



**HAL**  
open science

# US Technology Companies and State Surveillance in the Post-Snowden Context: Between Cooperation and Resistance

Félix Tréguer

► **To cite this version:**

Félix Tréguer. US Technology Companies and State Surveillance in the Post-Snowden Context: Between Cooperation and Resistance. [Research Report] CERI. 2018. halshs-01865140

**HAL Id: halshs-01865140**

**<https://shs.hal.science/halshs-01865140>**

Submitted on 30 Aug 2018

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

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



Distributed under a Creative Commons Attribution 4.0 International License

**UTIC Deliverable 5**

**US Technology Companies and State Surveillance in the  
Post-Snowden Context:  
Between Cooperation and Resistance**

Author: Félix Tréguer (CERI-SciencesPo)

# Executive Summary

This deliverable looks at the growing hybridization between public and private actors in the field of communications surveillance for national security purposes. Focusing on US-based multinationals dominating the digital economy globally which became embroiled in the post-Snowden debates (companies like Google, Apple, Facebook, Microsoft, Yahoo), the report aims at understanding the impact of the Snowden scandal on the strategies of these companies in relation to state Internet surveillance.

To that end, the report identifies seven factors that are likely to influence the stance of a given company and its evolution depending on the changing context and constraints that it faces across time and space. These factors are: the firm's internal corporate culture, the pressure coming from the human rights field, the importance of user trust on these companies' businesses, their sensitivity to regulatory changes, the identification of the firm managers to the power elite, the firm's dependence on public procurements and, finally, the existence of criminal sanctions for non-cooperation.

The report then applies this constraint structure affecting the participation of large Internet firms in public-private surveillance assemblages through two case-studies looking at post-Snowden debates in the United States and in France. We observe important differences depending on the considered country in the initial phase of the scandal (2013-2015). In the US, we first see overt and multi-pronged resistance strategies being staged, which can be read as an instance of double-dealing (in the sense that commitments to human rights actually reinforced the position of these firms in their respective markets). In France these companies faced a much more antagonist environment, partly resulting from existing public-private alliances, and their initial attempt at resistance to the expansion of state surveillance capacities was immediately denounced by government officials as hypocritical, considering their own commercial surveillance practices. This subsequently led to much less intense and much more discreet forms of resistance.

But overtime, from 2015 on, the influence of the human rights field withered along with the media attention devoted to state surveillance. Through securitization discourses, the agenda became dominated by terrorist threats and similar trends towards greater cooperation materialised on both sides of the Atlantic – especially regarding the issue of the monitoring and takedown of terrorism-related content on online platforms –, suggesting strong transnational field effects. As a consequence, while we note variations depending on the companies and the two countries under consideration, the public-private stand-offs eventually resulted in coherent mechanisms producing similar outcomes.

In concluding the deliverable, we build on these case studies to argue that such ongoing public-private hybridization processes need to be framed in the context of wider shifts affecting modern bureaucracies – with the growing importance of data governance for modern state power –, and point to the adverse impact of these trends on the rule of law.

# Table of Contents

<b>Executive Summary</b> .....	<b>2</b>
<b>1. Introduction</b> .....	<b>4</b>
1.1 Goal of the deliverable.....	7
1.2 Brief literature review.....	7
1.3 Methodology of this report.....	10
1.4 Research Questions & Outline.....	11
<b>2. Hypothesis on the Constraint Structure of Large Internet Firms in Debates on State Surveillance</b> .....	<b>13</b>
2.1 Internal corporate culture.....	13
2.2 Pressure from human rights field.....	14
2.3 User trust and business stakes.....	15
2.4 Regulatory stakes.....	17
2.5 Identification to and dependency on power elite.....	17
2.6 Firm’s dependence on public procurements.....	18
2.7 Criminal sanctions.....	19
<b>3. (Re)configuration of Public-Private Assemblages in Internet Surveillance: Case-Studies</b> .....	<b>22</b>
3.1 US: “Big Tech” stages resistance.....	22
3.2 France: Facing established public-private alliances.....	46
<b>4. Conclusion: Changing Bureaucracies, Security &amp; the Rule of Law</b> .....	<b>61</b>
<b>References</b> .....	<b>65</b>
<b>Appendix 1: Roundtable “The Internet, Private Actors and Security Challenges” (CERI, October 9<sup>th</sup>, 2017)</b> .....	<b>71</b>
Programme.....	71
Draft transcription by Barthélémy Michalon.....	72

# 1. Introduction

In June 1831, a Frenchman under the name of Alexandre Ferrier sought to create the first privately-held optical telegraph line between Calais, in Northern France, and London. Ferrier was an adventurous entrepreneur who did not back away from bold ideas. After all, such a privately-owned telecommunications infrastructure could not only serve the interest of French industry barons willing to track stock prices in the world financial capital, but also to the French government who could use it for its diplomatic communications. Moreover, there was no law sanctioning the *de facto* monopoly of the French state over telegraph networks.

Ferrier was bold, but he also knew that he would be more cautious to ask the government for an explicit authorization. In turn, Casimir Périer, head of the government, wanted an informed opinion on the matter. Yes, Ferrier's proposal was unusual but, after all, many political and business elites agreed that the telegraph could be a boon for the emerging industrial revolution (Flichy, 1991). Could the the government seriously consider keeping its monopoly over the telegraph? Many thought not.

## Privatizing the telegraph?

But Alphonse Roy, the man Périer turned to in order to make up his mind, had an entirely different view on the matter. As the newly-appointed Director of the Telegraph Service at the Ministry of Interior, Roy wrote a letter that offered a more-than-tepid response to Ferrier's project. "Mr. Ferrier's request is entirely inadmissible," he wrote. And so no one could be mistaken, he added: "The claim that a telegraph line owned by individuals could be established across the strait to extend the line of the State that ends in Calais, and that it could be of any service to the government, is something completely illusory."

Why? First of all, as Roy explained, "the Administration would never entrust diplomatic secrets to agents who are not responsible to her (...)." But the argument seemed specious. For one thing, every diplomatic cable was encrypted in Chappe code and, according to historian Paul Charbon, was "completely unintelligible for those in charge of transmitting it" (Charbon, 1991). More crucially, the heart of the matter was the absolutely unthinkable notion that the French state might lose its monopoly over telecommunications infrastructure. As Roy argued more convincingly, "the existence of this telegraph communication would necessarily harm the present privilege of the government to be the first instructed of all important news."

Over the next six years, the French administration worked on a plan to retain its monopoly over the deployment and exploitation of telegraph networks, while starting to open its use to the general public. In 1837, the Minister of the Interior, Adrien de Gasparin, appeared before the Parliament to defend a new law designed to put that plan into effect. The goal was to criminalise every transmission not sanctioned by the government and not sent over its own lines.

Speaking before the house, Gasparin tried to stir support by referring to the "revolt of the Canuts", a social unrest that had taken place a few years earlier among textile factory workers in Lyon. At the time, the only people who could have been sentenced under the new law were petty speculators who had fraudulently transmitted financial news to businessmen in Bordeaux, Lyon or Marseilles,

allowing their rich clients to take advantage over their competitors still dependent on the postal service. But these did not seem as dangerous for the regime as the rebellious workers protesting the violence of the industrial revolution. According to Gasparin, “it is by organizing themselves like the French administration that they tried to defeat us” (Gasparin, 1837). “Many elements of success failed them,” he stressed, “but we can affirm without exaggeration that it was especially the telegraph that failed them.” According to the Minister, the latter would have allowed insurgents “to impress upon their movements a formidable precision” by spreading the word of the rebellion to various industrial centers across the country.

After highlighting the risk of sedition that the liberalisation of the telegraph would entail, Gasparin moved to the core of the matter. Yes, he assured the members of Parliament, the government had tried “to reconcile the interest of public order with those of industry” by breaking the monopoly and by establishing a governmental surveillance of private telegraph lines. “We do not like monopolies for themselves”, swore Gasparin. “We would be glad to extend to everybody the facilities which the telegraph has brought to the Government. But the guarantees that we are offered are truly illusory.”

“No doubt,” he claimed, the operators working on these private lines “would faithfully transmit the dispatches delivered to them by our intermediary.” And “of course,” he continued, “we would be careful to examine these dispatches, and to let pass only those which appear innocent.” “But how can we be certain that a hidden meaning has not been attached, through certain conventions, to the sentences that would appear to be the most harmless?” According to him, a privatized telecommunications infrastructure was a challenge that the modern state simply could not handle. All the techniques of power institutionalized since the 16<sup>th</sup> century to control the subversive effect of the printing press while allowing it to serve the interests of the state and of early capitalism would come crumbling.

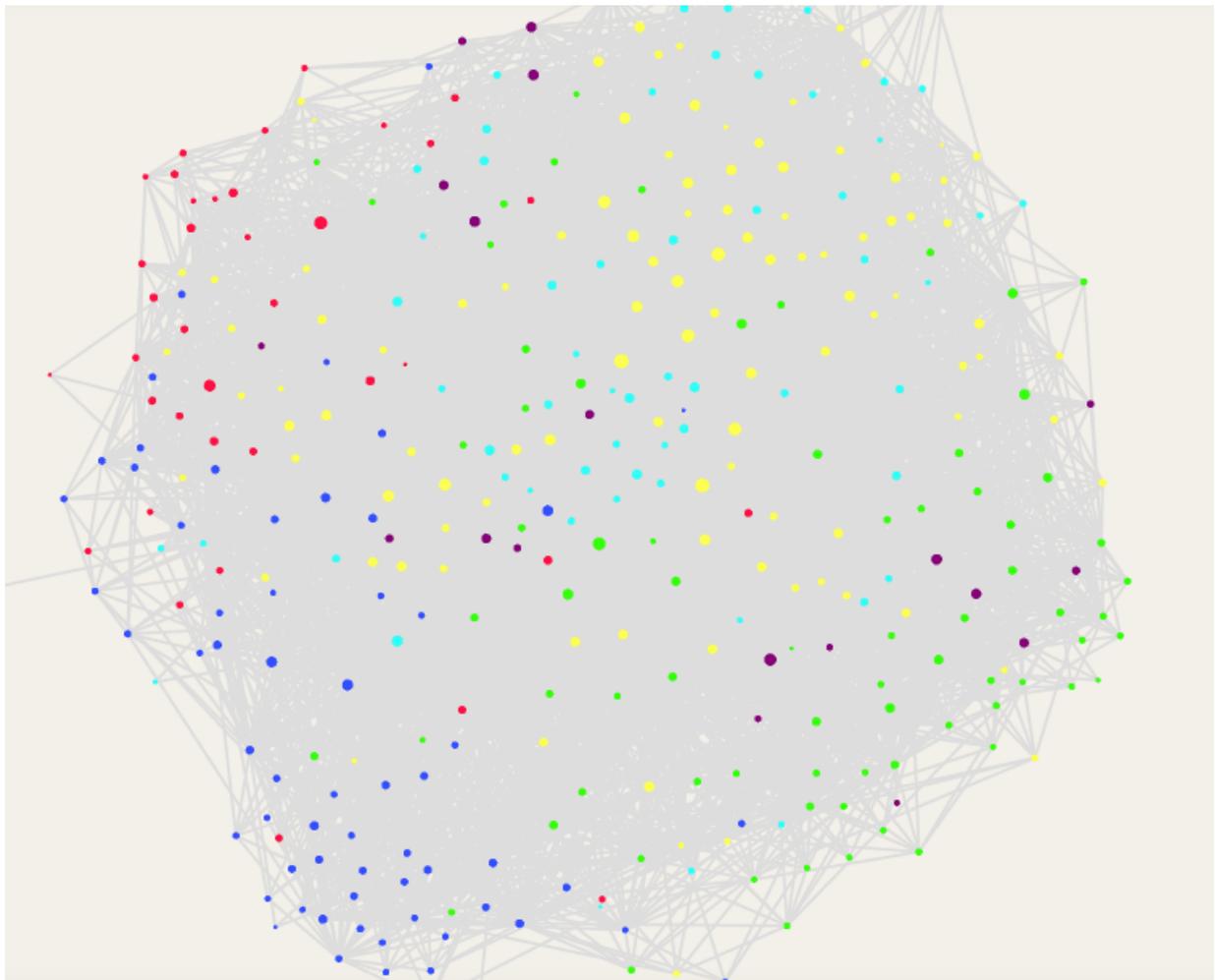
### **The growing privatization of telecommunications network**

In many respect, Foy and Gasparin fought a rear-guard battle. From the 1840s on, the development of the electrical telegraph would accelerate national and transnational communications flows, as the industrial revolution spurred the demand for communications. By the end of the 19<sup>th</sup> century, private corporations did not only made extensive use of the telegraph and of the new communication technology of the time, the telephone, but also played a growing role in the construction and management of national and international infrastructures (Barty-King, 1980; Headrick, 2012).

Fast-forward 150 years. Neo-liberal policies launched in the 1980s have dismantled the public and private monopolies over telecommunications networks. After the powerful telecommunications corporations and media industries, the “Internet revolution” has given way to a new generation of private actors who exert unprecedented power over transnational computer networks. Despite the early cyberlibertarian hopes – as the late countercultural icon John Perry Barlow wrote in 1996 at the address of world governments, “you have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear” (Barlow, 1996) – states have found ways to transpose their traditional techniques of power to the digital realm (Goldsmith & Wu, 2006). And when they do – for instance to engage in the large-scale monitoring of Internet communications – they do so in interaction with many private actors who own parts of the multi-layered architecture of global communication networks.

## Private actors in post-Snowden controversies

Beyond the role of private actors in these secret surveillance practices, many private companies also engage in the debates regarding state security practices and their impact on the digital ecosystem. For one, the Snowden controversies unleashed in June 2013 show the various types of actors mobilized around these issues. At the early stage of the UTIC project, we undertook a Web cartography of post-Snowden controversies, using a Web-curation tool developed by Sciences Po's Medialab (Jacomy, Girard, Ooghe, & Venturini, 2016).



Web cartography of actors mobilised in post-Snowden controversies. Private actors are in the upper-left corner in red color. Explore online at: <https://frama.link/A3W9CoY>

In these controversies on Internet surveillance, various categories of private actors got involved. As a starting point, we chose to regroup them in the following, rather classical topology:

- Multinationals firms of the digital economy, whether there are US-based Information Technology (IT) firms, large platforms or hosting providers collecting vast amounts of data, or telecom operators. They appear as both actors and targets of these controversies, as they are pointed out for their participation in state surveillance apparatuses.

- National and regional digital economy companies (again, online services, hosting and access providers) offering alternative services to those pointed out as exposed to the NSA and other Five-Eyes surveillance programs.
- Cybersecurity providers, who took the opportunity of the Snowden disclosures to promote their services and other technical counter-measures to companies and public institutions willing to better protect their data assets from spying and surveillance.
- Trade groups and lobbies, engaged in negotiations with public authorities, either with the goal of enacting reforms of applicable surveillance or of calling for tougher cybersecurity policies to protect “digital sovereignty”.

## 1.1 Goal of the deliverable

One needs to take these categories with care. They tend to obscure the complex power struggles not only between these sub-sectors but also within them (Bourdieu, 2014b). Their agents are engaged in multi-faceted distinction strategies that need to be traced to understand how post-Snowden debate on surveillance has impacted them.

In first analysis, it looks like the controversies unleashed by the Snowden documents deeply affected the power relationships between the various actors involved in or mobilized around state surveillance practices. For private actors – and especially the US-based multinational online service providers, software editors and online platforms on which this deliverable focuses –, it first seemed as if the debate has significantly undermined the influence of intelligence agencies on a significant part of various private actors of the digital economy, while investigative journalists, lawyers and human rights defenders in various Non-Governmental Organizations (NGOs) and politicized hackers and engineers saw a boost in their ability to influence these actors. But as this deliverable will show, the situation is actually more nuanced and varies depending on the countries, sub-sectors of the digital economy and the very companies under consideration.

To account for this complexity, we need to understand why, in a given context, some companies choose to collaborate with intelligence agencies, while others are more inclined to resist getting implicated in state surveillance apparatus. To that end, we need to identify the factors that are likely to influence the stance of a given company and its evolution depending on the changing context and constraints that it faces across time and space. But before we delve in this analysis, let us give an overview of the existing literature most relevant to our task.

## 1.2 Brief literature review

Our analysis of post-Snowden conflicts between private actors involved in the digital economy and states draws from, and hopes to contribute to, two main streams of literature.

### **The public-private distinction in critical security studies**

The first important stream comes from political science and international relations. An important reference in this regard is Tim Mitchell’s *Limits of the State* (1991). This seminal article was written in reaction to post-Marxist conception of the state which were influenced by cybernetics and offered to think of the “political system” (rather than the state) as an information processing apparatus (see,

e.g., Easton, 1957), or which – from the late 1970s on – purported to “bring the state back in” by focusing on decision-making processes. Mitchell aimed at offering a third way, going back to the crucial and difficult question of the boundary between society and the state. According to him,

“the elusiveness of the state-society boundary needs to be taken seriously, not as a problem of conceptual precision but as a clue to the nature of the phenomenon. Rather than searching for a definition that will fix the boundary, we need to examine the detailed political processes through which the uncertain yet powerful distinction between state and society is produced” (idem, p. 78).

Accordingly, Mitchell calls for studying the state not “as a free-standing entity, whether an agent, instrument, organization or structure, located apart from and opposed to another entity called society”, but rather as a multiplicity of political arrangements that produce structural effects that maintain social and political order. From this perspective, “the boundary of the state is merely the effect of such arrangements and does not mark a real edge. It is not the border of an actual object (idem, p. 94). Rather, “producing and maintaining the distinction between state and society is itself a mechanism that generates resources of power.” Delving on the relationship between public administrations and private sector organizations like energy multinationals or private banks, Mitchell however goes on to caution that:

“The approach to the state advocated here does not imply an image of the state and private organizations as a single, totalized structure of power. On the contrary, there are always conflicts between them, as there are between different government agencies, between corporate organizations, and within each of them” (p. 90).

Mitchell’s response builds on the work of French theorists like Bourdieu and Foucault, to whom we will get back in the conclusion of this report. But to sum their influence, both offered new ways for questioning taken-for-granted notions like the state and, as a consequence, develop a more complex understanding of power relations. Mitchell’s approach takes up Foucault’s invitation to study the “state” as power practices rather than through – mostly legal – concepts deriving from the “state’s internal rationality”. It also echoes the work of Pierre Bourdieu, who approximately at the same time as Mitchell as questioning the limits of the state, was giving his “On the State” lectures at the *College de France* between 1989 and 1992, in which he for instance stressed that “the state (...) is not a bloc, it is a field” (Bourdieu, 2014a).

This line of thinking became increasingly influential as the sub-field of critical security studies emerged from the mid-1990s on (Peoples & Vaughan-Williams, 2010). With the rise of security privatization in the context of neo-liberal economic policies and given the opposition to these processes, a growing number of scholars paid attention to the public-private distinction (Abrahamsen & Leander, 2015). Subjects like the role of private security guards, the role of private companies in the logistics of military forces, subcontractors in the intelligence field all became part of a growing field of inquiry which, in its critical component, aimed at questioning the public-private distinction. For instance, looking at private security firms, Abrahamsen and Williams, argued that “the significance and impact of security can only be understood by moving beyond the public-private distinction, with the recognition of how these distinctions are being reconfigured into networks and practices indicative of new relations of power” (Abrahamsen & Williams, 2010).

Against those insisting that the privatization of security was one more evidence of the weakening of

traditional state sovereignty, the authors argued that “privatization is not a challenge to prevailing structures of authority, but is embedded in, and inseparable from, transformations in governance.” Looking at laying new theoretical foundations for understanding how private security is historically and socially constituted, the authors introduce the concept of “global security assemblages”:

“[Global security assemblages are] transnational structures and networks in which a range of different actors and normativities interact, cooperate and compete to produce new institutions, practices and forms of deterritorialized security governance” (p. 90).

