the law of the US and the UK (Bigo, Carrera, Hernanz, & Scherrer, 2014). International surveillance will remain completely outside of this redress procedure.

Among other notable provisions, one forbids the oversight body from reviewing communications data obtained from foreign agencies. The law also fails to provide any framework to regulate (and limit) access to the collected intelligence once it is stored by intelligence and law enforcement agencies, thereby running counter to

recent rulings by the Court of Justice of the European Union (CJEU) (Woods, 2016).

4.2. Mobilisation Against the Controversial French Intelligence Bill

By the time the Intelligence Bill was debated in Parliament, in April 2015, human rights organisations partnering in OLN had built the kind of networking and expertise that made them more suited to campaign against national security legislation.

They led the contention during the three-month-long parliamentary debate on the Bill, acting as the core of a network of actors typical of post-Snowden contention (see Figure 2), including international partners in the NGO world, groups of scientists, engineers and hacker groups, French independent companies from the digital sector, and even a few security experts (including former intelligence analysts or a former anti-terrorist judge). These actors also received backing from leading national and international human rights organisations (data protection agency, Council of Europe, UN special rapporteurs, etc.).

Interestingly, to the contrary of the full-fledged contention waged in the US or the UK, large US technology firms like Google or Microsoft declined to engage in the French debate, perhaps out of fear for being cornered for their double-speak on privacy and antagonising French officials, who regularly accused them of engaging in intrusive forms of commercial surveillance. As for their French competitors, like telecommunications companies Orange, SFR and others, their even greater dependence on and proximity with the state political elite probably explain why they chose to remain neutral bystanders.

Overall, contention played an important role in barring amendments that would have given intelligence agencies even more leeway than originally afforded by the bill. Whereas the government hoped for a union sacrée, contention also managed to fracture the initial display of unanimity. MPs from across the political spectrum (including several within both socialist and conservative ranks) fought against the bill, pushing its proponents to amend the text in order to bring significant safeguards compared to the government's proposal. However, the general philosophy of the text remained intact. In June 2015, the bill was eventually adopted with 438 votes in favour, 86 against and 42 abstentions at the National Assembly and 252 for, 67 against and 26 abstentions at the Senate.

The implementation decrees were adopted by the government between October 2015 and February 2016, giving civil society opponents a two-month window to introduce several important legal challenges before the Council of State which are, at the time of writing, still pending. Other legal challenges have been introduced before the ECHR.

5. Conclusion: Facing the Snowden Paradox

The first Snowden disclosures and the global scandal that followed held the promise of an upcoming rollback of the techno-legal apparatus developed by the NSA, the GCHQ and their counterparts to intercept and analyse large portions of the world's Internet traffic. State secrets and the "plausible deniability" doctrine often used by these secretive organisations could no longer stand in the face of such overwhelming documentation. Intelligence reform, one could then hope, would soon be put on the agenda to relocate these surveillance programmes within the boundaries of the rule of law.

Almost four years later, however, what were then reasonable expectations have likely been crushed. Intel-