The notion of “assemblage” here refers to the way security governance is increasingly achieved through fluctuating arrangements of networks of state, corporate and voluntary actors. As other authors drew the notion of assemblage to other theoretical foundations (e.g. deleuzian like (Haggerty & Ericson, 2000), Abrahamsen and Williams ground it in Bourdieu’s notion of “fields” to highlight the evolution of material, symbolic and cultural forms of capital within the security field. Rather than the erosion of state power highlighted by some theorist of globalization, their approach builds on Saskia Sassen’s concept of “disassembly” to highlight the fact that assemblage is actually a *process* whereby some components of state are configured in new power structures as formerly public functions are transferred to the private sector.

To come back to the role played today by large technology companies in the field of state surveillance, there nothing “natural” or “normal” about it. This is what the historical anecdote that opens up this report helps us remember. But at a more theoretical level, the public-private category – which has become a central theme in security studies (Williams, 2010),– also helps see ongoing processes in a way that can teach us something about the changing nature of state power.

### **Surveillance and the political economy of the digital**

Our research topic can also be situated in the history of public-private hybridization in the development and use of information and communication technologies. From the work of Edwin Black on the role of IBM in the Holocaust (2012) to Christophe Lécuyer’s history of Silicon Valley (2007) and approaches anchored in political history (Mattelart, 2010), political economy (Foster & McChesney, 2014) but also journalistic inquiries that take a historical perspective (Harris, 2014; Levine, 2018), many references point to the World War II and Cold War origins of the computer industry and of today’s surveillance society.

These histories of US technology industries are complemented by critical approaches at the intersection of political theory and political economy. Among them, some insist on breaking away with the naive conception of the network society as being abstracted from capitalism, instead pointing to the continuity between contemporary actualization of capitalism and previous periods (McChesney, 2013; Schiller, 2000). Dan Schiller refers to the “digital capitalism” to:

“point to a new phase change in a five-hundred-year history that has been marked by abiding tendencies: capital's continually extended use of wage labor, its search for new and often contested side of commodification, and its episodic crises, wherein rampant financial speculation triggers a fall into depression and economic stagnation” (Schiller, 2014)

Building on these analytical corrections, other authors aim to complement what are seen as shortcomings in surveillance studies. In his work on surveillance, Christian Fuchs for instance

underlines the the general lack of consideration of Marx's work in surveillance theories (Fuchs, 2013). Against Anthony Giddens' claim that Marx ignored surveillance altogether, the author shows that for Marx, both economic and state surveillance played a key, complementary role by sustaining the capitalist logic of capital accumulation. At the theoretical level, he argues that the notion of accumulation can help unify various approaches of surveillance. He ends by underlying that although capitalism and the rise of the bourgeois class led to the separation of the private and the public spheres and hence of the notion of privacy, the latter is constantly threatened by capitalism: “An antagonism between privacy ideals and surveillance is therefore constitutive for capitalism.”

Exploring these contradiction in the context of social media platforms, Fuchs and Trottier further stress the significance of social media in the history of surveillance (Fuchs & Trottier, 2015). For them, online social media represent the first type of media to bring together three forms of sociality (cognition, communication, cooperation) and the various social roles or identities taken by social actors in the different structures of social life (state, the economy and culture, and the intersection of these three spheres with the civil society). The boundaries between these different spheres of social life becomes more liquid as communicative action is absorbed in a single profile on integrated socio-technical platforms, who have commercial incentives to collect the most extensive amount of data about their users. According to the authors, the convergence of these commercial social media and state policing has three major implications: the rise of categorical suspicion, increased social sorting and the normalization of surveillance.

Coming from a background in psychology and economics, Shoshana Zuboff has also taken up the notion of “surveillance capitalism” coined by Bellamy Foster and McChesney (2014) to point to a new evolution of capitalism, whereby data extraction and analysis become a new managerial paradigm wielding a new form of power alien to democratic institutions. According to Zuboff:

“Surveillance capitalism is immune to the traditional reciprocities in which populations and capitalists needed one another for employment and consumption. In this new model, populations are targets of data extraction. This radical disembedding from the social is another aspect of surveillance capitalism’s anti-democratic character” (Zuboff, 2015).

Of course, as this report will show, the very logic of surveillance capitalism runs through other institutional spheres. As David Lyon writes, “not merely have the technolgies of surveillance been hugely upgraded, but surveillance practices are also common to all organizations” (Lyon, 2015), and not least those associated with the security field.

## **1.3 Methodology**

Building on this background, we have adopted a interdisciplinary methodology in this report, by mixing political sociology, Science & Technology studies as well as policy and legal analysis to understand the strategies of large technology companies – and more specifically US tech companies – in the post-Snowden context.

In the second part of the report, where we describe and analyze these strategies by looking at specific episodes to underline variations, we draw on the methodological toolbox of contentious politics, a sub-field of political sociology (Tilly & Tarrow, 2015). By “episodes”, we mean “bounded sequences of continuous interaction, usually produced by an investigator’s chopping up longer streams of contention into segments for purposes of systematic observation, comparison, and

explanation” (p. 39).

To analyze these episodes and track the continuities and changes in the relationship between state actors and private companies with relation to Internet surveillance, we use public positions as expressed or relayed in the media, public hearings, official reports, blog posts. We also look at statements produced as part of national reforms of legal rules attached to intelligence and surveillance, as well as court cases on these issues. Finally, when useful, we also resort to the Snowden archive, look at the technical deployments and offer legal analysis when they help shed light on the strategies of these companies or of state actors.

This desk research is complemented by five interviews, almost all with senior corporate affairs executives in leading US technology companies. Questions asked during interviews touched on:

- the internal dimension of the post-Snowden debates, that is how they affected the way Internet companies approach issues related to Internet surveillance internally, internal procedures surrounding sensitive political matters, policy priorities, etc.
- the relationship of policy officers tasked with handling issues related to security and law enforcement with their counterparts in other companies, or privacy advocates working for advocacy groups, NGOs, etc.
- the effect of post-Snowden debates on the relationship of these firms with states, how they dealt with post-Snowden privacy claims, securization strategies used by state officials to promote greater cooperation between Internet firms and law enforcement and intelligence agencies, etc.

During these semi-structured interviews, conducted in various settings (privately over-the-phone or during a dedicated public conference), we sought to get a better understanding of the power dynamic at play in the contentious episodes that we were studying, try to go beyond the veil of secrecy and public-relation strategy put forth by these actors. Although we were not always successful, in some cases we were able to obtain information that shed new light on behaviors and strategies that were hitherto hard to explain. The internal workings of multinational companies – all the more when we specifically consider their dealings with intelligence and law enforcement agencies – remain for the most part secret, and more time and resources would have been necessary to benefit from more extensive “insider knowledge”.

## **1.4 Research Questions & Outline**

Through this report, we sought to answer several research questions:

- The most significant one relates to how the strategies of major Internet firms are debated and decided upon, to locate the spaces of struggles that determine whether a given company in a given context to decide where that company should fall on the cooperation-resistance (to participation to secret state surveillance) axis. We started from the premise that these spaces are disseminated across several social spaces, some internal to the companies or the digital economy sector, some external and occupied by state actors and security professionals, or human rights defenders and privacy advocates, across which senior policy officers in these companies navigate.

- Beyond the spaces and the “where”, we wanted to know “why”, that is what are the factors determining whether these companies collaborate or resist to surveillance; and more specifically what are the effect of the proximity (or lack of thereof) of Internet firms with security professionals on the strategies of the various actors engaged in the controversies. Here, variations can be temporal or spatial, evolving across time or changing depending on which country/region is considered.
- Beyond observable behaviors, this research sought to provide evidence of the fact that the field of state surveillance is exposed to particular effects resulting from it also being a stage, a place where a significant part of the struggle is a public one, relayed by major media outlets. This publicity shapes the actors' strategy, and our analysis will aim to locate instances of “double-dealing”, that is cases “whereby leaders, managers, officials or delegates of a field appear to be acting in a disinterested or principled manner 'for the field' and its values” but are actually serving their own interests (Webb, Schirato, & Danaher, 2002).
- Finally, and perhaps most importantly, this deliverables looks at “post-Snowden surveillance debate” as one of the many battle fronts of a process whereby modern states and associated practices of power are being reconfigured through their relationships with private sector technology firms. In other words, through various assemblages in which the forms of capital associated with surveillance capitalism gain a higher status in the administrative field, the “regimes of surveillance” championed by firms like Google or Facebook have structural effects that reconfigure the political arrangements that we call the state.

To investigate these questions, we first offer some hypothesis on the “constraint structure” in which large Internet firms evolve. Then, as a way to test these hypothesis and showcase variations in the outcomes of post-Snowden contention of the strategies of these companies, we track several episodes of contention that are reconfiguring the public-private security assemblages in the field of state surveillance in the aftermath of the Snowden disclosures in the US and in France. In the concluding section, we go back to history and political theory to gather key takeaways regarding contemporary public-private assemblages tasked with controlling information flows.

## 2. Hypothesis on the Constraint Structure of Large Internet Firms in Debates on State Surveillance

To begin our inquiry, we propose a “constraints structure” regarding the factors that influence how a firm will fall in the cooperation/resistance spectrum. Based on prior knowledge and working in an inductive approach inspired by “Grounded Theory” (Glaser & Strauss, 1999), we have refined a set of working assumptions. These interdependent factors are exemplified by facts and anecdotes and are aimed at working as a heuristic model as we begin to explore some of our research questions.

### 2.1 Internal corporate culture

“Don’t be evil”. Google’ historic, and naive, company motto is but one illustration of the fact that Silicon Valley public-facing companies built on an image of liberty and altruism historically attached to Internet technologies. As Barbrook & Cameron wrote in their seminal article on the *The Californian Ideology*, this credo is characterised by a “a mix of cybernetics, free market economics, and counter-culture libertarianism” (Barbrook & Cameron, 1995). Even today, according to Christopher Soghoian, a senior policy analyst studying surveillance technologies at the American Civil Liberties Union, “even though they have an awful reputation on consumer privacy issues, when it comes to government privacy, they generally tend to put their users first”. “There’s this libertarian, pro-civil liberties vein that runs through the tech companies.”<sup>1</sup>

On June 6<sup>th</sup> 2013, The Washington Post and The Guardian released articles, respectively written by Laura Poitras and Glenn Greenwald, revealing the existence of the PRISM program. Greenwald’s article opened with the following lines: “The National Security Agency has obtained direct access to the systems of Google, Facebook, Apple and other US internet giants, according to a top secret document obtained by the Guardian.”<sup>2</sup> The article stressed that “although the [NSA’s] presentation claims the program is run with the assistance of the companies, all those who responded to a Guardian request for comment on Thursday denied knowledge of any such program.” And indeed, the companies denied the existence of “direct access” of the NSA or the FBI to their servers. They claimed to be following the law, but that they had never heard of such a programme.

For them, the PRISM disclosure opened a long sequence during which through public relations and change in corporate practices, they sought to distance themselves from the US establishment. But although it remained veiled by secrecy, there were also signs that the revelations provoked strong distress from within these companies, with many of their employees being puzzled and shocked to hear that they could indirectly be taking part in the surveillance apparatus on which investigative journalists were shedding light. One of our interviewees, who was working at Yahoo at the time, remembers the suspicious look of many of its colleagues at the time:

“Something I mostly remember is a lot of shock, a lot of e-mails, a lot of phone calls, from colleagues, from friends asking “what is it exactly you're doing?” Perhaps a weird

---

1. Quoted in Miller, C. C. (2013, June 13). Secret Court Ruling Put Tech Companies in Data Bind. *The New York Times*. Retrieved from <http://www.nytimes.com/2013/06/14/technology/secret-court-ruling-put-tech-companies-in-data-bind.html?pagewanted=all>:

2. Greenwald, G., & MacAskill, E. (2013, June 13). NSA Mines User Data of Facebook, Google and Others. Retrieved March 13, 2018, from <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>

look from other teams saying, “well, is it actually legal what you are doing on the fifth floor?”. So, a lot of questions, [as I was] struggling to reconcile what I was reading in the press and what I was actually doing” (Appendix 1).

In a sector whose corporate culture is marked by what Boltanski and Chiapello have called the “new spirit of capitalism” (Boltanski & Chiapello, 1999) and that base their public image on the emancipatory potential of new technologies, these revelations may have caused a form of cognitive dissonance. Whether we consider lawyers and other legal workers whose task is to craft and advertise the privacy policies of these companies while balancing human rights with antagonist business objectives, or engineers who identify themselves with the politicised branch of the hacker movement (Coleman, 2011), it is likely that such personnel will exert a form of pressure on the company’s leaders to push for policies that can better respect the rights of their users. This is all the more true that public advocates like Snowden himself tried to stir the political conscience of engineers and computer scientists across the digital sector in his public appearances.<sup>3</sup>

In a more recent illustration, the partnership between the US Department of Defense and Google to provide solutions aimed at analysing drone footage also sparked discontent internally.<sup>4</sup> During a speech in the Fall of 2017, Eric Schmidt, then still Executive-Chairman at Google-Alphabet, explained that “there’s a general concern in the tech community of somehow the military-industrial complex using their stuff to kill people incorrectly.”<sup>5</sup>

## 2.2 Pressure from human rights field

One of the first elements likely to influence the cooperation-resistance of companies providing some forms of public utilities is the pressure exerted by public groups devoted to the protection of human rights. In the US, the aftermath of the first Snowden disclosures, NGOs like the Electronic Frontier Foundation, which have historically nurtured strong ties with Silicon Valley companies, engaged in various strategies aimed at pushing them to adopt resistance strategies, for instance by beefing up their encryption standards.

These episodes where private companies are exposed to pressure from the human rights field can have a lasting impact on their stance and position vis-à-vis law enforcement. If a company has a record of handling human rights scandal, it is more likely to have developed internal procedures and codes of conduct aimed at pursuing their business interests while conforming to international human rights standards.

One interesting example is Yahoo. The Snowden disclosures revealed that, in 2007, Yahoo resisted its enrolment into the PRISM programme. In front of the Foreign Intelligence Surveillance Court (FISC), the company argued that it should be able to offer some transparency to its users on the amount of data handed over to the FBI by virtue of so-called National Security Letters, which went against the no-disclosure requirements. The stand-off eventually led the FBI to threaten Yahoo of a

---

3. See, e.g.: Couts, A. (2014, March 10). Edward Snowden at SXSW: Encryption is the answer to NSA surveillance. Retrieved February 17, 2018, from <https://www.digitaltrends.com/web/edward-snowden-sxsw-2014-speech-live/>

4. Conger, K. (2018, March 6). Google Is Helping the Pentagon Build AI for Drones. Retrieved March 9, 2018, from <https://gizmodo.com/google-is-helping-the-pentagon-build-ai-for-drones-1823464533>

Conger, K. (2018, May 14). Google Employees Resign in Protest Against Pentagon Contract. Retrieved 15 May 2018, from <https://gizmodo.com/google-employees-resign-in-protest-against-pentagon-con-1825729300>

5. Quoted in: Conger, K. (2018, March 6). Google Is Helping the Pentagon Build AI for Drones. Retrieved March 9, 2018, from <https://gizmodo.com/google-is-helping-the-pentagon-build-ai-for-drones-1823464533>

\$250 000 fine per day for its non-compliance and to a legal challenge on which we will come back.<sup>6</sup>

So a puzzling question is: what are the factors that can help explain such a resistance? At this stage, these are just hypothesis, but it is worth noting that in 2005, Yahoo became embroiled an intense scandal when the company chose to hand over personal information it held over a Chinese dissident named Shi Tao, leading to Shi's arrest, incarceration and subsequent condemnation to a 10-year jail term. This episode turned into a public relation disaster. In 2006 and 2007, it led to litigation and public hearings at the US Congress. In front of a panel where members attacked Yahoo's co-founder Jerry Yang, accusing the companies executives of being “moral pygmies” and asking them to “beg for forgiveness” to Shi's mother who was in attendance on that day.<sup>7</sup> Parallels were also made by Congress members with the Holocaust.

During this episode, Yahoo pledges to be working with human rights organizations on an industry code of conduct aimed at protecting human rights. It would eventually lead to a pan-industry commitment to joining the Global Network Initiative. According to one of our interviewees who worked at Google:

“Yahoo! was the first company to implement a program that was a Human Rights program, so you had a department within the company where you would have called some people that were hired to review a lot of the policy decisions on data, on surveillance, some on advertising, depending on the exact scope, to think about all those issues from a Human Rights angle in a systematic way” (Appendix 1).

What is for sure is that by the time the FBI required Yahoo to join the PRISM programme, the company had been embroiled in a hard-hitting scandal and many of its lawyers and executives were necessarily very sensitive to the human rights implications of collaborating with law enforcement and intelligence agencies, and were in a strong positions to plead for resistance.

But the case of Yahoo also illustrates how rapidly these strategies can shift. Eventually, Yahoo lost its case before the FISC and in the first 10 months of 2013, Yahoo users were the most targeted in the combined requests sent by both the NSA and the FBI.<sup>8</sup> Also, in 2016, Reuters reported based on testimonies by inside sources that the board of the company had responded favourably to a request of the NSA to install a scanning device on its data centers to monitor the content of messages. The Chief Technology Officer was not informed of this operation and allegedly resigned when he became aware of the scheme (see below).<sup>9</sup>

## 2.3 User trust and business stakes

Companies operating in competitive markets, even when they are in dominant positions, are usually more dependent on the trust of their users. This is all more true in the digital sector where, as teams at Google are used to say, “competition is just one click away”.

---

6. Zetter, K. (2014, September 11). Feds Threatened to Fine Yahoo \$250K Daily for Not Complying With PRISM. Retrieved March 13, 2018, from <https://www.wired.com/2014/09/feds-yahoo-fine-prism/>

7. AP, (2007, November 7). Yahoo Criticized in Case of Jailed Dissident. *The New York Times*. Retrieved from <https://www.nytimes.com/2007/11/07/technology/07yahoo.html>

8. Kelion, L. (2014, February 4). Tech firms detail NSA-FBI demands. *BBC News*. Retrieved from <http://www.bbc.com/news/technology-26031092>

9. Reuters. (2016, October 4). Yahoo secretly scanned customer emails for US intelligence-sources. Retrieved October 5, 2016, from <http://www.reuters.com/article/us-yahoo-nsa-exclusive-idUSKCN1241YT>

At the peak of the Snowden controversy, leaders of the US digital sector became wary of the impact of the revelations on their short-term and long-term business prospects. Groups like EFF were informing the public about alternatives to dominant services through its “PRISM break” website, documenting of the free software, decentralized alternatives to dominant services.<sup>10</sup> Abroad, other large companies and public officials were stressing the need for national institutions and critical service and infrastructure providers to review their data management policies, and move away from US-based providers and relocate their data – an attempt at restoring “digital sovereignty” that has been denounced as “digital nationalism” by critics (Chander & Lê, 2015; Bauer, Lee-Makiyama, van der Marel, & Verschelde, 2014; for a critique of arguments in favour of digital nationalism, see Kuner, 2015).

For the computing and IT industry, this caused much concern. Think tanks and trade groups in Washington drafted reports on the potential financial losses of the Snowden debacle.<sup>11</sup> Companies like Google and Facebook insisted on the importance of restoring their “users' trust” and staged their commitment to protecting their users' rights. Their initial reaction was to denounce a misrepresentations and exaggerations in the commentaries offered on PRISM (as Google's CEO and Chief Legal Officer wrote at the time, “the U.S. government does not have direct access or a “back door” to the information stored in our data centers. We had not heard of a program called PRISM until yesterday.”).<sup>12</sup> They also claimed that they followed legal procedures (“we provide user data to governments only in accordance with the law. Our legal team reviews each and every request, and frequently pushes back when requests are overly broad or don't follow the correct process”). And finally, they asked for more transparency (“this episode confirms what we have long believed—there needs to be a more transparent approach”), and even staged these demands(Google's Chief Legal Officer, David Drummond, wrote an open letter to the offices of the Attorney General and the Federal Bureau of Investigation asking for transparency on the number of National Security Letters it received, and what data was served in response).<sup>13</sup> As one Microsoft interviewee puts it:

“The question of trust really went on the top of the discussion with the customers, with the government (not only the agencies but also the policy-makers), because at that time they realised that this question of trust could impact a lot the development of technology across the world” (Appendix 1).

But business interests can also push a company to indirectly cooperate with law enforcement, by providing new avenues for surveillance. For instance, Web 2.0 around 2005 and the “movement of the cloud” prominent around 2010 were not only a marketing phenomenon, but also an industry trend that led major Internet firms to concentrate hosting capacities (Mosco, 2014), thus theoretically reducing the transaction costs associated with state surveillance (law enforcement agencies have fewer actors to whom they can send request, allowing for smoother processes). Today, so-called “Big Data”, “Artificial Intelligence” and “Machine Learning” represent new technical and business paradigms for which companies in the IT sector invest a lot of money in

---

10. See <https://prism-break.org/en/>

11. See, e.g., Bauer, M., Lee-Makiyama, H., van der Marel, E., & Verschelde, B. (2014). *The Costs of Data Localisation: Friendly Fire on Economic Recovery* (ECIPE Occasional Paper No. 12). Brussels: European Centre for International Political Economy. Retrieved from [http://www.ecipe.org/app/uploads/2014/12/OCC32014\\_1.pdf](http://www.ecipe.org/app/uploads/2014/12/OCC32014_1.pdf)

12. Drummond, D. (2013, June 11). Asking the U.S. government to allow Google to publish more national security request data. Retrieved March 13, 2018, from <https://googleblog.blogspot.com/2013/06/asking-us-government-to-allow-google-to.html>

13. Idem.

R&D.<sup>14</sup> By doing so, they nurture innovations that will be appropriated by law enforcement and intelligence agencies for their surveillance apparatuses. Research & Development is a major locus of the hybridization of public and private actors in the security field, and holds a prominent place in the history of the Internet (Levine, 2018).

## 2.4 Regulatory stakes

A series of regulatory stakes can also be a factor determining the room for manoeuvre of Internet firms. Multinational companies in the digital economy are indeed exposed to a number of regulatory stakes that can push them towards cooperation with state surveillance actors (McChesney, 2013).

For instance, such cooperation can be a way to gain backing and support from public authorities on regulatory issues that are seen as key for the company. Large players in the digital economy are particularly exposed to antitrust legislation and more generally competition law, but also to issues such as taxation, copyright law, privacy standards, etc.

At the international level, attention to regulatory stakes can also enable various forms of support, be it diplomatic backing in the context of trade negotiations (Powers & Jablonski, 2015) or even more simply access to relevant intelligence. For instance, in the context of the negotiations on the EU-US Privacy Shield, which regulates the transfer of personal data belonging to EU citizens from Europe (point of collection) to the US (point of storing), the US Department of Commerce defended the interests of the US digital sector, and likely developed its negotiating strategies in close partnerships with the leading corporations of the digital sector.

## 2.5 Identification to and dependency on power elite

In trying to understand the likelihood of a given company to resist to or cooperate with state surveillance, an important question to consider is the sociology of its stakeholders and chief executives.<sup>15</sup> Silicon Valley firms have a reputation of having leaders that are overtly defiant of traditional political circles, and sometimes stage a West Coast / East Coast opposition.<sup>16</sup> And as soon as cooperation leads to loss in user trust and starts undermining a company's financial prospects, stakeholders and investors might also push towards resistance, especially when there is public pressure coming from the human right field.

One interesting hypothesis that can't be explored in the context of this deliverable is whether the opening of a company's stock to external and institutional investors reinforces the incentive for cooperation, and/or a move towards a more traditional type of management, with executives that

---

14. Levy, S. (2016, June 22). How Google is Remaking Itself as a “Machine Learning First” Company. Retrieved June 29, 2016, from <https://backchannel.com/how-google-is-remaking-itself-as-a-machine-learning-first-company-ada63defcb70#.9cckskrs9>

15. Pour rappel : en décembre 2014, dans les entreprises citées dans PRISM, nombre d'entre elles se situaient dans le peloton de tête des plus hautes valorisations boursières de l'économie américaine. Apple, qui aime rappeler ses origines contre-culturelles, détient ainsi la première place, suivie de près par Microsoft (3ème) et Google (4ème).

16. For instance, regarding Apple, see: Lesne, C. (n.d.). Tim Cook et les « valeurs » de la Vallée. Retrieved February 26, 2016, from [http://www.lemonde.fr/ameriques/article/2016/02/25/tim-cook-et-les-valeurs-de-la-vallee\\_4871702\\_3222.html](http://www.lemonde.fr/ameriques/article/2016/02/25/tim-cook-et-les-valeurs-de-la-vallee_4871702_3222.html)

Panzarino, M. (2015, June). Apple's Tim Cook Delivers Blistering Speech On Encryption, Privacy. Retrieved June 15, 2015, from <http://social.techcrunch.com/2015/06/02/apples-tim-cook-delivers-blistering-speech-on-encryption-privacy/>

Romm, T. (2015, August 27). Apple Takes Washington. *Politico Magazine*. Retrieved from <http://www.politico.com/magazine/story/2015/08/tim-cook-apple-washington-politics-121821>

have been socialized in the same milieu as administrative and political elites. This is for instance a point made by WikiLeaks founder, Julian Assange, regarding Google/Alphabet's Eric Schmidt and other senior executives at Google, whose professional or personal trajectories are closely intertwined with personnel of the US State Department (Assange, 2014). This is also something pointed out Frank Pasquale, who points out that “the Silicon Valley, the highest financial sphere in New York and the pinnacle of military intelligence form a block that is increasingly unified” (Pasquale, 2015). We will come back to this issue later on. For now, let us mention some of the factors that may push for greater interdependencies between the tech industry and the state's security apparatus.

## 2.6 Firm's dependence on public procurements

A firm's final decision on whether or not to collaborate might depend on how much of its revenues are dependent on public tender tied to the defense and security sector. Such business dependency is true of companies that have developed a strategy for “large accounts” customers – for instance, Microsoft extracts around 2bn euro from European public-sector entities every year –,<sup>17</sup> and who are regular bidders for technology-related public tenders. For instance, in October 1992, during the first so-called “Crypto War”, as AT&T was about to market its first publicly-available telephone terminals equipped with encryption features, the head of the FBI, was able to call AT&T's CEO to offer a him a deal: Rather than use the encryption system developed by AT&T's own engineers, Sessions proposed that the telco giant instead use a system developed by the NSA and the National Institute of Standards and Technology (NIST) – a system that would become known as the “Clipper Chip” (Levy, 2001). The FBI's key asset in this bargain was of course the purchasing power of the state, as AT&T was then renegotiating a contract with the federal government that was worth over \$10bn. More recently, in 2007, a former Qwest Communications International executive alleged that the government retaliated to the company's refusal to join a surveillance program by revoking opportunities for hundreds of millions of dollars (the government refused to comment on the executive's allegations).<sup>18</sup>

But such dependence is not only true of large multinationals. Small tech companies – some of which appear in our graph – can also become strongly related to national security professionals. In the surveillance field, it is particularly the case of smaller companies providing software analytics solutions, like Qosmos or Palantir, or even SMEs infused with a particular “hacker ethos” and specialized in the trade of software vulnerabilities, like HackingTeam or Vupen, or in “spyware” devices. Because of their technical know-how, these companies have developed strong relationships with some of the most powerful intelligence agencies. We can assume that such mutual dependency results overtime to an homogenization of the involved actors' dispositions.

Another important aspect to the emergence of a “surveillance-industrial complex” (Ball & Snider, 2014) is the role of the army and intelligence community in developing or funding technologies that will become key assets for US firms. In other words, they do not act only as provider of technology with the government, but the later can use federal R&D budgets and other funding programs to act a

---

17. Schumann, H., & Simantke, E. (2017, May 13). Europas fatale Abhängigkeit von Microsoft. Retrieved February 13, 2018, from <http://www.tagesspiegel.de/weltspiegel/sonntag/cyber-attacken-auf-staatliche-it-europas-fatale-abhaengigkeit-von-microsoft/19628246.html>

18. Shane, S. (2007, October 14). Former Phone Chief Says Spy Agency Sought Surveillance Help Before 9/11. *The New York Times*. Retrieved from <https://www.nytimes.com/2007/10/14/business/14qwest.html>

prescriber and incubator of relevant technologies. One oft-cited example in this regard is the Central Intelligence Agency (CIA)'s venture capital firm In-Q-Tel.<sup>19</sup> Another example is the NSA's Technology Transfer Program (TTP), which is part of the Office of Research and Technology Applications. The program is used to make technologies like firewalls, new cryptology tools and other technologies available to the private sector. The NSA says that the TTP has contributed \$346 million to the US' GDP in the past decade, and has created around 1 300 jobs.<sup>20</sup> Of course, these trends are not specific to the US. For instance, in the EU, R&D reserarch programmes are also a major locus of public-private hybridization in security policiy (Bigo, Jeandesboz, Martin-Mazé, & Ragazzi, 2014; Siokas, 2018).

## 2.7 Criminal sanctions

The last factor is a tool that states can use to force cooperation, namely criminal sanctions targeting tech companies who would refuse to comply.

In the US, failure to abide to surveillance request – conveyed either through a National Security letter or a FISA court order – is punishable by law, as companies like Yahoo and Lavabit have come to know. The FISC's rule of procedure provide that “if a person or entity served with a Court order (the "recipient") fails to comply with that order, the government may file a motion for an order to show cause why the recipient should not be held in contempt and sanctioned accordingly.”<sup>21</sup> Dissuasive fines may be imposed, but jail sentences are also theoretically in order.<sup>22</sup>

Companies might react differently to the possibility of being found in “contempt of court” and threfore sanctioned, but the likely outcome is obedience. Although an appeal to the Foreign Intelligence Review Court (FISCR) is possible, such appeals are rare. As of 2008, only two rulings has been issued by the court, the second of which resulted from Yahoo's insistence. According Judge Reggie Walton – the presiding judge of the FISA court who wrote in July 2013 a lengthy reply to questions by Congress members –, this is was the first and only time that a company had ever argued before the FISCR.<sup>23</sup> This was to no avail, however, as the FISCR asserted the constitutionality of the Protect America Act of 2007's provisions that lifted the warrant requirement for the surveillance of foreign intelligence targets “reasonably believed” to be outside the United States).<sup>24</sup> According to the judge:

“ Notwithstanding the parade of horribles trotted out by the petitioner, it has presented no evidence of any actual harm, any egregious risk of error, or any broad potential for abuse. (...) Our decision [to uphold the contentious provisions of the Protect America

---

19. Yannuzzi, R. E. (2007). *In-Q-Tel: A New Partnership Between the CIA and the Private Sector*. Central Intelligence Agency.

20. New NSA technology goes on sale. (2017, July 19). Retrieved March 13, 2018, from <https://www.intelligenceonline.com/government-intelligence/2017/07/19/new-nsa-technology-goes-on-sale.108255127-bre>

21. United States Foreign Intelligence Surveillance Court Rules of Procedure. <http://www.uscourts.gov/sites/default/files/Rules%20of%20the%20Foreign%20Intelligence%20Surveillance%20Court>.

22. Palmer, B. (2013, June 13). What Happens When You Defy a Secret Government Order? *Slate*. Retrieved from [http://www.slate.com/articles/news\\_and\\_politics/explainer/2013/06/nsa\\_surveillance\\_what\\_if\\_google\\_and\\_verizon\\_refused\\_to\\_hand\\_over\\_data.html](http://www.slate.com/articles/news_and_politics/explainer/2013/06/nsa_surveillance_what_if_google_and_verizon_refused_to_hand_over_data.html)

23. The letter is available at : <https://www.leahy.senate.gov/imo/media/doc/Honorable%20Patrick%20J%20Leahy.pdf>

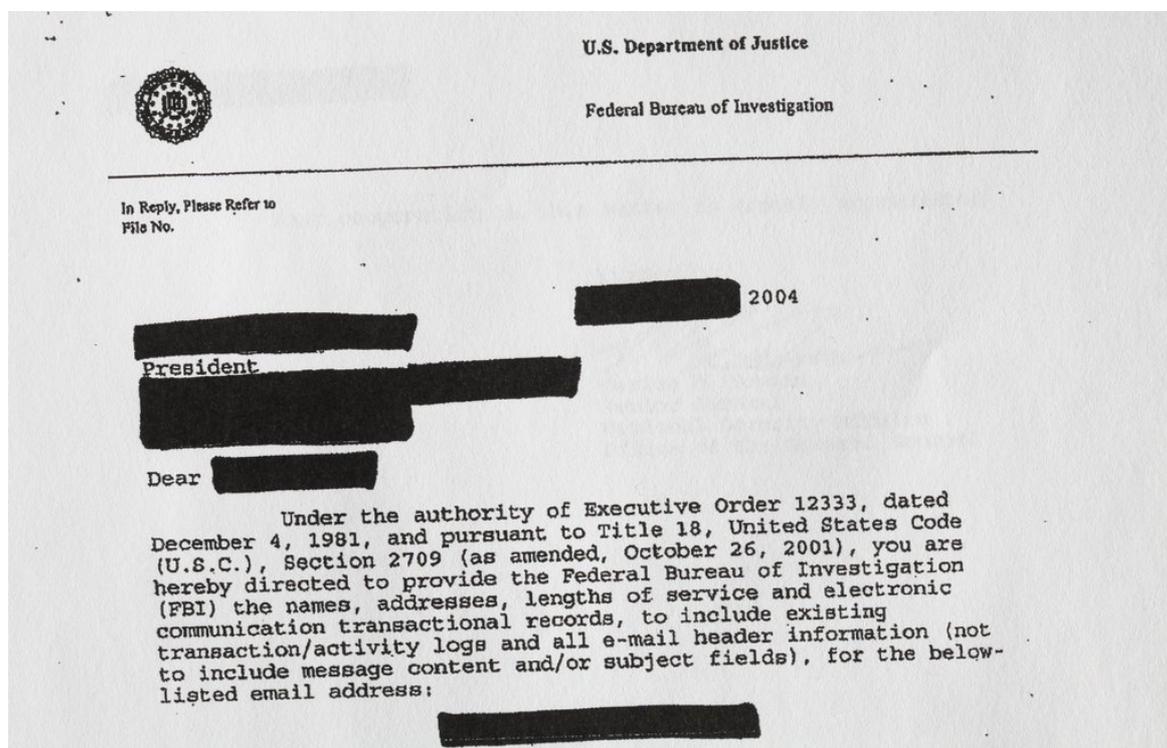
24. *In re Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, n°. 08-01 (Foreign Intelligence Surveillance Court of Review, Jan 15, 2009). Available at <https://fas.org/irp/agency/doj/fisa/fiscr082208.pdf>

Act] recognizes that where the government has instituted several layers of serviceable safeguards to protect individuals against unwarranted harms and to minimize incidental intrusions, its efforts to protect national security should not be frustrated by the courts”.<sup>25</sup>

Under those circumstances, using legal avenues to resist a FISC court order seems almost certain to fail.

The other secret procedure often used for surveillance purposed by US intelligence agencies are “National Security Letters.” National Security Letter (NSL) are an administrative subpoena created in 1978 and issued by the FBI without any judiciary approval. NSL often come with a non-disclosure clause that forbids the recipient from revealing the content and the very existence of the letter, except to a lawyer (so-called “gag order” provisions).

Companies have sometimes challenged NSL, and sometimes managed to strike down the “gag order” (Brust, 2012; Manes, 2015; Weinstein, 2015). For instance, in 2004, a small New York-based ISP called Calyx Internet Access Corporation created in 1994 to serve nonprofit organizations and alternative media outlets challenged a gag order received. This was the first of three lawsuits that put NSL in the spotlight and the growing abuse of the system following changes introduced by the 2001 PATRIOT Act. A 2006 report by the Department of Justice’s Attorney General also found that the FBI had “used NSLs in violation of applicable NSL statutes, Attorney General Guidelines, and internal FBI policies” (Doyle, 2015).



A portion of the redacted letter that the F.B.I. sent to Calyx Internet Access Corporation (Source:

25. Idem.

As we will see, NSL have been one of the focus of post-Snowden surveillance reform in the US, and they have become a better avenue for resisting surveillance orders, or at least giving them more publicity.

A third legal avenue for surveillance are search, issued by a court. In the midst of the Snowden debate, in the summer of 2013, the Texas-based encrypted email service Lavabit was thus ordered to give to the FBI the private keys of its Secure Sockets Layer (SSL) system, so as to enable the government to monitor the communications of Lavabit's most famous customer: Edward Snowden. Lavabit's founder and operator, Ladar Levison, refused to comply and was forced – not after FBI attempts at dissuading him from such a move – to shut down its business.<sup>26</sup>

In France, the 2015 Intelligence Act provides no clear legal avenue for companies would like to challenge surveillance requests, but an appeal before the Council of States is theoretically possible. There is however no indication of such lawsuit, while there is multiple evidence that large telecom firms like Orange have complied with surveillance requests whose legality was extremely doubtful, e.g. for the development of the DGSE extensive surveillance program from 2008 on or to help domestic intelligence spy on investigative journalists (Tréguer, 2016a, 2016b). The law however criminalizes the fact of refusing to comply with a surveillance order is punished by a two-year imprisonment term and a €150 000 fine (article L. 881-2 of the Code of Internal Security, or CIS). The same sentences apply to unauthorized disclosures regarding the "existence of the deployment" of a given surveillance technique (article L. 881-1 CIS). We have found no evidence that such sanctions have ever been used.

Similarly in the UK, during the parliamentary debate on the 2016 Investigatory Powers Act, a legal obligation on companies to assist UK intelligence and law enforcement agencies' surveillance activities was also created. The Act also contains a new criminal offence for these companies or their personnel to reveal that data has been requested.<sup>27</sup>

---

26. Zetter, K. (2016, March 17). A Government Error Just Revealed Snowden Was the Target in the Lavabit Case. Retrieved February 15, 2018, from <https://www.wired.com/2016/03/government-error-just-revealed-snowden-target-lavabit-case/>

27. See : UK Government, 2016, "Investigatory Powers Bill: Obligations on Communications Service Providers". Available at: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/530557/Obligations\\_on\\_CSPs\\_Factsheet.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/530557/Obligations_on_CSPs_Factsheet.pdf)

### 3. (Re)configuration of Public-Private Assemblages in Internet Surveillance: Case-Studies

In this section, we apply this framework of constraint structure developed in the previous section to understand the strategies of private and state actors in the aftermath of the Snowden disclosures. Constraint structures vary in time, space and according to the business sector and the company under consideration. In what follows, we focus on two different settings, namely the United States and France, and large consumer-facing online service providers.

#### 3.1 US: “Big Tech” stages resistance

In the private sector, the most spectacular reactions to the Snowden disclosures undoubtedly came from large online services providers. As already mentioned, some of the first disclosures on the PRISM program led these companies to being accused of actively collaborating with US intelligence outside of any legal framework. But other would follow, for instance the MUSCULAR programme were the same companies were pointed at for weak computer security practices that allowed the NSA to collect their traffic as it moved across their data centers spread out across the world.<sup>28</sup>

Of course, these online service providers were not the only companies being put in the spotlight. Even before Snowden, revelations pointing to the cooperation of companies like AT&T with the NSA surveillance programs had made the headlines. Such revelations – especially those of whistleblower Mark Klein from 2006 on –, were even the source of an amendment passed in the summer of 2008 to give retroactive immunity for the telecom companies that had engaged in these actions outside of any clear legal framework (Wagner, 2009). The Snowden disclosures only added to existing evidence.<sup>29</sup>

But for large online service providers, the Snowden disclosures and the scandal that ensued was a first. As already mentioned looking at Google’s initial response, the allegations that the US government had direct access to the these companies servers did not fare well. As one of our interviewees at Facebook put it, “there was a lot of shock and surprise and the fact that these allegations were being made and the fact that the US government was not correcting them” (Appendix 1).

The internal corporate culture, external pressure from the human rights field as well as the fear of loosing user’s trust led these companies to roll out a multi-pronged resistance strategy.