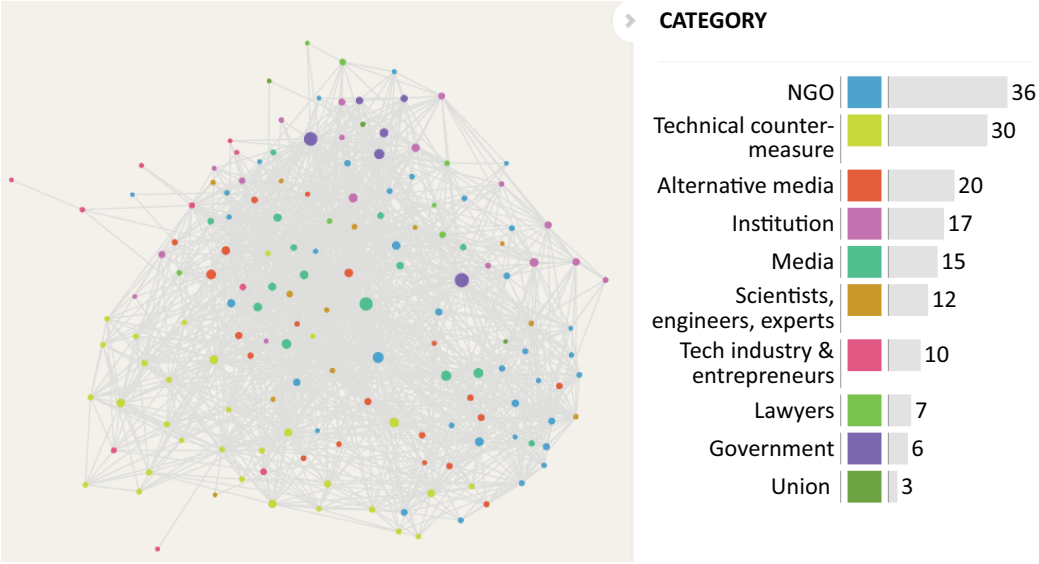

Figure 2. Web cartography of actors mobilised against the French Intelligence Bill. Explore the network online at the following address: https://is.gd/cLkzqh

ligence reform is being passed, but mainly to secure the legal basis for large-scale surveillance to a degree of detail that was hard to imagine just a few years ago. Despite unprecedented mobilisations against surveillance practices developed in the shadows of the "deep state", the latter are progressively being legalised. Hence the Snowden paradox.

France was the first liberal regime to engage in a sweeping, post-Snowden intelligence reform. There, even prior to 2013, the legal pressure exerted by human rights standards, and their application by supranational courts like the ECHR, had already triggered a slow process of legalisation. Post-Snowden contention only made that pressure stronger, pushing intelligence policymakers to secure and expand the surveillance capabilities of their agencies through intelligence reform, as soon as the political conditions seemed ripe.

While it would be tempting to see the Intelligence Act of 2015 as part of a certain French tradition when it comes to regulating the Internet (Mailland, 2001; Meyer & Audenhove, 2012; Tréguer, 2015), the situation in other countries suggests that the French case is part of a wider trend. In the Fall of 2016, the British Parliament passed the much-criticised Investigatory Powers Bill (Hintz & Dencik, 2016). Simultaneously in Germany, amendments to the so-called "G-10 law" were adopted to validate the large-scale surveillance powers of the country's foreign intelligence agency, the BND—also embroiled in the NSA scandal (Wetzling, 2016). In the Netherlands, an ongoing intelligence reform is raising similar concerns, while the reform of the US PATRIOT Act in June 2015 was extremely modest. Detailed cross-country comparisons are of course warranted. But despite important variations between these countries—for instance regarding the initial weaknesses and strengths of privacy advocacy in these different national contexts, or the role played by large US Internet firms in policy debates—, these other instances of post-Snowden intelligence reform seem to confirm the existence of the Snowden paradox.

Fifteen years after 9/11, which brought an abrupt end to the controversy on the NSA's ECHELON program (Campbell, 2000) and paved the way for the adoption of the PATRIOT Act in the US and similar legislation elsewhere, the threat of terrorism and associated processes of securitisation are hindering the global episode of contention opened by Edward Snowden. Securitisation creates a "chilling effect" on civil society contention, making legalisation politically possible and leading to a "ratchet effect" in the development of previously illegal security practices or, more generally, of executive powers. In that regard, post-Snowden intelligence reform stands as a stark reminder of the fact that, once coupled with securitisation, "a-legality" and national security become two convenient excuses for legalisation and impunity, allowing states to navigate the legal and political constraints created by human rights organisations and institutional pluralism.

During the debate on the French Intelligence Act, Urvoas stressed that the law was neither Schmitt's nor Agamben's states of exception (Urvoas, 2013b). But because it is "legal" or includes some oversight and redress mechanisms does not mean that large-scale surveillance and secret procedures do not represent a formidable challenge to the rule of law. Rather than a state of exception, legalisation carried on under the guise of the raison d'État amounts to what Sidney Tarrow calls "rule by law". In his comparative study of the relationships between states, wars and contention, he writes of the US "war on terror":

> Is the distinction between rule of law and rule by law a distinction without difference? I think not. First, rule by law convinces both decision makers and operatives that their illegal behavior is legally protected….Second, engaging in rule by law provides a defense against the charge they are breaking the law. Over time, and repeated often enough, this can create a "new normal", or at least a new content for long-legitimated symbols of the American creed. Finally, "legalizing" illegality draws resources and energies away from other forms of contention. (2015, pp. 165–166)

The same process is happening with regards to present-day state surveillance: the suspicionless interception of communications, "big data" preventive policing and large-scale computer hacking are becoming the new normal in intelligence practices. At this point in time, it seems difficult to argue that post-Snowden contention has hindered in any significant and lasting way the formidable growth of surveillance capabilities of the world's most powerful intelligence agencies.

And yet, while the current trend of legalisation is especially worrying considering the ongoing illiberal drift in Western democracies, the jury is still out. Besides legalisation, Post-Snowden contention is having another major outcome: new coordination in civil society both nationally and globally, with the formation of a transnational movement against Internet surveillance (Tarrow, 2016). This emerging movement has been documenting Internet surveillance like never before, undermining some of the secrecy that surrounds the intelligence field and hinders its democratic accountability. It has provided fresh political and legal arguments to reclaim privacy as a "part of the common good" (Lyon, 2015, p. 9), and helped push for the proliferation of legal and policy recommendations regarding the compliance of surveillance with human rights.

Most crucially, this emerging privacy movement has led courts—in particular the ECHR and the CJEU—to consider cases of historic importance that, in the long run, could prove to be game-changers. Strategic litigation has indeed the potential of turning the Snowden paradox on its head, that is to use these new laws—and the new legal opportunities it brings to privacy advocates—to counter

the surveillance practices that legalisation sought to legitimise in the first place.

Judges now appear as the last institutional resort against large-scale surveillance. If court actions fail, the only possibility left for resistance will lie in what would by then represent a most transgressive form of political action: democratising the use of strong encryption, and subverting the centralised and commodified technical architecture that made such surveillance possible in the first place.

Acknowledgements

This research was conducted for the UTIC project, supported by the French National Research Agency.

Conflict of Interests

The author declares no conflict of interests.

References

Association des Services Internet Communautaires. (2013, March 18). Surveillance de l'Internet, accès aux données d'utilisateurs: Pour un moratoire sur les régimes d'exception. *Association des Sites Internet Communautaires*. Retrieved from http://archive.is/firXs

Benkler, Y. (2011). A free irresponsible press: Wikileaks and the battle over the soul of the networked fourth estate. *Harvard Civil Rights-Civil Liberties Law Review*, *46*(2), 311–397.

Bigo, D., Carrera, S., Hernanz, N., & Scherrer, A. (2014). *National security and secret evidence in legislation and before the courts: Exploring the challenges* (Report to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs [LIBE] No. PE 509.991). Brussels: European Parliament. Retrieved from http://www.europarl.europa.eu/thinktank/fr/document.html?reference=IPOL_STU%282014%29509991

Breindl, Y. (2011). *Hacking the law: An analysis of internet-based campaigning on digital rights in the European Union*. Brussels: Free University of Brussels.

Buzan, B., & Wæver, O. (2003). *Regions and powers: The structure of international security*. Cambridge: Cambridge University Press.

Campbell, D. (2000). Inside Echelon: The history, structure, and function of the global surveillance system known as Echelon. *Telepolis*. Retrieved from https://www.heise.de/tp/features/Inside-Echelon-3447440.html

Chapuis, N. (2013, June 12). Urvoas: "Je n'ai pas rencontré de programme de surveillance similaire en France". *Le Monde*. Retrieved from http://www.lemonde.fr/politique/article/2013/06/12/urvoas-je-n-ai-pas-rencontre-de-programme-de-surveillance-similaire-en-france_3428507_823448.html

Chevallier, J. (1992). Le mythe de la transparence administrative. In *Information et transparence administrative* (pp. 239–275). Paris: Presses Universitaires de France.