---

28. Peterson, B. G., Ashkan Soltani, and Andrea. (2013, November 4). How we know the NSA had access to internal Google and Yahoo cloud data. *Washington Post*. Retrieved from <https://www.washingtonpost.com/news/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/>

29. See, e.g.: Gallagher, R., & Moltke, H. (2016, October 16). The NSA’s Spy Hub in New York, Hidden in Plain Sight. Retrieved November 17, 2016, from <https://theintercept.com/2016/11/16/the-nsas-spy-hub-in-new-york-hidden-in-plain-sight/>

Koop, P. (2015, August 31). FAIRVIEW: Collecting foreign intelligence inside the US. Retrieved September 8, 2015, from <http://www.matthewaid.com/post/128102123831/the-nsa-att-fairview-global-fiber-optic-cable>

## Multi-pronged resistance in the aftermath of Snowden

Resistance took different forms. Here we make a distinction between technical resistance, legal resistance, and political resistance.

### Technical resistance

Technical resistance is probably the most significant response brought by the Tech industry, one that would have the most significant impact at the operational level for intelligence and law enforcement agencies.

**Counter-measures:** In the immediate aftermath of Snowden, many of these companies accelerated the rolling-out of encryption and other computer security features that had been lingering on for years. Ensuring SSL/TLS connections for all these companies products, offering users encryption features on their terminals (smartphones especially), rolling out end-to-end encryption of communications content, etc.: Google, Microsoft, Facebook, Apple significantly increased the level of computer security on their products and servers. To give just a snapshot of these trends, Yahoo announced through a blog post of its Chief Information Security Official a series of new features in April 2014 that exemplifies the wider industry response:

“When I joined Yahoo four weeks ago, we were in the middle of a massive project to protect our users and their data through the deployment of encryption technologies as we discussed [in November 2013].

So today, we’re updating you on our progress:

- Traffic moving between Yahoo data centers is fully encrypted as of March 31.
- In January, we made Yahoo Mail more secure by making browsing over HTTPS the default. In the last month, we enabled encryption of mail between our servers and other mail providers that support the SMTPTLS standard.
- The Yahoo Homepage and all search queries that run on the Yahoo Homepage and most Yahoo properties also have HTTPS encryption enabled by default.
- We implemented the latest in security best-practices, including supporting TLS 1.2, Perfect Forward Secrecy and a 2048-bit RSA key for many of our global properties such as Homepage, Mail and Digital Magazines. We are currently working to bring all Yahoo sites up to this standard.
- Users can initiate an encrypted session for Yahoo News, Yahoo Sports, Yahoo Finance, and Good Morning America on Yahoo (gma.yahoo.com) by typing “https” before the site URL in their web browser.
- A new, encrypted, version of Yahoo Messenger will be deployed in coming months”<sup>30</sup>.

Following the revelation of the MUSCULAR program in late-October 2013, Google issued a swift

---

30. Stamos, A. (2014, April 2). Status Update: Encryption at Yahoo. Retrieved February 17, 2018, from <https://yahoo.tumblr.com/post/81529518520/status-update-encryption-at-yahoo>

response the next month by announcing to start encrypting of its traffic between its data centers.<sup>31</sup> People in charge of information security at Google responded to the news with anger and defiance. As the news about MUSCULAR started to emerge, Google security team engineer Brandon Downey wrote a post on its blog expressing his “personal opinion”; “Fuck these guys”. A few days later, another Google security engineer, Mike Hearn, announced the following:

“I now join [Downey] in issuing a giant Fuck You to the people who made these slides. I am not an American, I am a Brit, but it's no different – GCHQ turns out to be even worse than the NSA... The traffic shown in the slides is now all encrypted and the work the NSA/GCHQ staff did on understanding it, ruined.”<sup>32</sup>

In these “personal” take on the matter, resistance is clearly displayed, and it is such reactions that made the news then. But if it took a matter of days or months for these companies to upgrade their policies and practices after the Snowden disclosures, why had not they been established before? When asked these questions, our interviewees would use the same justifications as those issued at the time: these efforts at beefing up their information security standards had been underway for quite some time even before the Snowden disclosures. For instance, a high-level public affairs director at Microsoft claims that “we were already working on the security and we had made at this time already a lot of investment” (Appendix 1). A Google executive argued that “Google didn’t necessarily make any changes, although it certainly accelerated ongoing efforts that already existed at the time in terms of security (...) and educating its users” (idem). According to Rubinstein and Van Hoboken (2014) these technological fixes were a way to ensure that surveillance of their users’ communication would happen with their knowledge and assent, thereby reinforcing their position in the security field.

**Pressure from human rights and computer security fields:** These moves were called for by NGOs like EFF who called for and tracked progress regarding computer security at leading US tech firms through “scorecards,” but also prominent public advocates like Edward Snowden himself, who regularly called on these companies to act to make surveillance more difficult through encryption. In October 2014, Snowden addressed technology professionals at the South by Southwest festival. In addition to a “policy response” to mass surveillance, he insisted that:

“there’s also a technical response. And it’s the makers, it’s the thinkers, it’s the development community that can really crack those solutions to make sure we’re safe. You guys who are in the room now are all the firefighters. And we need you to help fix this.”<sup>33</sup>

The moves of these companies towards technical resistance need to be located in the more global context of the wake-up call that the Snowden disclosures issued to the “field of computer security;” dominated by actors with a strong technical capital, working as computer engineers, system administrators, cryptographers, etc. They are the social group that better grasps the technical intricacies of the modern-day surveillance, helping other actors to make sense of the Snowden

---

31. Miller, Rich. (2013, September 9). Google Boosting Encryption Between Data Centers. Retrieved 13 May 2018, from <http://www.datacenterknowledge.com/archives/2013/09/09/google-boosts-encryption-between-data-centers>

32. Gallagher, S. (2013, November 6). Googlers say “F\*\*\* you” to NSA, company encrypts internal network. Retrieved May 26, 2015, from <http://arstechnica.com/information-technology/2013/11/googlers-say-f-you-to-nsa-company-encrypts-internal-network/>

33. Couts, A. (2014, March 10). Edward Snowden at SXSW: Encryption is the answer to NSA surveillance. Retrieved February 17, 2018, from <https://www.digitaltrends.com/web/edward-snowden-sxsw-2014-speech-live/>

documents while engaging in a sustained effort aimed at improving computer security.

An important subgroup of the field are independent actors developing technical counter-measures, increasing the cost of surveillance through decentralized architectures and/or the use of cryptography. These tools are developed by small independent companies or non-profit collectives who typically display a “hacktivists” ethos, with the aim of democratizing the resort to such alternative tools. And to an extent it succeeded. It is often thanks to these small independent hacker collectives that tech multinationals were able to improve the security of their products and services. For instance, Facebook announced the experimentation of PGP encryption for email notifications with end-users. To do so, the company relied on a software developed by the open source GnuPG encryption project, which had been stalled for years due to lack of funding and benefited from \$50,000 donation by Facebook in mid-2015.<sup>34</sup> Facebook messaging tools and that of its subsidiary WhatsApp also began to use an end-to-end encryption solution called TextSecure developed by the small company called Open Whisper Systems, which develops Signal, a messaging application.<sup>35</sup>

Other important subcategories in the field of computer security which had a significant impact on these developments in the private sector include engineering professional groups (e.g. IEEE), cybersecurity experts (like CERTs) and Internet governance fora (in charge of developing or promoting Internet standards IETF or ISOC). While some of these groups had long warned about the surveillance capabilities of intelligence agencies, others have received the Snowden controversy as a wake-up call and launched new initiatives aimed at boosting computer security (Rogers & Eden, 2017). As recognized institutions dominated with a scientific ethos, these actors played an important role in bringing certification to the political claims of hacker collectives.

The overall effect of the Snowden disclosure, it seems, was to significantly increase the weight of the “computer security” field relative to other fields involved in post-Snowden controversies on surveillance, and therefore of the multipositioned actors present in this field in the other social settings in which they evolved. To keep afloat as the whole field was upgrading the “state of the art” of computer security to reflect the knowledge gains associated with the Snowden disclosures, large online service providers had some catching up to do, and accelerated technical developments that had been in the making but were arguable already overdue. In the post-Snowden context, NGOs, hackers, standard-making bodies collaborated with industry players, e.g. with the creation of Internet Security Research Group (ISRG) which set up “Let’s Encrypt” campaign aimed at speeding up the development of encryption in Web browsing.

Technical resistance coming from large multinationals and the wider “computer security field” has apparently had a strong effect on the the surveillance capacities of law enforcement and intelligence agencies, leading to revived controversies on encryption as we will see. According to General James Clapper, then the US Director of National Intelligence, “as a result of the Snowden revelations, the onset of commercial encryption has accelerated by seven years”.<sup>36</sup> Clapper said he based his

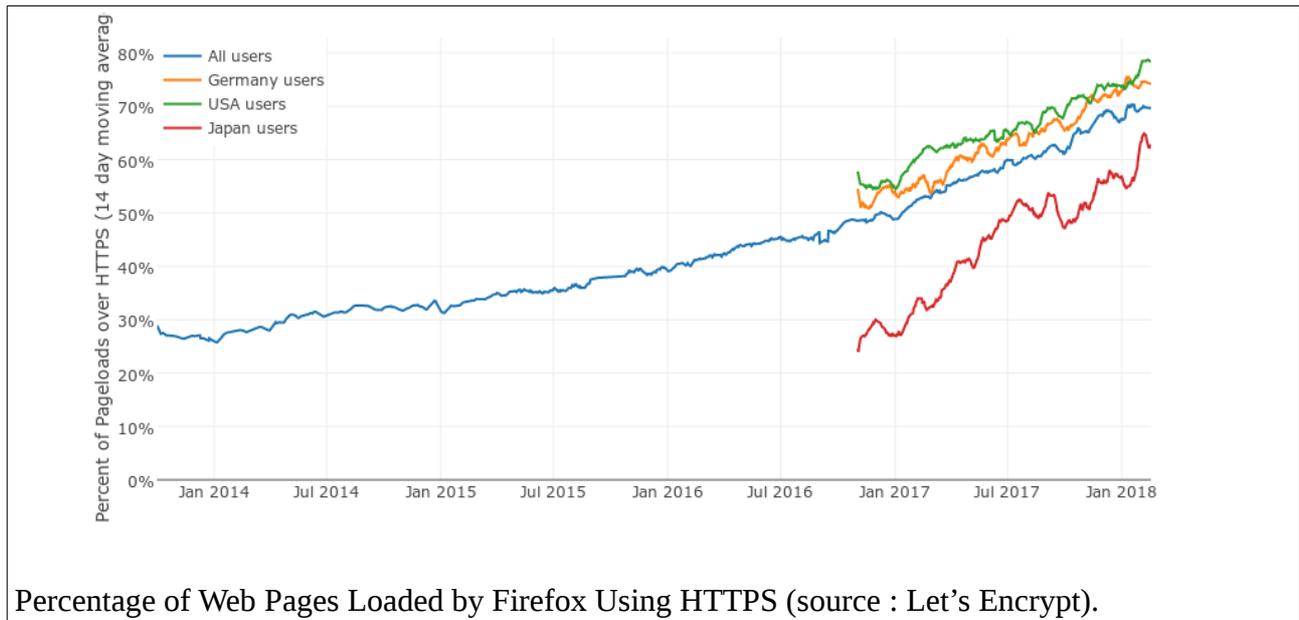
---

34. Moody, G. (2015, June 1). Facebook users can now add OpenPGP keys for improved email security. Retrieved June 1, 2015, from <http://arstechnica.co.uk/security/2015/06/facebook-users-can-now-add-openpgp-keys-for-improved-email-security/>

35. moxie. (2014, November 28). Open Whisper Systems partners with WhatsApp to provide end-to-end encryption. Retrieved February 17, 2018, from <https://signal.org/blog/whatsapp/>

36. McLaughlin, J. (2016, April 25). Spy Chief Complains That Edward Snowden Sped Up Spread of Encryption by 7 Years. Retrieved May 2, 2016, from <https://theintercept.com/2016/04/25/spy-chief-complains-that-edward-snowden-spiced-up-spread-of-encryption-by-7-years/>

comments on NSA forecasts issued three years earlier.



## Legal resistance

Another front of resistance of large online service providers is litigation. And here, we can see three main fronts in the litigation strategies set forth by these companies to alleviate surveillance capabilities: transparency, encryption and access to data held in the cloud.

**Litigating for transparency:** The first was a demand that was made really early after the first disclosures. It consisted in decreasing the level of secrecy surrounding the requests issued by law enforcement and intelligence agencies to these companies. For instance, Yahoo filed a case before the FISC with the aim to declassify its 2008 challenge, which it said would show that it had sought to resist its inclusion in the PRISM program and point to some of the ways in which the court by narrow down the range of information sought after by the government.<sup>37</sup>

With regards to detailed statistics about national security surveillance, the legal fight had also started before, and was only made more visible in the aftermath of Snowden. As previously mentioned, the gag orders often attached to National Security Letters and FISA warrants was one of the main criticism issued against this legal avenue for surveillance requests, and that debate had been going on since the mid-2000s. Some progress was being made. For instance, in March 2013, Google was able to report on the first aggregate amounts of NSL that it received, and the number of users affected by incremental range of 1,000.<sup>38</sup> But in the aftermath of Snowden, many of the problems identified with NSL and the FISA requests only became more acute. Through court action and litigation, and alongside NGOs like EFF, tech companies tried to enact meaningful changes in this field. In June 2013, Microsoft and Google joined efforts to file a lawsuit before the FISC to ask the court to be able to disclose some data about the data requests authorized by the court.<sup>39</sup>

37. Ackerman, S. (2013, July 30). Justice Department to declassify key Yahoo surveillance orders. Retrieved February 19, 2018, from <http://www.theguardian.com/world/2013/jul/30/justice-department-declassify-yahoo-surveillance-orders>

38. Transparency Report: Shedding more light on National Security Letters. (n.d.). Retrieved February 19, 2018, from <https://googleblog.blogspot.com/2013/03/transparency-report-shedding-more-light.html>

39. Arthur, C. (2013, June 28). Microsoft joins Google in demanding to disclose FISA requests. Retrieved February

While doing so, they also started releasing information about aggregates of the number of data requests they had received in the previous month to correct the impression resulting from the PRISM media coverage alleging that US intelligence had unlimited access to these companies' servers. For instance, Facebook and Microsoft's disclosures covered the second half of 2012: Facebook said it received between 9,000 and 10,000 requests from federal, state and local authorities for customer data during that period, while Microsoft said it received between 6,000 and 7,000. The numbers blended for the first time NSL and FISA requests.

Such disclosures had been validated by the FBI and the Department of Justice. Through the FISA lawsuit introduced by Google and Microsoft, these companies and the US government managed to strike a deal in January 2014 to give separate aggregate number for FISA requests and NSL. The deal also allowed the company to break down FISA requests to indicate whether the requests were related to the content of accounts or non-content information (such as subscriber name). "The administration is acting to allow more detailed disclosures about the number of national security orders and requests issued to communications providers, the number of customer accounts targeted under those orders and requests, and the underlying legal authorities," attorney general Eric Holder and director of national intelligence James Clapper said in a joint statement. The announcement echoes Barack Obama's speech of January 14<sup>th</sup>, 2014 in which the president had called for "new reporting methods" whereby "communications providers will be permitted to disclose more information than ever before to their customers."<sup>40</sup>

But the deal remained a small step forward. As the Guardian reported, "the disclosures are to be nonspecific, listed by the thousand and subject in some cases to a six-month delay – speaking to the large quantities of data that the government still plans on collecting from its technology partners. In order to be more specific about the amount of data turned over, the companies must be less specific about the type of data it is. The deal also explicitly points to a delay of up to two years on revealing information on data collected under surveillance programs the National Security Agency may yet develop."<sup>41</sup>

**Litigating for strong encryption:** Another major litigation effort came in the wake of the terrorist attack of San Bernadino in December 2015, when the FBI sought to force the "cooperation" of Apple in developing codes aimed at circumventing the full-disk encryption features that had been rolled out as part of the firm's technical resistance in the aftermath of Snowden (note that only the data of the five days prior to the attack were inaccessible – older data had been synchronized on iCloud and was handed over to US authorities). After the Charlie Hebdo attacks on 2015, mounting criticism against the growing resort to encryption features by the US tech industry came from the French, the British and the US governments.<sup>42</sup> That sequence reached a peak in the US in late-2015,

---

19, 2018, from <http://www.theguardian.com/technology/2013/jun/28/microsoft-google-fisa-united-states-government>

40. McCarthy, T. (2014, January 17). Obama announces new limits on NSA surveillance programs – live reaction. Retrieved February 19, 2018, from <http://www.theguardian.com/world/2014/jan/17/obama-nsa-surveillance-reforms-speech-live>

41. Dredge, S. (2013, June 18). Yahoo joins Facebook, Google and others in revealing US surveillance requests. Retrieved February 19, 2018, from <https://www.theguardian.com/technology/2013/jun/18/yahoo-reveals-us-surveillance-requests-nsa>

42. Watt, N., & Wintour, P. (2015, January 15). David Cameron seeks cooperation of US president over encryption crackdown. Retrieved from <http://www.theguardian.com/uk-news/2015/jan/15/david-cameron-ask-us-barack-obama-help-tracking-islamist-extremists-online>

Yadron, D. (2015, January 16). Obama Sides with Cameron in Encryption Fight. Retrieved from <http://blogs.wsj.com/digits/2015/01/16/obama-sides-with-cameron-in-encryption-fight/>

early-2016. In 2014, Apple had extended encryption to text messages and other forms of data on their smartphones, announcing that for all devices running iOS 8 or later version, it would not be able to perform the sort of “data extractions” in response to search warrants. But in the case of the San Bernardino attacker’s iPhone, Apple was presumably still able to bypass the encryption by developing some bits of code. Using a 1789 statute providing the court extensive authority, the FBI therefore sought to force Apple into developing it.<sup>43</sup> During this sequence, much of the computer industry and telecom companies like AT&T intervened in the case in defence of Apple.<sup>44</sup> Blackberry and Bill Gates, Microsoft’s retired founder, were some of the few exceptions.<sup>45</sup> As Gates was making the news as “backing the FBI” in the ongoing dispute,<sup>46</sup> Microsoft President and Chief Legal Officer Brad Smith insisted that “trust is the absolute foundation of our entire industry”, and that strong encryption was one of the way of restoring it.<sup>47</sup>

Here again, tech firms that got involved in the debate would count on the support of the wider “computer security” field, who saw encryption has absolute necessity, and joined in the debate to bring certification to the companies’ claims. A key development in this regard was the publication of a report by Harvard’s Berkman-Klein Center for Internet & Society, co-authored by people like Joshep Nye or Bruce Schenier (Project, 2016). Published in February 2016, as the Apple-FBI stand-off was ongoing, it presented the following conclusions:

“Although we were not able to unanimously agree upon the scope of the problem or the policy solution that would strike the best balance, we take the warnings of the FBI and others at face value: conducting certain types of surveillance has, to some extent, become more difficult in light of technological changes (...).

However, the question we explore is the significance of this lack of access to communications for legitimate government interests. We argue that communications in the future will neither be eclipsed into darkness nor illuminated without shadow. Market forces and commercial interests will likely limit the circumstances in which companies will offer encryption that obscures user data from the companies themselves, and the trajectory of technological development points to a future abundant in unencrypted data, some of which can fill gaps left by the very communication channels law enforcement fears will “go dark” and beyond reach.”

Meanwhile, US public authorities appeared extremely fragmented. While prosecutors sided with the FBI, even NSA officials like James Clapper or Michael Hayden as well as the Secretary of Defense defended the industry’s position from a cybersecurity standpoint.<sup>48</sup> Despite disagreements from

---

43. Jeong, S. (2015, October 13). The Obscure 1789 Statute That Could Force Apple to Unlock a Smartphone. Retrieved February 21, 2016, from <http://motherboard.vice.com/read/writs-and-giggles>

44. See the joint brief from Amazon.com, Box, Cisco Systems, Dropbox, Evernote, Facebook, Google, Lavabit, Microsoft, Mozilla, Nest Labs, Pinterest, Slack Technologies, Snapchat, WhatsApp, and Yahoo!. Briefs from the American Civil Liberties Union, the Electronic Frontier Foundation, Access Now, and the Center for Democracy and Technology also supported Apple. <https://www.apple.com/newsroom/2016/03/03Amicus-Briefs-in-Support-of-Apple/>

45. Champeau, G. (2015, December 18). Blackberry s’oppose au chiffrement de bout en bout. Retrieved January 6, 2016, from <http://www.numerama.com/business/135533-blackberry-plaide-contre-le-chiffrement-de-bout-en-bout.html>

46. Kulwin, N. (2016, February 23). Bill Gates Is Backing the FBI in Its Case Against Apple. Retrieved February 23, 2016, from <https://recode.net/2016/02/22/bill-gates-is-backing-the-fbi-in-its-case-against-apple/>

47. Barss, P. (2016, March 1). “Trust in technology has been eroded” says Microsoft. Retrieved March 3, 2016, from <http://www.infosecurity-magazine.com/news/rsac-trust-in-technology-eroded/>

48. Manach, J. M. (2016, March 31). Crypto: pourquoi l’ex-chef de la NSA défend Apple. Retrieved April 3, 2016, from <http://bugbrother.blog.lemonde.fr/2016/03/31/crypto-pourquoi-lex-chef-de-la-nsa-defend-apple/> Perloth, N.

(2016, March 2). Defense Secretary Takes Position Against a Data ‘Back Door.’ *The New York Times*. Retrieved from

intelligence committee members,<sup>49</sup> Congress-members were also aligned with the position of the tech industry.<sup>50</sup>

Eventually, the legal stand-off was never legally resolved, as the FBI pulled out of the case when it announced that a small digital forensic company had been able to provide assistance in unlocking the phone.<sup>51</sup> Fragmented over the issue, the Obama administration apparently stuck to the middle-ground option outlined in the draft options paper on approached to encryption from the US National Security Council (NSC) from mid-2015, that is a few months before the San Bernadino case made headlines.<sup>52</sup> The document defined this approach as “calling on deferring legislation and other compulsory actions” against the use of encryption features by the US computer industry:

“(…) The administration would seek industry's voluntary assistance to modify their technologies to address law enforcement's concerns” Alternatively, “the administration [could] still ask providers to assist law enforcement in any way that they can within their current technological framework. In either case, these calls for assistance could be done publicly or privately, depending on the preferred engagement framework.”

This sequence marked the end of a major episode during which the antagonism between the industry and major actors of the US law enforcement nexus could be staged. It is this option of “deferring legislation” and sticking to the status quo that has prevailed up until now.

**Limiting access to cloud data:** The third important front for the litigation strategies of US online service providers was the legal regime associated with online “cloud” data. Two cases are of particular importance in this regard.

In June 2014, the Supreme Court of the United States issues its first significant ruling on surveillance since the first Snowden disclosures. In *Riley v. California*,<sup>53</sup> it unanimously held that the warrantless search and seizure of digital contents of a cell phone during an arrest is unconstitutional. According to Chief Justice John G. Roberts:

“Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans “the privacies of life”. The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.”

He went on to explain that:

“Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter. But the analogy crumbles entirely when a cell

---

<http://www.nytimes.com/2016/03/03/technology/defense-secretary-takes-position-against-a-data-back-door.html>

49. Ackerman, S., & Francisco, S. T. D. Y. in S. (2016, March 1). Congress tells FBI that forcing Apple to unlock iPhones is “a fool’s errand.” *The Guardian*. Retrieved from

<http://www.theguardian.com/technology/2016/mar/01/apple-fbi-congress-hearing-iphone-encryption-san-bernardino>

50. Ackerman, S., & Francisco, S. T. D. Y. in S. (2016, March 1). Congress tells FBI that forcing Apple to unlock iPhones is “a fool’s errand.” *The Guardian*. Retrieved from

<http://www.theguardian.com/technology/2016/mar/01/apple-fbi-congress-hearing-iphone-encryption-san-bernardino>

51. Armerding, T. (2017, January 30). FBI v. Apple: One year later, it hasn’t settled much. Retrieved January 31, 2017, from <http://www.csoonline.com/article/3160485/mobile-security/fbi-v-apple-one-year-later-it-hasn-t-settled-much.html>

52. US National Security Council. (2015). *Draft options paper on strategic approaches to encryption*. Washington DC.

53. *Riley v. California*, No. 13-132, 573 U.S.(2014).

phone is used to access data located elsewhere, at the tap of a screen. That is what cell phones, with increasing frequency, are designed to do by taking advantage of ‘cloud computing (...). The United States concedes that the search incident to arrest exception may not be stretched to cover a search of files accessed remotely—that is, a search of files stored in the cloud.”

U.S. companies did not intervene directly in the case, but exactly a year after the first Snowden disclosures, they helped put the highlight on this first major win for the right to privacy. According to Microsoft’s legal counsel Brad Smith, “for those of us at Microsoft and other tech companies who are seeking to ensure that the Fourth Amendment protects information stored in the cloud, these are encouraging words.” “Both the judicial and legislative branches have taken new steps to protect privacy. It’s not unreasonable to hope that now more than ever, there is an important opportunity to bring people together to address next-generation privacy issues,” he added.<sup>54</sup>

Another major case regarding access to online data is currently being litigated by the Supreme Court: The *Microsoft Ireland* case (Christakis, 2017). The case originates from a December 2013 ruling whereby a US judge ordered Microsoft to give to US authorities access to the content of emails and subscriber information of a suspect in a drug trafficking case that were held on servers located in Ireland, invoking the Stored Communications Act of 1986. Microsoft refused to comply with that demand that sought to circumvent the international mechanisms of mutual legal assistance normally applicable, saying that the Act had no extraterritorial effect. The Court of Appeal of the Second Circuit sided with Microsoft, and the government appealed to the Supreme Court, which accepted to review the case in October 2017. Deputy Solicitor General Jeffrey Wall argued that the Appellate Court’s order had led Microsoft, Google and Yahoo to deny law enforcement’s request to accessing information stored on servers outside the United States, hampering criminal investigations. But separately the Department of Justice has also indicated that “Google has reversed its previous stance and informed the government that it will comply with new Section 2703 warrants outside the 2nd Circuit (while suggesting that it will appeal the adverse decisions in one or more existing cases).”<sup>55</sup> Given these disparities in prevailing legal interpretations, a clarification through the Supreme Court decision would have clarified the scope of the relevant statute. It was bound to have far-reaching implications, and many parties have intervened in the case through amicus curiae, like business organizations from Germany or France, the European Commission and Members of the European Parliament, and many NGOs.<sup>56</sup> According to Theodore Christakis, a professor in international law:

“If the Supreme Court finds in favour of the US government, that means that, tomorrow, the US authorities could, for example, issue a mandate requiring Microsoft or another cloud provider operating in the United States (Apple, Amazon, IBM, Google, Facebook etc.) to submit the “content data” of a French national suspected of a crime in the United States (including, for example, a journalist accused of undermining US national security), even though this French citizen lives in France and his data are stored by the relevant supplier in France, and this without using an international request for legal

---

54. Smith, B. (2014, June 28). The privacy week that was. Retrieved February 19, 2018, from

[https://blogs.technet.microsoft.com/microsoft\\_on\\_the\\_issues/2014/06/28/the-privacy-week-that-was/](https://blogs.technet.microsoft.com/microsoft_on_the_issues/2014/06/28/the-privacy-week-that-was/)

55. Kravets, D. (2017, September 14). Google stops challenging most US warrants for data on overseas servers.

Retrieved February 15, 2018, from <https://arstechnica.com/tech-policy/2017/09/feds-google-stops-challenging-most-us-warrants-for-data-on-overseas-servers/>

56. United States v. Microsoft Corp, Docket N° 17-2. <http://www.scotusblog.com/case-files/cases/united-states-v-microsoft-corp/>

assistance or any other form of cooperation with the French authorities” (Christakis, 2017).

In late March 2018 however, Microsoft filed a brief supporting the Department of Justice to dismiss the case, arguing that it was now pointless considering that Congress had passed a new legislation on transborder access to online data.<sup>57</sup> An unconvincing justification considering that the new Act fails to solve the issue at hand in that case.<sup>58</sup> But the Supreme Court agreed and dismissed the case.<sup>59</sup> We come back to the CLOUD Act at the end of the following subsection.

## Political resistance

Technical and legal resistance are always accompanied by lobbying efforts aimed at influencing policy-makers. Since 2013 – and beyond the issues already mentioned which also mobilized the lobbying teams of online service providers (e.g. encryption, transparency, transborder access to cloud data, etc.) – three important reforms of US surveillance laws led to joint resistance strategies. These were coordinated by the various industry players, who even moved to set up a joint-public relation campaign through ReformGovernmentSurveillance.com, sponsored by AOL, Facebook, Google, Microsoft, Twitter, Yahoo and others. On December 9<sup>th</sup>, 2013, these companies placed a full-page advertisement in major newspapers to broadcast an open letter to President Barack Obama and Congress asking them “to take the lead and make reforms that ensure that government surveillance efforts are clearly restricted by law.”

**Patriot Act Section 215:** The first full-fledged campaign for coalition would come 18 months later when section 215 of the Patriot Act, on which was based many of the NSA’s surveillance programs.<sup>60</sup> In May 2015, an appellate court ruled that the Patriot Act did not authorize the National Security Agency to collect Americans’ calling records in bulk. But given the national security interests at stake, the judge decided to let Congress take action, since Section 215 of the Patriot Act would expire on the first of June.<sup>61</sup> The debate in Congress was fierce, but in a last minute move and with the implication of the Obama White House, new provisions were adopted to provide a new legal basis for the surveillance capacities that relied on the Patriot Act. The USA Freedom Act, as it would be called,<sup>62</sup> was thus adopted on June 2<sup>nd</sup>, 2015, after more than 20 other attempts at reforming the surveillance powers of US agencies had failed.<sup>63</sup> Besides responding to the tech

---

57. Microsoft calls for dismissal of U.S. Supreme Court privacy fight. (2018, April 4). *Reuters*. Retrieved from <https://www.reuters.com/article/us-usa-court-microsoft/microsoft-calls-for-dismissal-of-u-s-supreme-court-privacy-fight-idUSKCN1HA2KH>

58. “Because Ireland is not party to an executive agreement, Microsoft now is faced with a compulsory production order that has extraterritorial reach and nothing in the CLOUD Act permits a motion to quash the warrant or requires a court to conduct a comity analysis using the same factors that would be required if there were an executive agreement in place.” See: Gidari, A. (2018, April 9). What will Microsoft and Ireland do with the new CLOUD Act warrant? Retrieved April 10, 2018, from <https://iapp.org/news/a/does-the-cloud-act-raise-more-questions-than-it-answers/>

59. Supreme Court dismisses warrant case against Microsoft after CLOUD Act renders it moot. (2018, April 17). Retrieved April 19, 2018, from <http://social.techcrunch.com/2018/04/17/supreme-court-dismisses-warrant-case-against-microsoft-after-cloud-act-renders-it-moot/>

60. P/K, G. door. (n.d.). Electrospace.net: Section 215 bulk telephone records and the MAINWAY database. Retrieved January 22, 2016, from <http://electrospace.blogspot.fr/2016/01/section-215-bulk-telephone-records-and.html>

61. Stempel, J. (2015, May 7). NSA’s phone spying program ruled illegal by appeals court. *Reuters*. Retrieved from <https://www.reuters.com/article/us-usa-security-nsa/nsa-phone-surveillance-not-authorized-u-s-appeals-court-idUSKBN0NS11N20150507>

62. The name of the Act stands for: Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act.

63. Gallagher, R. (2013, October 29). U.S. Lawmakers Launch Assault on NSA Domestic Snooping. *Slate*. Retrieved

companies' request for greater transparency (e.g. by creating new avenues to challenge gag orders attached to National Security Letters or imposing new reporting requirements on US authorities), the Act prohibits NSA to collect and store domestic call records in bulk. Instead, the NSA must apply for a warrant from the FISA Court, which approves specific and targeted selectors to be provided to telecommunication providers, who use them for querying their own databases and only these results are handed over to NSA. The Act also enabled the presiding judges of the FISA courts to designate five individuals to serve as amicus curiae during cases that entails novel or significant interpretation of the legal framework. During the whole legislative process on the bill; the "Reform Government Surveillance" industry group was very active in pushing for legislation that would contribute to "rebuilding the essential element of trust not only in the technology sector but also in the U.S. government." According to the companies, "as a result of increasing concern about the level of access the U.S. government has to user-generated data held by technology companies, many domestic and foreign users have turned to foreign technology providers while, simultaneously, foreign jurisdictions have implemented reactionary policies that threaten the fabric of the borderless internet."<sup>64</sup> After the bill was adopted, it reacted with a short statement:

"We commend the Senate for passing the USA Freedom Act, a bill that makes significant progress in reforming U.S. government surveillance programs and practices. The action today shows the United States' leadership in ensuring transparency and accountability of government actions that impact the privacy and trust of Internet users."<sup>65</sup>

As we can see, trust was again central theme to the concerns voiced by the industry. We will discuss the actual impact and shortcomings of this reform in the following section.

**US Judicial Redress Act:** In January 2016, the coalition also celebrated the adoption of the US Judicial Redress Act, adopted by the US to make good on its promise to grant EU citizens a right to redress before US courts to protect their privacy rights, which was made in the context of the negotiations of the so-called Privacy Shield agreement.<sup>66</sup>

In June 2016, human rights NGOs and industry joined forces when Congress started considering a bill that would have expanded surveillance powers exerted under the framework of Nation Security Letters defined by the Electronic Communications Privacy Act (ECPA) of 1986. According to a letter sent by this new coalition to the proposed amendment would have extended the range of subscriber information available to law enforcement to new categories of items, such as the websites that a person visited, the time spent on those sites, email metadata, location information and IP addresses.<sup>67</sup> This was a significant extension compared with the existing language of the ECPA, which was drafted before the advent of the Internet and limited such subscriber information to "the name, address, length of service, and local and long distance toll billing records." The effort

---

from

[http://www.slate.com/blogs/future\\_tense/2013/10/29/sensenbrenner\\_and\\_leahy\\_s\\_usa\\_freedom\\_act\\_seeks\\_to\\_curb\\_ns\\_a\\_domestic\\_spying.html](http://www.slate.com/blogs/future_tense/2013/10/29/sensenbrenner_and_leahy_s_usa_freedom_act_seeks_to_curb_ns_a_domestic_spying.html)

64. <https://reformgs.tumblr.com/post/118692011732/rgs-joins-coalition-urging-house-leadership-to>

65. [https://www.aclu.org/sites/default/files/field\\_document/ectr\\_coalition\\_letter\\_6-6.pdf](https://www.aclu.org/sites/default/files/field_document/ectr_coalition_letter_6-6.pdf)

66. Reform Government Surveillance Applauds the Senate Judiciary Committee on the Judicial Redress Act, Urges Swift Action in the Full Senate. (2016, January 28). Retrieved February 20, 2018, from <https://reformgs.tumblr.com/post/138233977817/reform-government-surveillance-applauds-the-senate>

67. Tech firms say FBI wants browsing history without warrant. (n.d.). Retrieved February 20, 2018, from <https://www.engadget.com/2016/06/07/fbi-ecpa-ammendment-browsing-metadata-no-warrant/>

was successful in killing the bill.<sup>68</sup> The coalition has been supporting another bill, the Email Privacy Act, which would close a loophole of the existing ECPA which allows the government to obtain access emails, data in cloud storage more than 180 days old, without a court warrant.

**FISA Section 702:** One last important effort specific to the US was the renewal of Section 702 of FISA, which expired at the end of 2017. In a letter sent to the leadership of the US Congress in late February 2017, the coalition listed its priorities regarding government surveillance. Regarding FISA Section 702, the letter underlined that:

“As Congress moves towards reauthorizing these powers, we would support changes to Section 702 that enhance transparency, provide greater programmatic oversight, and strengthen protection of sensitive personal data. Among the reforms that we would like to work with you on are narrowing the type of information that can be collected under Section 702; requiring judicial oversight for searching the contents of 702 material for the communications of a US person (given that US persons are not the target of 702); allowing companies to disclose the number of requests they receive by legal authority; further declassification of FISA Court orders; and providing greater transparency around how the communications of US persons that are incidentally collected under Section 702 are searched and used, including how often it is “queried” using identifiers that are tied to US persons.”<sup>69</sup>

FISA Section 702 has been described as a “crown jewel” of the intelligence community in the US, a provision that underlies the most important of its surveillance programs. And as early as March, the Trump administration made clear that it would seek a “permanent and clean” reauthorization, meaning that no substantive changes would be brought to the law.<sup>70</sup> This was again stressed in September in a letter sent by the Attorney General Jeff Sessions and the Director of National Intelligence Daniel R. Coats to Congress leadership.<sup>71</sup>

On January 11<sup>th</sup> 2018, Congress passed the FISA Amendments Reauthorization Act, which will remain valid until 2023. The later fails to respond to the concerns of privacy advocates, although it slightly increases the level of transparency and protection for US-persons.<sup>72</sup> Legal experts argue that

68. Empowering Law Enforcement to Keep America Safe Act of 2016. <https://www.congress.gov/bill/114th-congress/senate-bill/3369/all-info>

69. See also the demands made by the trade group CCIA in May 2017: “First, reauthorization legislation should codify recent changes made to “about” collection pursuant to NSA’s Upstream program. This reform would merely codify changes already embraced by the U.S. government with the imprimatur of the Foreign Intelligence Surveillance Court (FISC) to correct deficiencies that implicate the constitutional rights of U.S. citizens. Second, reauthorization legislation should require judicial oversight of government queries of the contents of 702 material for the communications of U.S. persons (given that U.S. persons are not the target of 702). Third, reauthorization legislation should narrow the definition of “foreign intelligence information” under FISA to reduce the likelihood of collecting information about non-U.S. persons who are not suspected of wrongdoing. Fourth, increasing oversight and transparency of Section 702 collection will improve confidence in both its utility and lawfulness. Companies should be allowed to disclose the number of requests they receive by a legal authority and should be permitted to make more granular disclosures concerning the volume of national security demands that they receive. We also support further declassification of FISC orders. Finally, there should be greater transparency around how the communications of U.S. persons that are incidentally collected under Section 702 are searched and used, including how often 702 databases are queried using identifiers that are tied to U.S. persons.” <https://www.ccianet.org/wp-content/uploads/2017/05/702-letter-201705-FINAL.pdf>

70. Volz, D., & Holland, S. (2017, March 1). White House supports renewal of spy law without reforms: official. *Reuters*. Retrieved from <http://www.reuters.com/article/us-usa-trump-fisa-idUSKBN16855P>

71. Letter by Attorney General Sessions and Director of National Intelligence Coats Urging Congress to Reauthorize Title VII of the Foreign Intelligence Surveillance Act. (2017, September 11). Retrieved February 21, 2018, from <https://www.justice.gov/opa/pr/letter-attorney-general-sessions-and-director-national-intelligence-coats-urging-congress>

72. Kohse, E. (2018, January 18). Summary: The FISA Amendments Reauthorization Act of 2017. Retrieved February

its implementation could lead to upgraded procedures to protect the rights of US residents and foreigners alike, in a way which might alleviate some of the concerns undermining the legal prospects of the Privacy Shield agreement in Europe.<sup>73</sup> Overall, the Bill responded to the major issues voiced by the industry, although the absence of progress for non-US persons and the resulting risks for the Privacy Shield agreement represent a liability for them.

**The CLOUD Act:** On March 23<sup>rd</sup>, 2017, US President Donald Trump signed into law the CLOUD Act (or Clarifying Lawful Overseas Use of Data Act). This piece of legislation – first presented by the Department of Justice in mid-2016 –<sup>74</sup> was added in last minute to a spending bill revise the legal framework regulating US law enforcement access to online data stored overseas as well as access do data by foreign law enforcement authorities to data held in the US. The goal is to provide a streamlined legal avenue to bypass MLAT procedures and limit the extra-territorial effects of the Stored Communications Act (the later was opposed by tech firms and debated in the context of the *Microsoft Ireland* case, see above).