Cybercrime Convention Committee. (2014). *T-CY Guidance Note #3 transborder access to data* (No. T-CY [2013]7 E). Strasbourg: Council of Europe. Retrieved from https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/T-CY%282013%297REV_GN3_transborder_V11.pdf

EFF. (2014). *Necessary & proportionate: International principles on the application of Human Rights to communications surveillance*. Retrieved from https://en.necessaryandproportionate.org

Errera, R. (2003). Les origines de la loi française du 10 juillet 1991 sur les écoutes téléphoniques. *Revue Trimestrielle des Droits de l'Homme*, *55*, 851–870.

Fédération Internationale des Droits de l'Homme. (2013, July 12). Affaire Snowden: La FIDH saisit l'ONU. *FIDH*. Retrieved from https://archive.is/mSEZo

Follorou, J. (2013, October 30). Surveillance: La DGSE a transmis des données à la NSA américaine. *Le Monde*. Retrieved from http://www.lemonde.fr/international/article/2013/10/30/surveillance-la-dgse-a-transmis-des-donnees-a-la-nsa-americaine_3505266_3210.html

Follorou, J., & Johannès, F. (2013, July 4). La totalité de nos communications espionnées par un supercalculateur. *Le Monde*. Retrieved from http://www.lemonde.fr/ societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html

French Government. (2008). *Livre blanc sur la défense et la sécurité nationale*. Paris: French Government.

French Government. (2015, November 19). *#Antiterrorisme: Manuel Valls annonce des mesures exceptionnelles*. Paris: French Government. Retrieved from http://archive.is/x1zhB

French National Assembly. (2013). *Audition du préfet Erard Corbin de Mangoux, Directeur Général de la sécurité extérieure (DGSE) au ministère de la Défense* (Compte Rendu n° 56). Paris: French National Assembly.

French Presidency. (2014, July 9). *Compte-rendu public du Conseil national du renseignement*. Retrieved from https://archive.is/7W2jm

Fuster, G. G. (2014). *The emergence of personal data protection as a fundamental right of the EU*. Berlin: Springer Science+Business.

Giroux, H. A. (2014). ISIS and the spectacle of terrorism: Resisting mainstream workstations of fear. *Philosophers for Change*. Retrieved from https://philosophersforchange.org/2014/10/07/isis-and-the-spectacle-of-terrorism-resisting-mainstream-workstations-of-fear

Hintz, A., & Dencik, L. (2016). The politics of surveillance policy: UK regulatory dynamics after Snowden. *Internet Policy Review*, *5*(3). doi:10.14763/2016.3.424

Hourdeaux, J. (2016, June 6). Comment les services de renseignement ont mis en place une surveillance

générale du Net dès 2009. *Mediapart*. Retrieved from https://www.mediapart.fr/journal/france/060616/comment-les-services-de-renseignement-ont-mis-en-place-une-surveillance-generale-du-net-des-2009

Jauvert, V. (2015, July 1). Comment la France écoute (aussi) le monde. *Le Nouvel Observateur*. Retrieved from http://tempsreel.nouvelobs.com/societe/20150625.OBS1569/exclusif-comment-la-france-ecoute-aussi-le-monde.html

Joinet, L. (2013). *Mes raisons d'État: Mémoires d'un épris de justice*. Bayonne: La Découverte.

La Quadrature du Net. (2013, July 29). Newsletter #51. *LQDN*. Retrieved from https://www.laquadrature.net/fr/newsletter/newsletter-51

Lyon, D. (2015). *Surveillance after Snowden*. Cambridge: Polity Press.

Mailland, J. (2001). Freedom of speech, the internet, and the costs of control: The French example. *New York University Journal of International Law & Politics*, *33*.

Manach, J. M. (2010, October 2). Frenchelon: La DGSE est en "1ère division". *Le Monde*. Retrieved from http://bugbrother.blog.lemonde.fr/2010/10/02/frenchelon-la-dgse-est-en-1ere-division

Manach, J.-M. (2013, July 11). La DGSE a le "droit" d'espionner ton Wi-Fi, ton GSM et ton GPS aussi. *Le Monde*. Retrieved from http://bugbrother.blog.lemonde.fr/2013/07/11/la-dgse-a-le-droit-despionner-ton-wi-fi-ton-gsm-et-ton-gps-aussi

Marzouki, M. (2009). "Non à Edvige": Sursaut ou prise de conscience? *Plein Droit*, *80*, 21–26. Retrieved from http://www.gisti.org/spip.php?article1477

Meili, S. (1998). Cause lawyers and social movements: A comparative perspective on democratic change in Argentina and Brazil. In A. Sarat & S. Scheingold (Eds.), *Cause lawyering: Political commitments and professional responsibilities* (pp. 487–522). Oxford: Oxford University Press.

Meyer, T., & Audenhove, L. V. (2012). Surveillance and regulating code: An analysis of graduated response in France. *Surveillance & Society*, *9*(4), 365–377.

Reflects.info. (2016, June 6). Qosmos et le gouvernement Français, très à l'écoute du Net dès 2009. *Reflects.info*. Retrieved from https://reflets.info/qosmos-et-le-gouvernement-francais-tres-a-lecoute-du-net-des-2009

Rubinstein, I. S., Nojeim, G. T., & Lee, R. D. (2014). Systematic government access to personal data: A comparative analysis. *International Data Privacy Law*, *4*(2), 96–119.

Schulhofer, S. (2015). *Access to national security information under the U.S. Freedom of Information Act* (Public Law Research Paper No. 15–14). New York, NY: NYU School of Law. Retrieved from https://papers.ssrn.com/abstract=2610901

Schulze, M. (2015). Patterns of surveillance legitimization. The German discourse on the NSA scandal. *Surveillance & Society*, *13*(2), 197–217.

Tarrow, S. (2015). *War, states, and contention: A comparative historical study* (1st ed.). Ithaca and London: Cornell University Press.

Tarrow, S. (2016). *Close interaction, incompatible regimes, contentious challenges: The transnational movement to protect privacy*. Berlin: Berlin Social Science Center. Retrieved from https://www.researchgate.net/project/Transnational-Movements-and-the-Protection-of-Privacy/update/582c8dc608ae91d0fe24f203

Tilly, C., & Tarrow, S. (2015). *Contentious politics* (2nd ed.). New York, NY: Oxford University Press.

Tréguer, F. (2015). Hackers vs states: Subversion, repression and resistance in the online public sphere. *Droit et Société*, *91*(3), 639–652.

Tréguer, F. (2016a). *From deep state illegality to law of the land: The case of internet surveillance in France*. Paper presented at the 7th Biennial Surveillance & Society Conference (SSN 2016) "Power, Performance and Trust", Barcelona, Spain. Retrieved from https://halshs.archives-ouvertes.fr/halshs-01306332/document

Tréguer, F. (2016b). *French constitutional council strikes down 'Blank Check' provision in the 2015 Intelligence Act*. Retrieved from https://halshs.archives-ouvertes.fr/halshs-01399550/document

UK Home Office. (2016). *Operational case for bulk powers*. London: British Government. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf

Urvoas, J.-J. (2013a, July 4). *Big Brother à la française? Commentaires*. Retrieved from http://archive.is/7SGgk

Urvoas, J.-J. (2013a, October 30). Il faut renforcer le contrôle des services de renseignement en France. *Le Monde*. Retrieved from http://www.lemonde.fr/idees/article/2013/10/30/il-faut-renforcer-le-controle-des-services-de-renseignement-en-france_3505116_3232.html

Urvoas, J.-J., & Verchère, P. (2013). *Rapport en conclusion des travaux d'une mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement* (Commission des Lois No. 1022). Paris: National Assembly. Retrieved from http://www.assemblee-nationale.fr/14/controle/lois/renseignement.asp

Wetzling, T. (2016). *The key to intelligence reform in Germany* (Europäische Digitale Agenda). Retrieved from http://www.stiftung-nv.de/sites/default/files/snv_g10.pdf

Woods, L. (2016, December 21). Data retention and national law: The ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber). *EU Law Analysis*. Retrieved from https://eulawanalysis.blogspot.fr/2016/12/data-retention-and-national-law-ecj.html

About the Author

Félix Tréguer works on past and present contention around the protection of civil rights and communicational autonomy on the Internet. He is a junior researcher at CERI-Sciences Po, where he looks at post-Snowden controversies for the UTIC project. He is a founding member of the Paris-based digital rights advocacy group *La Quadrature du Net*.