The Bill passed with wide-ranging support from the tech sector (which took an active role in crafting it)<sup>75</sup> but was criticized by human rights organizations. According to EFF:

- “Enable foreign police to collect and wiretap people's communications from U.S. companies, without obtaining a U.S. warrant.
  - Allow foreign nations to demand personal data stored in the United States, without prior review by a judge.
  - Allow the U.S. president to enter "executive agreements" that empower police in foreign nations that have weaker privacy laws than the United States to seize data in the United States while ignoring U.S. privacy laws.
  - Allow foreign police to collect someone's data without notifying them about it.
  - Empower U.S. police to grab any data, regardless if it's a U.S. person's or not, no matter where it is stored.”<sup>76</sup>

The main criticism coming from NGOs is one underlying the lack of debate on these complex issues.

“Microsoft, who call for the dismissal of the case pending before the Supreme Court on whether the US government could seek access to data stored in Ireland outside of MLAT procedures as a result of the adoption of the Act, instead stresses that the text provides important safeguards:

---

19, 2018, from <https://www.lawfareblog.com/summary-fisa-amendments-reauthorization-act-2017>

73. Goitein, E., & Litt, R. (2018, February 20). A Way Forward on Section 702 Queries. Retrieved February 21, 2018, from <https://www.justsecurity.org/52737/section-702-queries/>

74. Wong, C. M. (2017, September 18). US Cross-Border Data Deal Could Open Surveillance Floodgates. Retrieved September 20, 2017, from <https://www.hrw.org/news/2017/09/18/us-cross-border-data-deal-could-open-surveillance-floodgates>

75. See, e.g.: Walker, K. (2017, June 22). Digital security and due process: A new legal framework for the cloud era. Retrieved July 4, 2017, from <http://www.blog.google:443/topics/public-policy/digital-security-and-due-process-new-legal-framework-cloud-era/>

76. Ruiz, D. (2018, March 22). Responsibility Deflected, the CLOUD Act Passes. Retrieved April 10, 2018, from <https://www.eff.org/deeplinks/2018/03/responsibility-deflected-cloud-act-passes>

“First, the CLOUD Act creates the authority and framework for the U.S. to establish international agreements that on a reciprocal basis will enable law enforcement agencies to access data in each other’s countries to investigate and prosecute crimes. These 21st century agreements will supplement the older and slower Mutual Legal Assistance Treaties, or MLATs, that governments around the world understandably have been complaining about. These new agreements can combine digital and other modern processes to enable law enforcement to work effectively and quickly.

Second, the CLOUD Act protects privacy and other human rights by stipulating that these international agreements can only be established with countries that protect privacy and other human rights and by subjecting the Executive Branch’s assessment of these aspects to congressional review (...).

Third, the CLOUD Act creates strong norms to govern surveillance requests in the new international agreements. These effectively incentivize governments to update their digital privacy laws to ensure that law enforcement requests are narrow, incorporate specific rule of law protections, are subject to judicial review or oversight, and meet baseline legal standards around accountability and transparency.

Fourth, the CLOUD Act ensures that these new international agreements will not become vehicles for requiring cloud service providers to create back doors to break encryption. The Act states explicitly that terms of these agreements “shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data.”<sup>77</sup>

Despite these reassurances, the fact remains that the CLOUD Acts furthers entrenches the privatization of the justice system, by giving to tech companies the only possibility to oppose a specific access request from a third country after the US government has passed a bilateral agreement with that country, where MLAT procedures entrusted judges with that task. Also, it gives a new leverage to the US government (the fact of granting a third country a bilateral agreement under the CLOUD Act) which will likely be used to further the diplomatic interests of the US at the expense of human rights. These are just some of the most obvious problems of a text that is reaped with ambiguities.<sup>78</sup>

In Europe, the adoption of the CLOUD Act has raised concerns considering the upcoming proposal for a “directive on electronic evidence,” presented on April 17<sup>th</sup>, 2018.<sup>79</sup> EU Justice Commissioner Vera Jourova reacting by bemoaning the US move which narrows down the range of options available to European lawmakers and in effect pre-empt their debate: “Unfortunately,” she said, “the US Congress has adopted the US Cloud Act in a fast-track procedure, which narrows the room for the potential compatible solution between the EU and the US,” she said in a statement.”<sup>80</sup> The timing indeed suggests that this was precisely the goal of this rushed adoption. The UK and the US

---

77. Smith, B. (2018, April 3). The CLOUD Act is an important step forward, but now more steps need to follow. Retrieved April 9, 2018, from <https://blogs.microsoft.com/on-the-issues/2018/04/03/the-cloud-act-is-an-important-step-forward-but-now-more-steps-need-to-follow/>

78. See: Singh Guiliani, N., & Shah, N. (2018, March 16). The CLOUD Act Doesn’t Help Privacy and Human Rights: It Hurts Them. Retrieved April 10, 2018, from <https://lawfareblog.com/cloud-act-doesnt-help-privacy-and-human-rights-it-hurts-them>

79. Security Union: Commission facilitates access to electronic evidence. (2018, 417). Retrieved April 19, 2018, from [http://europa.eu/rapid/press-release\\_IP-18-3343\\_en.htm](http://europa.eu/rapid/press-release_IP-18-3343_en.htm)

80. Nielsen, N. (2018, March 26). Rushed US Cloud Act triggers EU backlash. Retrieved April 10, 2018, from <https://euobserver.com/justice/141446>

have, for the past two years, been negotiating an agreement that will now be updated to respect the new US legal framework. The EU Commission is expected to follow suit on similar negotiations.

### **The limits of resistance: the extractive data economy and the Snowden paradox**

These three different types of resistance made the news. But here and there, one could also see that much of what these actors could have done to better protect privacy was simply not done.

On the issue of encryption for instance, much of the efforts of large communication provider consisted in respecting the state of the art. They did not go much further. In launching new products for instance, they often disregarded implementing strong encryption by default. It was the case of Google with its new messaging service called Allo. A FBI source reacted to the news by saying that “having this as an opt-in feature is certainly useful to us”.<sup>81</sup> Sometimes, like in the case of Microsoft’s Skype, significant changes in the functioning of the software failed to introduce any new protection for privacy, and no indication was given regarding the use of encryption.<sup>82</sup> The strong encryption features, even when they are used by default, only relate to content, which allows the companies to mine metadata and still extract many information that is useful on their consumers’ behavior to serve them with targeted advertising, and which can be handed over to law enforcement.<sup>83</sup> The fact is that much of the digital economy is built on personal data and profiling (Casilli, 2017; Fuchs, 2013; Fuchs & Trottier, 2015), and the protection of users privacy must always be balanced against that reality. Despite the privacy-by-design pledges and internal review mechanisms, the business-models of these companies and the very nature of modern-day technologies like Artificial Intelligence create inescapable limits on what we have referred to here as “technical resistance.”

Even when encryption may render some surveillance techniques less attractive to intelligence agencies (for instance Deep Packet Inspection techniques), the fact remains that these companies are territorially headquartered and infrastructurally anchored in the US make them prone to the full legal power of US authorities.

Yahoo’s roll-out of SSL encryption on its products in 2014 made real-time surveillance of its traffic from backbone networks impracticable. So intelligence agencies issued a directive – presumably authorized by the FISC – forcing that traffic scanning to take place from within Yahoo’s data centers, according to the revelations made by Reuters in October 2016:

“Yahoo Inc last year secretly built a custom software program to search all of its customers’ incoming emails for specific information provided by U.S. intelligence officials, according to people familiar with the matter.

---

81. Nakashima, E., & Tsukayama, H. (May 2016). People like Edward Snowden say they will boycott Google’s newest messaging app. Retrieved May 23, 2016, from <https://www.washingtonpost.com/news/the-switch/wp/2016/05/21/why-people-like-edward-snowden-say-they-will-boycott-googles-newest-messaging-app/>

82. Bright, P. (2016, July 20). Skype finalizes its move to the cloud, ignores the elephant in the room. Retrieved July 20, 2016, from <http://arstechnica.com/information-technology/2016/07/skype-finalizes-its-move-to-the-cloud-ignores-the-elephant-in-the-room/>

83. Biddle, S. (2016, September 28). Apple Logs Your iMessage Contacts — and May Share Them With Police. Retrieved September 29, 2016, from <https://theintercept.com/2016/09/28/apple-logs-your-imessage-contacts-and-may-share-them-with-police/>

Fox-Brewster, T. (2017, January 22). Forget About Backdoors, This Is The Data WhatsApp Actually Hands To Cops. Retrieved February 21, 2018, from <https://www.forbes.com/sites/thomasbrewster/2017/01/22/whatsapp-facebook-backdoor-government-data-request/>

Rees, M. (2016, July 21). Windows 10 : pourquoi la CNIL met en demeure Microsoft. Retrieved July 21, 2016, from <http://www.nextinpact.com/news/100719-windows-10-pourquoi-cnil-met-en-demeure-microsoft.htm>

The company complied with a classified U.S. government demand, scanning hundreds of millions of Yahoo Mail accounts at the behest of the National Security Agency or FBI, said three former employees and a fourth person apprised of the events.

Some surveillance experts said this represents the first case to surface of a U.S. Internet company agreeing to an intelligence agency's request by searching all arriving messages, as opposed to examining stored messages or scanning a small number of accounts in real time.

It is not known what information intelligence officials were looking for, only that they wanted Yahoo to search for a set of characters. That could mean a phrase in an email or an attachment, said the sources, who did not want to be identified.”<sup>84</sup>

In this case, what is interesting to note is that Reuters' source indicate the company's board and general counsel failed to implicate the information security team, which found the scanning program a few week after its installation eventually led to the departure of Yahoo's Chief Information Security Officer Alex Stamos.<sup>85</sup> This suggests that even through they may have been put at the forefront of the public-relation strategies of the companies to rebuilt user trust, information security personnel remain rather weak at the board level. Also, Reuters' revelations came one month after the company had revealed that in 2014, “state-sponsored” hackers had access to 500 million customer accounts. What is also interesting is that Yahoo apparently did not challenge the directive as it had in 2007. According to Reuters, “Mayer and other executives ultimately decided to comply with the directive last year rather than fight it, in part because they thought they would lose.” Asked whether they had received similar surveillance orders, other companies (which most likely would not be legally allowed to say if it were the case) said that they had not. Google and Apple made clear that if they had, they would have challenged them in court.<sup>86</sup>

When it comes to legal and political resistance, they too have their limits. The case of the US indeed confirms that despite an increased degree of transparency, surveillance reform introduced since 2013 in liberal regimes with powerful intelligence agencies leads to what we have called a “Snowden paradox” (Tréguer, 2017a): Intelligence reform, rather than rolling-out capacities for large-scale and suspicionless surveillance, has provided a detailed legal basis for these capacities, bringing a few new safeguards and slightly decreasing the level of secrecy to secure their legality and legitimacy.

As we have seen, the main progress has been on the front of transparency. But the USA Freedom

---

84. Reuters. (2016, October 4). Yahoo secretly scanned customer emails for US intelligence-sources. Retrieved October 5, 2016, from <http://www.reuters.com/article/us-yahoo-nsa-exclusive-idUSKCN1241YT>

85. According to Reuters: “Some Yahoo employees were upset about the decision not to contest the more recent edict and thought the company could have prevailed, the sources said. They were also upset that Mayer and Yahoo General Counsel Ron Bell did not involve the company's security team in the process, instead asking Yahoo's email engineers to write a program to siphon off messages containing the character string the spies sought and store them for remote retrieval, according to the sources. The sources said the program was discovered by Yahoo's security team in May 2015, within weeks of its installation. The security team initially thought hackers had broken in. When Stamos found out that Mayer had authorized the program, he resigned as chief information security officer and told his subordinates that he had been left out of a decision that hurt users' security, the sources said. Due to a programming flaw, he told them hackers could have accessed the stored emails. Stamos's announcement in June 2015 that he had joined Facebook did not mention any problems with Yahoo.”

86. Conger, K. (n.d.). Twitter, Microsoft, Google and others say they haven't scanned messages like Yahoo. Retrieved October 5, 2016, from <http://social.techcrunch.com/2016/10/04/twitter-microsoft-and-google-say-they-havent-scanned-messages-like-yahoo/>

Act for the first time codifies the principle of bulk collection in US law.<sup>87</sup> The legislative changes around NSL allowing a judge to review attached gag orders has been selectively used by companies like Google and Facebook.<sup>88</sup> These and other reforms had no actual effect on limiting large-scale surveillance conducted by US intelligence. Consider these take-aways from the 2016 transparency report published by the Office of the Director of National Intelligence (ODNI) in March 2017:

- “Even after steps were taken to reduce the collection of phone call metadata—ending bulk collection of phone company records and limiting collection to specific requests against records held by telecommunications providers—the National Security Agency collected over 151 million phone call records while tracking only 42 targets.
- The number of Foreign Intelligence Surveillance Court (FISC) "probable cause" orders [for people inside the US] issued per year has stayed relatively steady, with 1,559 orders issued by FISC applying to an estimated 1,687 targets—336 of whom are "US persons." However, the total number of "targets" tracked through Internet surveillance and other means under FISA's Section 702 has steadily climbed well beyond that, reaching a total of 106,469 tracked individuals in 2016.
- The number of queries against the data collected through Internet taps for information about Americans by the NSA and CIA also grew year over year in 2016. The report estimated that 5,288 "known US person" searches were conducted against content gathered with "upstream" collection—up from 4,672 in 2015.
- A more accurate count of the number of times the intelligence community searched for information on Americans comes from the report's "estimated number of queries concerning a known US person of unminimized noncontents information"—in other words, searches specifically looking for Americans by identifying metadata, such as name or phone number. In 2013, there were 9,500 of these; by 2016, that number had grown to 30,335.”<sup>89</sup>

As was repeatedly said since 2013 – and during our interviews (Appendix 1) –, the resistance strategies of Big Tech firms were already ongoing before Snowden. For many companies – especially those like Yahoo who had already faced human rights scandals –, there was already an understanding of the fact that secrecy and lack of public knowledge on the reality of the large-scale surveillance capacities and the lack of appropriate safeguards undermined their reputation. The Snowden disclosures only intensified them and pushed companies to put these fights in the public realm in order to restore user trust. According to an executive from Facebook who was not working there at the time of the first disclosures:

“The change that the Snowden revelations did for my colleagues was that suddenly those topics, which were part of a long list of topics we were covering, were pushed

---

87. Sacks, S. (2015, May 13). USA Freedom Act Passes House, Codifying Bulk Collection For First Time, Critics Say. Retrieved August 31, 2015, from <https://theintercept.com/2015/05/13/usa-freedom-act/>

88. According to EFF: ““While a handful of Silicon Valley giants including Apple, Dropbox, Pinterest, and Uber all committed to invoking reciprocal notice for every NSL, we’re disappointed that others, such as Google and Facebook choose only to confront NSL gag orders on a case-by-case basis. The NSL system is broken and companies should invoke reciprocal notice systematically.” Cardozo, N. (2017, July 10). Requiring Judicial Review for Every Gag Order Is a Simple Way to Have Our Backs: Apple Does but Google and Facebook Fall Short. Retrieved February 19, 2018, from <https://www.eff.org/deeplinks/2017/07/requiring-judicial-review-every-gag-order-simple-way-have-our-backs-apple-does>

89. Gallagher, S. (2017, May 3). US Intelligence “transparency report” reveals breadth of surveillance by NSA, others. Retrieved February 20, 2018, from <https://arstechnica.com/tech-policy/2017/05/us-intelligence-transparency-report-reveals-breadth-of-surveillance-by-nsa-others/>

front and center, and that US surveillance reform suddenly became one of the main priority, the legislation we were working on and most of our lobbying efforts were being directed toward that topic” (Appendix 1).

Oftentimes, media coverage overly emphasised the antagonism between private actors and the government. For instance, commenting on the Apple-FBI fights and the unwillingness of the Obama administration to introduce legislation to limit encryption, Benjamin Wittes, editor in chief of Lawfare and a Senior Fellow in Governance Studies at the Brookings Institution, said it provided “a vivid illustration of how overrated the power of the so-called national security state really is when its interests don't coincide with those of Silicon Valley.”<sup>90</sup> That statement seems exaggerated, as one key lesson of the internal White House memo that Wittes comments in this post is also that the government clearly contemplated the possibility of “voluntary assistance,” possibly in a “private” way to avoid the chilling effects that publicity might have on such cooperation. We know from the Snowden archives that prior to 2013, the NSA spends \$250 million a year to work with tech companies to make commercial software – and in particular encryption software – more exploitable.<sup>91</sup> Regarding the FBI-Apple dispute, research actually suggests that compared to the encryption debates of the 1990s, the camp of those defending “strong encryption” matured, diversified and put forward new-found arguments regarding the importance of encryption (Schulze, 2017). It also counted prominent supporters from “deep state” circles at the NSA or the Pentagon, which can likely be attributed to the growing importance of the cybersecurity field within it.

So rather than overemphasising the divide between public and private actors, these traditional distinctions deserve to be blurred and the complex struggles and negotiation processes regarding surveillance put in a broader context. What we are pointing at is the fact that despite the “staged resistance” in the aftermath of Snowden, large technology companies remain increasingly tied to national security policies. In that process, they are only fostering their integration in the field of the state and, besides surveillance, there are plenty of other issues on which the state officials in the security field and technology companies can see eye to eye.

This is true of another national security issue that has strong adverse effects on human rights: the censorship of another national security issue also problematic from a human rights perspective but less sensitive in terms for public relation, that of online terrorist content. In the US and Europe, there has been a growing pressure on online service providers to police the content shared by their users in a extra-judicial setting, and companies have reacted by hiring more staff, subcontracting companies, and developing automatic filtering tools. Despite human right concerns, that cooperation is taking place without any legal pressure being leveraged against the companies.

Ahead of a meeting in the Silicon Valley in February 2016 between Cabinet members, intelligence officials and tech companies, the then White House press secretary Josh Earnest told reporters that “many of these technology companies that are participating in the meeting today are run by patriotic Americans and would want to cooperate.”<sup>92</sup> A key aspects of the discussion laid in understanding

---

90. Wittes, B. (2015, September 18). The Obama Administration’s Encryption Wrangling. Retrieved February 19, 2018, from <https://www.lawfareblog.com/obama-administrations-encryption-wrangling>

91. Borger, J., Ball, J., & Greenwald, G. (2013, September 6). Revealed: how US and UK spy agencies defeat internet privacy and security. Retrieved February 22, 2018, from <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>

92. Quoted in: Jose, D. Y. J. C. W. in S., & California. (2016, January 8). Silicon Valley appears open to helping US spy agencies after terrorism summit. *The Guardian*. Retrieved from

how technology could be used to boost censorship and propaganda efforts.<sup>93</sup> A few months later, companies like Google and Facebook were announcing major innovations in their efforts on extra-judicial automated censorship – something that the government would not be able to do considering the “First amendment” issues raised by such policies: Reuters reported that “some of the web’s biggest destinations for watching videos have quietly started using automation to remove extremist content from their sites.”<sup>94</sup> There was no public comment from the company, somewhat contradicting their pledge to transparency.

### **Completing the integration of Big Tech to the US state in the age of “data governance”**

In its seminal work on the “power elite” (Mills, 1959), U.S. sociologist Charles Wright Mills observed the power positions in the political, economic and military sectors to conclude that there was a triangle of power, within which a small number of people could occupy power positions that were interchangeable and circulating. Mills noted in particular that proximity of business and government officials could be seen by the ease and frequency with which men passed from one realm to another, – a phenomenon that became known as the “revolving door”. He also asserted that the growing structural integration of these three sectors was the result of each of the elite domains becoming both larger and more centralized, and increasingly integrated with other spheres.

Now, the companies on which this deliverable focuses on have become in less than three decades the highest market valuations globally. Tech is now the largest sector in global capitalization, amounting to 3,582\$bn, before financials (3,532\$bn), consumer goods (2,660\$bn), health care (2,300\$bn), oil & gas (1,411\$bn) or telecommunications (859\$bn).<sup>95</sup>

---

<http://www.theguardian.com/technology/2016/jan/08/technology-executives-white-house-isis-terrorism-meeting-silicon-valley-facebook-apple-twitter-microsoft>

93. The agenda of the meeting listed the following questions: “How can we make it harder for terrorists to leveraging the internet to recruit, radicalize, and mobilize followers to violence?”

b. How can we help others to create, publish, and amplify alternative content that would undercut ISIL?

c. In what ways can we use technology to help disrupt paths to radicalization to violence, identify recruitment patterns, and provide metrics to help measure our efforts to counter radicalization to violence?

d. How can we make it harder for terrorists to use the internet to mobilize, facilitate, and operationalize attacks, and make it easier for law enforcement and the intelligence community to identify terrorist operatives and prevent attacks?” <https://www.theguardian.com/technology/2016/jan/07/white-house-summit-silicon-valley-tech-summit-agenda-terrorism>

94. Menn, J., & Volz, D. (2016, June 25). Exclusive: Google, Facebook quietly move toward automatic blocking of extremist videos. *Reuters*. Retrieved from <http://www.reuters.com/article/us-internet-extremism-video-exclusive-idUSKCN0ZB00M>

See also: Facebook says Artificial Intelligence has sped up removal of terrorist content. (2017, November 29). Retrieved February 22, 2018, from <https://www.usatoday.com/story/tech/2017/11/28/facebook-says-artificial-intelligence-has-spiced-up-removal-terrorist-content/903615001/>

95. PricewaterhouseCoopers. (2017). *Global Top 100 Companies by market capitalisation (31 March 2017 update)*. Retrieved from <https://www.pwc.com/gx/en/audit-services/assets/pdf/global-top-100-companies-2017-final.pdf>

Rank	Company	Region	Industry Segment	Current Market Value (\$B)	2016 Revenue (\$B)
1	Apple	USA	Tech – Hardware	\$801	\$218
2	Google / Alphabet	USA	Tech – Internet	680	90
3	Microsoft	USA	Tech – Software	540	86
4	Amazon	USA	Tech – Internet	476	136
5	Facebook	USA	Tech – Internet	441	28
6	Berkshire Hathaway	USA	Financial Services	409	215
7	Exxon Mobil	USA	Energy	346	198
8	Johnson & Johnson	USA	Healthcare	342	72
9	Tencent	China	Tech – Internet	335	22
10	Alibaba	China	Tech – Internet	314	21
11	JP Morgan Chase	USA	Financial Services	303	90
12	ICBC	China	Financial Services	264	85
13	Nestlé	Switzerland	Food / Beverages	263	88
14	Wells Fargo	USA	Financial Services	262	85
15	Samsung Electronics	Korea	Tech – Hardware	259	168
16	General Electric	USA	Industrial	238	120
17	Wal-Mart	USA	Retail	237	486
18	AT&T	USA	Telecom	234	164
19	Roche	Switzerland	Healthcare	233	51
20	Bank of America	USA	Financial Services	231	80
<b>Total</b>				<b>\$7,207</b>	<b>\$2,497</b>

Table : 2017 Global Market Capitalization (Source: CapIQ. Market value data as of 5/26/2017).

Not only are Silicon Valley companies dominating the global world of business, their influence of politicians has reached impressive proportions. In the US, the strong relationship between Google and the Obama administration and the Democratic Party has been well documented. Eric Schmidt, Executive Chairman of Google from 2001 to 2017 and of Alphabet Inc. from 2015 to 2017, became a member of President Obama's transition advisory board, before joining the President's Council of Advisors on Science and Technology (PCAST). He was joined to that latter position by Adrian Aoun, Google Artificial Intelligence's chief. As for Google Internet Evangelist Vint Cerf, he was appointed to the National Science Board (2013-2018); while former Google board member and venture capitalist John Doerr seated on the now defunct President's Council on Jobs and Competitiveness and President's Economic Board (2009-2013).

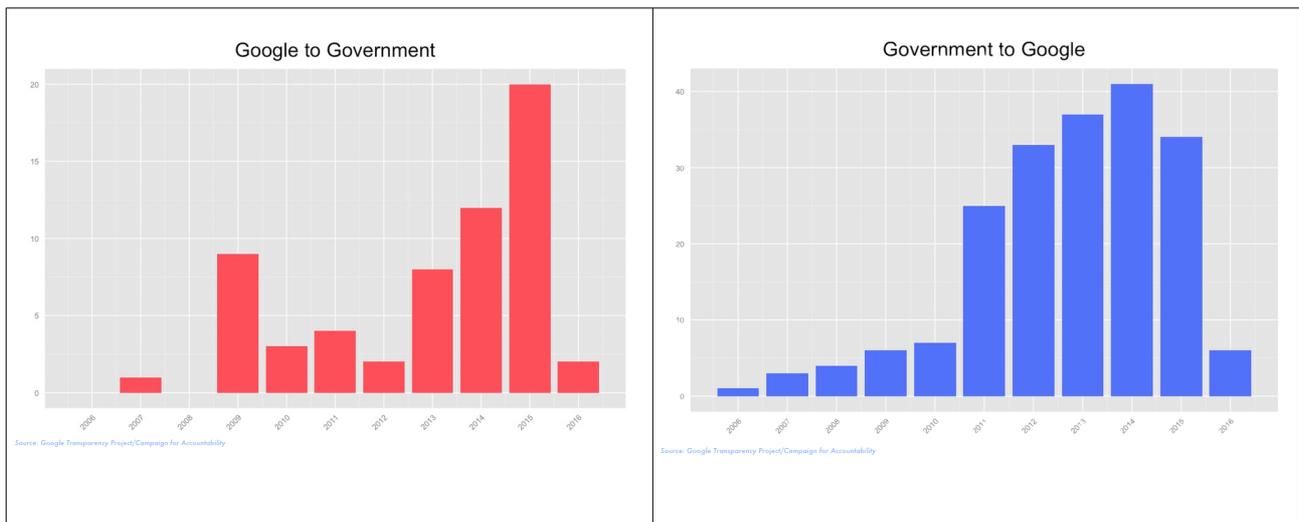
But this fact speaks to a much broader trend, documented by the US-based Campaign for Accountability who worked on the growing exchanges of personnel between Google and governments on both sides of the Atlantic through its "Google Transparency Project".<sup>96</sup> According to the project:

"The Google Transparency Project has so far identified 258 instances of "revolving door" activity (involving 251 individuals) between Google or related firms, and the federal government, national political campaigns and Congress during President Obama's time in office. That included:

- 53 revolving door moves between Google and the White House. Those involved 22 former White House officials who left the administration to work for Google, and 31 Google executives (or from Google's main outside firms) who joined the White House, or were appointed to federal advisory boards.

96. <https://googletransparencyproject.org/>

- 28 revolving door moves between Google and government positions involving national security, intelligence or the Department of Defense. Seven former national security and intelligence officials and 18 Pentagon officials moved to Google; while three Google executives moved to DoD.
- 23 revolving door moves between Google and the State Department during the Obama administration. Eighteen former State Department officials joined Google, while five Google officials took up senior posts at the State Department.
- 9 moves between Google and its outside lobbying firms and the Federal Communications Commission, which handles a growing number of regulatory matters with a major impact on the company’s bottom line.”<sup>97</sup>



97. Google’s Revolving Door (US). (2017). Retrieved February 13, 2018, from <https://googletransparencyproject.org/articles/googles-revolving-door-us>

Number of career moves between the U.S. government and Google (and vice versa) between 2006 and 2016. Source : Google Transparency Project/Campaign for Accountability

Now, in the aftermath of Trump's election, many have described as growing divorce between the incoming Republican administration and the tech industry. In December 2016, Trump supporter and venture capitalist Peter Thiel organized a meeting between leader of the tech industry and the then President-elect. Attendees included Microsoft CEO Satya Nadella, Apple CEO Tim Cook, Jeff Bezos of Amazon and The Washington Post, Larry Page and Eric Schmidt of Alphabet and Google, Facebook COO Sheryl Sandberg, Elon Musk of Tesla and SpaceX, Oracle CEO Safra A. Catz, Microsoft CEO Satya Nadella, Intel CEO Brian Krzanich, Cisco CEO Chuck Robbins, and IBM CEO Ginni Romett. Trump commented about the pro-Democratic leanings of these companies, and what he saw as a boost in popularity among them after his elections. "They're all talking about the bounce. So right now everybody in this room has to like me – at least a little bit – but we're going to try and have that bounce continue," he said.<sup>98</sup> Later on, there would be widespread criticisms coming from the tech industry regarding Trump's immigration and climate policies.<sup>99</sup>

But at many level of the US government, the integration of large tech firms in the administrative field in advancing. This began under the Obama administration, as analysed by Evgeny Morozov (Morozov, 2013), and continues to this day. In late-March 2017, Donald Trump signed a memorandum order establishing the "American Technology Council", an initiative led by its son-in-law and Senior Advisor Jared Kushner to modernize the US public sector.<sup>100</sup> The Council includes cabinet members and staffers, including the Secretary of Defense, the Secretary of Commerce, the Director of National Intelligence, and the U.S. Chief Technology Officer. During the first meeting of the council, in April, Apple CEO Tim Cook, IBM CEO Ginni Rometty, Microsoft CEO Satya Nadella, Amazon CEO Jeff Bezos, and Oracle co-CEO Safra Catz. In June 2017, the White House organized its "tech week". This is an account of the meeting that speaks to the sort of issues discussed then:

"Building on work that began under Obama, the Trump White House believes federal agencies should behave more like the private sector, not just in the way they buy and use technology but in the services they offer citizens who need to interact with Washington.

For the nation's tech heavyweights, however, those reforms aren't just the stuff of a modern, digitally minded government — they're also potential business opportunities. And executives like Cook, Schmidt and Bezos sought to shape the Trump administration's thinking on those issues during an afternoon of closed-door

---

98. Jardin, X. (2016, December 14). Trump meets with tech leaders: Apple, Facebook, Google, Amazon, IBM, Microsoft, Oracle, Tesla, Intel. Retrieved December 15, 2016, from <https://boingboing.net/2016/12/14/trump-meets-with-tech-elite-fr.html>

99. Isaac, D. S., Mike, & Benner, K. (2017, January 29). Silicon Valley's Ambivalence Toward Trump Turns to Anger. *The New York Times*. Retrieved from <https://www.nytimes.com/2017/01/29/technology/silicon-valleys-ambivalence-toward-trump-turns-to-anger.html>

Kerstetter, J. (2017, June 2). Tech Roundup: Divide Between Trump and Silicon Valley Grows. *The New York Times*. Retrieved from <https://www.nytimes.com/2017/06/02/technology/tech-roundup-divide-between-trump-and-silicon-valley-grows.html>

100. O'Brien, S. A. (2017, May 1). Trump creates American Technology Council to "modernize" federal digital services. Retrieved February 22, 2018, from <http://money.cnn.com/2017/05/01/technology/trump-american-technology-council/index.html>

brainstorming sessions.

A session on cloud computing, for example, featured some of the industry's leading players: Keith Block, the chief operating officer and president of Salesforce, as well as the chiefs of Intel and IBM, multiple sources confirmed to Recode. They discussed the ways the U.S. government can cut down on some 6,000 costly data centers in its control and shift those responsibilities to the private sector, a move that could mean a windfall for any tech company that might someday win such contracts.

The Trump administration also focused on federal procurement — and it devoted a brainstorming workshop to the sort of reforms the White House can proffer to make it easier for the U.S. government to buy the most cutting-edge tools on the market.

There, it was the likes of some of Washington's most aggressive tech sellers — like Palantir, which provides its data-sifting tools to U.S. national security agencies — offering their thoughts on ways to lower barriers, sources told Recode. Amazon and Oracle also attended those sessions.

One of Silicon Valley's leading venture capitalists, John Doerr, even brought the leader of one of his portfolio companies — Nuna Health — to the procurement meeting. The firm, run by Jini Kim, compiles and extracts insights from health care data, specifically from Medicaid. And speaking later at a public roundtable with the president, Doerr urged Trump to be the “data liberation administration” — releasing more of the government's stores of data, particularly around health care, for private-sector use.

“If you set the data free,” he said, “the entrepreneurs can do the rest.”<sup>101</sup>

Eric Schmidt, then the executive chairman of Google's parent company Alphabet, said that Trump helped foster “a huge explosion of new opportunities.” As suggested by the Google Transparency Project, Schmidt's behavior since the election of Trump has been that of a mediator of a corporation, and even a whole industry increasingly “ingratiating itself with the Trump administration while cashing on the resistance.”<sup>102</sup>

These reconfiguring public-private assemblages designed for the age of “data governance” are also developing in the national security field. In March 2016, Schmidt was also appointed by Ash Carter, then Secretary of Defense, as chairman of the Defense Innovation Board (DIB) of the Department of Defense, a position that he still holds at the time of writing despite him quitting its official positions at Alphabet/Google in January 2018.<sup>103</sup> On its webpage, the DIB is described as an innovation think-tank:

“Through pilot programs and experiments within DoD, the DIB can bring in new perspectives from the private sector and academia, work with DoD partners to test

---

101. Romm, T. (2017, June 20). Behind the scenes at President Trump's private talks with the tech industry. Retrieved June 21, 2017, from <https://www.recode.net/2017/6/20/15838646/trump-apple-amazon-google-microsoft-tech-week>

102. Google ingratiates itself with the Trump Administration... While cashing in on the resistance. (2017). Retrieved February 13, 2018, from <https://googletransparencyproject.org/articles/google-ingratiates-itself-trump-administration>

103. Gabrielle, L., & Georeen, T. (2018, January 22). US military, Silicon Valley: Partnership will revolutionise the battlefield. Retrieved February 13, 2018, from <http://www.foxnews.com/tech/2018/01/19/us-military-teams-up-with-silicon-valley-to-revolutionize-battlefield.html>

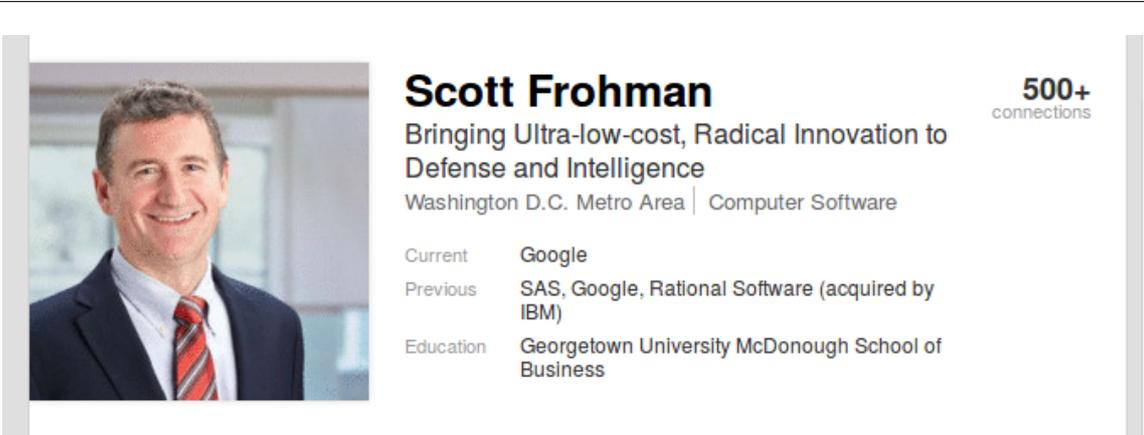
Pellerin, C. (2017, October 25). Defense Innovation Board Chair: Recommendations Making an Impact. Retrieved February 13, 2018, from <https://www.defense.gov/News/Article/Article/1353822/defense-innovation-board-chair-recommendations-making-an-impact/>

hypotheses, gather data, and encourage the imagination and critical thinking need to consider new solutions. This process is rapid, creative, collaborative, and ultimately saves time and money.”<sup>104</sup>

In one of its recommendation entitled “Forge New Approach to Data Collection, Sharing, and Analysis”, the DIB makes the following analysis of the importance of data to 21<sup>st</sup> century statehood:

“Data is the 21st century equivalent of a global natural resource, like timber, iron, or oil previously – indispensable for sustaining military innovation and advantage. The next global conflicts will be fueled by data. The rapidly expanding power of new mathematical and computing techniques to reveal insights into intentions and capabilities, and to enhance accuracy, lethality, and speed, depend on immense data sets to train algorithms and from which to extract information. The data that provide the raw materials from which to identify patterns, as well as the anomalies that defy them, constitute the fuel that powers the engine of Machine Learning (ML). Whoever amasses and organizes the most data first will sustain technological superiority, so it is incumbent upon the Department to collect, store, share, analyze, and protect its data faster and better than its competitors. Data must be regarded as one of the most powerful resources in the Department’s arsenal.”<sup>105</sup>

Companies like Google indeed and their executives are selling solutions that are aimed at expanding the technological superiority and “efficiency” of these apparatus at “ultra-low-coast” (see below). According to the LinkedIn profile of Scott Frohman, “through the use of Google's capabilities remade for the enterprise, the government gets innovation fast and with significantly reduced cost.”



Caption of the LinkedIn profile of Scott Frohman, Google’s Director of Defense and Intelligence Sales since April 2017 (june 2018).

Data and algorithmic governmentality are becoming the norm of bureaucratic procedures, leading to new organizational patterns that heavily rely on the experience of the technology sector. In France too, the same logic can be seen.

104. <http://innovation.defense.gov/Recommendations/>

105. Recommendations Defense Innovation Board. (October 2017). Retrieved February 22, 2018, from <http://archive.is/IXaXR>

## 3.2 France: Facing established public-private alliances

In the US, one could argue that online service providers and software editors started from positions very external to the US government. But if the PRISM slides – or the increasing lobbying of these companies in Washington DC – are any indication, their progressive integration to the US state apparatus was engaged more than a decade ago.

In France, this process was still in a very early phase when the Snowden disclosures started in mid-2013. At first, the disclosures only reinforced existing public-private assemblages. Business and regulatory stakes further complicated the matter, giving US tech companies much less leeway to stage resistance.

### A first and failed attempt at resistance

As we have explained elsewhere (Tréguer, 2017a), legal controversies around communications surveillance did not start with Snowden. In the 1980s, several scandals and condemnations of France by the European Court of Human Rights (ECHR) has already led to the adoption of basic legal framework for extra-judicial state surveillance. In 2001 and 2006, the adoption of blanket data retention and access to metadata for anti-terrorism purposes re-ignited the debate. But generally speaking, the secrecy surrounding intelligence activities and the general lack of interest of much of the human rights field ensured that telecom companies – and in particular the former state monopoly Orange – and the state could cooperate, even outside of a proper legal framework, to advance the capacities of intelligence agencies. Hosting providers – the legal status that most US tech companies surveyed in the report have in France – had to provide subscriber information upon request, but for the most part, they remained a marginal component of the public-private dispositifs used to monitor Internet communications.

French national security policymakers were very much aware that the existing framework failed to comply with the standards of the European Court of Human Rights (ECHR). And so intelligence reform was announced for the first time in 2008, under the presidency of Nicolas Sarkozy (2007-2012). But the reform then lingered, which in turn created the political space for the parliamentary opposition to carry the torch. By the time the Socialist Party got back to power, in 2012, its officials in charge of security affairs were the ones pushing for a sweeping new law that would secure the work of people in the intelligence community and, incidentally, put France in line with democratic standards.

Then came Edward Snowden. At first, the Snowden disclosures deeply destabilized these plans, creating a new dilemma for the proponents of legalization: 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 legalization. But on the other hand, they had put the issue of surveillance at the forefront of the public debate and therefore made such a legislative reform politically risky and unpredictable.

In late 2013, a first attempt at partial legalization (widening access to metadata) gave rise to new coordination within civil society groups opposed to large-scale surveillance, which reinforced these fears. Ironically, the controversies was started by a trade group that included companies like Google and Microsoft. The *Loi de programmation militaire* (or LPM, a military planning bill) had been

debated in Parliament since October 2013, and an amendment was introduced in the Senate to vastly expand the range of metadata accessible to intelligence agencies, including in real-time, apparently to legalize some of the “deep packet inspection” techniques that intelligence agencies had been experimenting since 2009.<sup>106</sup>

It shouldn't have, but the amendment did come as a surprise to many in the advocacy sphere, to the extent that it even went unnoticed for quite some time. Eventually, on November 20<sup>th</sup>, the *Association des services de l'Internet communautaire* (ASIC) –a professional lobbying organization representing online social services including Google France, AOL, eBay, Facebook, Microsoft, Skype and French companies like Deezer or Dailymotion– released a brief on article 13.<sup>107</sup> The later was framed as an infringement on the right to privacy, and ASIC called on the government and lawmakers to adopt a “moratorium” on any text creating “rules of exception” for accessing users' data. ASIC also started a petition to relay these calls on the platform change.org (the later would end up only 45 “supporters”).

At first, only minor online tech media relay these calls. But six days later, on November 26<sup>th</sup>, the prominent conservative news-paper Le Figaro releases a sensationalist article entitled: “Telephone, Internet: The State Will Soon Be Able to Spy on Everything.”<sup>108</sup> The article relayed the analysis of ASIC, with quoted of the organization's head.

On December 3<sup>rd</sup>, the leading (though relatively small) French digital rights advocacy group, La Quadrature du Net, finally reacted with a press release (both in French and English) denouncing article 13: “How is it possible,” it asked, “that after only a few months of Edward Snowden's revelations the French government proposes a bill so detrimental to our fundamental rights?” It was relayed by the anglophone and influential tech blog Boing Boing.

The next day, on December 4<sup>th</sup>, the Minister of Digital Affairs, Fleur Pellerin, was interviewed in Le Monde. The interview's headline stressed that, since the first Snowden disclosure, she was “the first member of the government to react on surveillance of the digital sphere.” In the interview, Pellerin introduced what would become an important justification in the coming months (both in intelligence policy debate and cybersecurity debates): Pellerin framed the Snowden disclosures – which had documented the role of Silicon Valley corporations in US surveillance programs– as a confirmation that these “hegemonic” private actors were a major threat for privacy and broader European interests, casting their defense of digital rights in France as a sign of their double-dealing on the issue

The mobilization against article 13 was short and intense, but it eventually failed. Despite an attempt at public resistance, US tech companies would soon face an hostile context fueled by securitization discourse from French officials and their local competitors, leading them to tread much more carefully and discretely on these issues.

---

106. Tréguer, F. (2017, November 15). Renseignement : derrière le brouillard juridique, la légalisation du Deep Packet Inspection. Retrieved from <https://halshs.archives-ouvertes.fr/halshs-01649986/document>

107. Association des Sites Internet Communautaires Internet Communautaires. (2016, March 18). Surveillance de l'Internet, accès aux données d'utilisateurs : pour un moratoire sur les régimes d'exception. Retrieved January 18, 2017, from <http://archive.is/firXs>

108. Leclerc, J.-M. (2013, November 25). Téléphone, Internet: l'État pourra bientôt tout espionner. Retrieved March 18, 2016, from <http://www.lefigaro.fr/actualite-france/2013/11/25/01016-20131125ARTFIG00570-telephone-internet-l-etat-pourra-bientot-tout-espionner.php>

## Immediately post-Snowden, a growing antagonism between the French state and US companies

Three general lines of justification were used by the French government and its private allies to discredit, or weaken, the position and public standing of US tech companies in the aftermath of Snowden.

**“Digital sovereignty”:** The Snowden disclosures, by displaying the secret forms of cooperation between US tech companies and US agencies, led to renewed concerns regarding France’s strategic interest and the fact that these companies with significant market power in France – both for average consumers and many private and public institutions – might in fact be a proxy for the US government. That was for instance the description offered by Bernard Barbier, former technical director at the French Directorate General for External Security (DGSE):

“The Americans feel lie they are ten to fifteen years ahead of us, and put the GAFAs (Google, Apple, Facebook, Amazon] and the old Europe back to back. They have introduced vulnerabilities in a number of tools to turn them into cyber-weapons, and this vulnerability is turned against us. The Americans have no intention to abandon their supremacy and their lead. For them, cyberspace will be the cyberspace of the GAFAs. And the GAFAs are associated with the NSA.”<sup>109</sup>

Another example of similar securization discourse could be found in the 2015 report of the *Secrétariat Général de la Défense et de la Sécurité Nationale* (SGDSN) on “digital security.” After having mentioned state-sponsored and non-state cyberattacks and other forms of cybercriminality and espionage, the report goes on to stress that:

“A new challenge has emerged: the accumulation of digital wealth by an oligopoly of companies using their dominant position to hinder the arrival of new entrants and capture the added value of this emerging economy that will exploit data to invent new services, improve our daily life, or increase the availability of public services. Among this data are first and foremost our personal data, including those attached to our privacy. Mastering this mass of data opens the door to economic destabilization and to sophisticated forms of propaganda, or of guidance of beliefs and habits. In this sense, this challenge – because of its national scale and strategic stakes – directly affects defense and national security.”<sup>110</sup>

These statements must be put in the context of the fierce competition, and fear, that French and other European “legacy” technology companies must face in the digital age, as they try to challenge or resist the domination of US companies. In this regard, the Snowden disclosures allowed these companies and their allies in government to renew their calls for public policies that would reinforce their positions in the digital sector. The argument of “digital sovereignty” thus helped legitimize state subsidies – decided much earlier in 2009 – of €285 millions in two projects of “sovereign clouds” for data storage – one headed by Orange, the other by SFR. These led to

---

109. François, P.-O. (2015, September 21). Cyberattaques : «Beaucoup de pays se font passer pour des Chinois». Retrieved September 6, 2016, from [http://www.liberation.fr/futurs/2015/09/21/beaucoup-de-pays-se-font-passer-pour-des-chinois\\_1387621](http://www.liberation.fr/futurs/2015/09/21/beaucoup-de-pays-se-font-passer-pour-des-chinois_1387621)

110. Secrétariat Général de la Défense et de la Sécurité Nationale. (2015). *La Stratégie nationale pour la sécurité du numérique : une réponse aux nouveaux enjeux des usages numériques*. République française. Retrieved from <http://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/>

commercial failures, despite the fact that other French companies (and that we called “independent” in the introduction) were already offering similar commercial offers.<sup>111</sup> But these were much smaller in size and most importantly much more autonomous from the state – OVH for instance resisted the pressure from the government to unilaterally discontinue its service to WikiLeaks in the midst of the “Cablegate” in December 2010 (Tréguer, 2015) and later opposed the Intelligence Bill.

In 2014, a French executive decree modified article R.153-2 of the Monetary and Financial Code to subject the investments of foreign firms in the field of network security and online communications to the prior approval of the state.<sup>112</sup> In April 2016, the ministry of the Interior also ordered public authorities willing to archive their digital data to do so by using so-called “sovereign clouds”.<sup>113</sup>

At the national and European levels,<sup>114</sup> the adoption of cybersecurity policies since 2011 had led to the formation of new relationships between the administrative field and European companies in business sectors deemed of strategic interest (beyond tech, in the energy, transportation, military sectors) (e.g. (Pohle, Hösl, & Kniep, 2011; Poupard, 2016). The negotiations around the “Network Information Security” (NIS) directive provided an illustration of these trends, with the formation of a European cybersecurity cyber-militaro-industrial complex<sup>115</sup> This echoes processes that had taken place a few years earlier in the United States (Brito & Watkins, 2011), but in Europe these were also fueled by the Snowden controversies from 2013 on.

**Fundamental rights:** The second line of justification was that of fundamental rights. We have already seen how a Minister of François Hollande used them to dismiss the arguments put forward by a trade group comprised of many US companies against the expansion of state surveillance in France. Such a defense line was adopted on many occasions, especially in 2015 during the legislative debate on the Intelligence Bill. Bernard Cazeneuve, the Minister of the Interior, for instance said in mid-April at the National Assembly that the critics of the Bill were missing the real danger:

“The Internet operators hold our personal data, and I’m sure that many of them use extraordinarily intrusive techniques regarding our own existences (...). This does not raise any problem when it is done by big international trusts (...) but when a state offers to prevent terrorism on the Internet, it is suspected of pursuing unworthy ends!”<sup>116</sup>

Even the ruling of the Court of Justice of European Union striking down the “Safe Harbor” agreement between the EU and the US in 2016 would be used to favor the adoption of mandatory

---

111. Cuny, D. (2015, January 13). Le cloud à la française, histoire d’un flop ? Retrieved May 2, 2015, from <http://www.latribune.fr/technos-medias/informatique/20150113triba29598d73/le-cloud-a-la-francaise-histoire-d-un-flop.html>

kitettoa. (2015, March 13). France Cyber Security : une idée française de la sécurité française... : Reflets. Retrieved March 30, 2015, from <http://reflets.info/france-cyber-security-une-idee-francaise-de-la-securite-francaise/>

112. Décret n° 2014-479 du 14 mai 2014 relatif aux investissements étrangers soumis à autorisation préalable. <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028933611&categorieLien=id>

113. [https://francearchives.fr/file/f7ace4517613a246583fd2dd673a0e6d0f86c039/static\\_9151.pdf](https://francearchives.fr/file/f7ace4517613a246583fd2dd673a0e6d0f86c039/static_9151.pdf)

114. See for instance the project of “sovereign cloud” in Germany: Stupp, Catherine. (2015, August 20). Germany to set up “Bundescloud” [Text]. Retrieved August 20, 2015, from

<http://www.euractiv.com/sections/infosociety/germany-set-bundescloud-316939>

115. For an illustration, see for instance: ANON., (2016, January 26). For the first time, the European Cybersecurity Industry Leaders Propose Recommendations Towards European Cybersecurity Policy. In : *Thales Group* [en ligne]. [Consulté le 1 juillet 2016]. Disponible à l’adresse : <https://www.thalesgroup.com/en/critical-information-systems-and-cybersecurity/press-release/first-time-european-cybersecurity>.

116. Tréguer, F. (2015, June). Etats et entreprises à l’assaut de la vie privée. *Le Monde Diplomatique*.

obligations to store digital data regarding European citizens in Europe.<sup>117</sup> French tech companies and their “sovereign cloud” projects were thus framed as a way to better protect the privacy of French citizens.<sup>118</sup>

An interesting – although ill-fated – initiative in this regard was the announce in early 2014: ensuring the encryption of the email services provided French Internet access providers (Orange, SFR-Numéricable, Free, Bouygues and LaPoste.net). A charter to that effect was signed a year later, promising that email communications would be encrypted between French providers. But end-to-end encryption was not in order, which made the announcement a quite deceptive one for privacy advocates. According to the director of the *Agence Nationale pour la Sécurité des Systèmes d’Information* (ANSSI), the cybersecurity agency in charge of negotiating the charter with French providers, it was necessary to ensure that “points in clear” would be available for law enforcement purposes so as to “make encryption and lawful interception co-exist.”<sup>119</sup>

**A “joint responsibility” in the face of terrorism:** The third line of justification reinforcing traditional alliances between security professionals and “legacy” private actors. For instance, in August 2016, Bernard Cazeneuve, France’s interior minister, met his German counterpart Thomas de Maizière to discuss new measures that would limit the use of encrypted communications across the EU, saying it was “a central issue in the fight against terrorism.”<sup>120</sup>

In that context, the European competitors of US tech companies have therefore tried to play the card of contrasting their own approach to national security challenges to that of their US counterparts playing the “resistance” card. As European head of states and law enforcement officials put growing pressure on companies like Whatsapp, Google or Apple whose newly implemented encryption features made surveillance and other investigatory tools less effective, some of the companies with close ties to the government readily affirmed their commitment to voluntarily cooperating with the government.

Stéphane Richard, CEO of Orange – whose close ties with French intelligence have been documented –,<sup>121</sup> for instance lashed at Google for its “encrypted data” going in “that go to data centers we know nothing about.”<sup>122</sup> This language echoes the framing of encryption adopted by the *Service central de l’informatique et des traces technologiques* of the French investigatory police, who shortly after the November 2015 Paris attacks said that “industrial actors, especially American

---

117. Rees, M. (2016, April 29). Les sénateurs interdisent le traitement des données françaises stockées hors Europe. Retrieved April 29, 2016, from <http://www.nextinpact.com/news/99675-les-senateurs-interdisent-traitement-donnees-francaises-stockees-hors-europe.htm>

118. AFP. (2014, July 7). «Big data» : le plan de la France pour concurrencer les géants américains. Retrieved March 24, 2015, from <http://www.lefigaro.fr/secteur/high-tech/2014/07/07/01007-20140707ARTFIG00046-big-data-le-plan-de-la-france-pour-concurrencer-les-geants-americains.php>

119. Champeau, G. (2014, February 20). Les e-mails de France seront chiffrés et stockés en France. Retrieved March 23, 2015, from <http://www.numerama.com/magazine/28502-les-e-mails-de-france-seront-chiffres-et-stockes-en-france.html>

Rees, M. (2015, October 5). Une charte avec les FAI français pour le chiffrement des flux emails. Retrieved October 5, 2015, from <http://www.nextinpact.com/news/96749-une-charte-avec-fai-francais-pour-chiffrement-emails.htm>

120. Jones, S. (2016, August 22). EU spymasters lobby for change in encryption law. *Financial Times*. Retrieved from <http://www.ft.com/cms/s/0/08fe566e-679e-11e6-ae5b-a7cc5dd5a28c.html>

121. Follorou, J. (2014, March 20). Espionnage : comment Orange et les services secrets coopèrent. *Le Monde.fr*. Retrieved from [http://www.lemonde.fr/international/article/2014/03/20/dgse-orange-des-liaisons-incestueuses\\_4386264\\_3210.html](http://www.lemonde.fr/international/article/2014/03/20/dgse-orange-des-liaisons-incestueuses_4386264_3210.html)

122. Graillet, G. (2014, December 11). Le P-DG d’Orange défie Google. Retrieved March 9, 2015, from [http://www.lepoint.fr/economie/le-pdg-d-orange-cogne-sur-google-11-12-2014-1888830\\_28.php](http://www.lepoint.fr/economie/le-pdg-d-orange-cogne-sur-google-11-12-2014-1888830_28.php)

ones, constantly innovate with the purpose of privatizing stored data to make it inaccessible to any third party that does not detain the codes.”<sup>123</sup> Michel Combes, then CEO of the telecom equipment manufacturer Alcatel, said that “it would not be illogic to allow public authorities to know when goes on on the networks, in an appropriate legal framework.”<sup>124</sup>

### **Towards greater cooperation**

These forms of cybersecuritization reinforcing the traditional alliances between the French state and some of its “national digital champions” put US tech companies in an uncomfortable positions. As a matter of fact, during the 2015 debate on the French Intelligence, rather than the full-fledged resistance witnessed in late-2013, or later in the United States and in the UK – although probably to a lesser degree –, gave way to much more discreet forms of opposition. Microsoft, Facebook, Twitter and Google’s lobbyists were invited for a committee hearing.<sup>125</sup> But subsequently, even though French independent companies from the tech sector led a small campaign against the Bill (nicknamed “Ni pigeons ni espions”), US companies did not join.

They would however file an amicus brief in June 2015 when the adopted bill was sent for constitutional review through the trade group ASIC. Other than that, their attitude was one of a readiness to adapt their business practice to restore the confidence of their large account customers. While resisting calls for creating new obligations to store data in France or Europe, US tech companies have been increasingly showcasing their investments in European infrastructures and European digital economies and shield them from US intelligence and law enforcement (a strategy that also explains why the *Microsoft Ireland* case is of such great importance).<sup>126</sup> We will come back on some of these business initiatives, but for the purpose of this deliverable, of even greater importance is these firms’ increasing willingness to cooperate with the French and other European governments on national security issues.

**Streamlining surveillance requests:** Despite the antagonist rhetoric fuelled by European lawmakers like former French minister Bernard Cazeneuve, the collaboration between US tech firms and law enforcement officials have been making important progress in the past few years.

In 2014, France created a new position at the Interior Ministry, that of a so-called “cyber-prefect.”<sup>127</sup> Announced by Cazeneuve, it aimed at coordinating France’s policies with respect to “cyber-threats.” After a position of adviser on cyberthreats to the minister, it would take in January 2017 the form of a decree establishing “interministerial delegate for security industries and the fight against cyberthreats” (*délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces*).<sup>128</sup> The later provides that the delegate shall act:

---

123. Borredon, L., & Untersinger, M. (2016, February 19). Chiffrement : les enjeux du conflit Apple-FBI touchent la police française. Retrieved February 22, 2016, from [http://www.lemonde.fr/pixels/article/2016/02/19/chiffrement-et-terrorisme-les-enjeux-du-conflit-apple-fbi-touchent-la-police-francaise\\_4868385\\_4408996.html](http://www.lemonde.fr/pixels/article/2016/02/19/chiffrement-et-terrorisme-les-enjeux-du-conflit-apple-fbi-touchent-la-police-francaise_4868385_4408996.html)

124. Barroux, D., Counis, A., & Schmitt, F. (2015, March 1). Michel Combes : « Le patriotisme économique n’est pas un gros mot ». Retrieved March 9, 2015, from <http://www.lesechos.fr/tech-medias/hightech/0204190139261-michel-combes-michel-combes-le-patriotisme-economique-nest-pas-un-gros-mot-1097709.php#>

125. <http://www.assemblee-nationale.fr/14/rapports/r2697.asp>

126. Microsoft Announces Plans to Offer Cloud Services from German Datacenters. (2015, November 11). Retrieved March 9, 2018, from <https://news.microsoft.com/europe/2015/11/11/45283/>

127. Lausson, J. (2014, June 5). La France aura son “cyberpréfet.” Retrieved February 11, 2018, from <https://www.numerama.com/magazine/29589-france-cyberprefet.html>

128. Décret n° 2017-58 du 23 janvier 2017 instituant un délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces au ministère de l’intérieur.

<https://www.legifrance.gouv.fr/eli/decree/2017/1/23/INTA1635805D/jo>

“in the framework of the national strategy for digital security and transversal policies of the ministry of the interior, in particular those relative to purchase and to the security and governance of information and communication systems.

In order to develop and protect the industrial and technological capacity of the nation in the field of security and the fight against cyber-threats, he initiates partnerships and defines plans of action at the level of the ministry.

He also ensures the dialogue of the Ministry of the Interior and of the various involved ministries, and between the Ministry of the Interior and public and private actors, such as security industries, including in its international dimension.”

After the Paris attacks of January 2015, Bernard Cazeneuve decided to put greater pressure on US companies. Like the Obama officials would do a few months later, he decided to travel to the Silicon Valley in February 2015 to call for greater cooperation. There, he met with Apple’s Technology Vice-President Bud Tribble, Rachel Whetstone and David Drummond from Google Public Affairs and Business Development teams, but also Facebook and Twitter’s Vice-Presidents for Government Affairs, Elliot Schrage and Colin Crowell.<sup>129</sup> Cazeneuve congratulated Microsoft for its cooperation in transmitting the content of the emails of the Hotmail account of one of the Paris attackers. This was addressed by Marc Mossé, director of Public Affairs in Europe:

“I remember the Charlie Hebdo attack, we were asked by the French government to provide some information. We have been able to provide the data in 45 minutes while the terrorists were still active, and it has been done according to the US law in case of emergency when people could be killed or there is a risk for the life of people you can give access to data in certain circumstances we have be able to provide this data in 45 minutes so there is an efficient way to collaborate and at the same time to respect the due process of law” (Appendix 1).

A similar process unfolded ten months later:

“When the Bataclan attack started (...) I turned on the TV and I looked at the events and I called my colleagues, well, in fact at the highest level of the company and I said “something is happening in Paris, I don’t know what, it could be extremely serious and we have to be ready to answer the questions that could come from the law enforcement department” (...). We have been able to provide information in no more than 90 minutes during this attack. So there is way to collaborate in respect of the law and it’s important to remind it because, again, I do not see any opposition between public safety and privacy, and it’s not new because of technology.”

This form of cooperation that conformed with the US law that these companies must comply with was therefore already undergoing. But through this new dialogue fostered by the US executives and the French minister, it would break new grounds.

The content of the talk held in Silicon Valley in February 2015 remained secret but another meeting was convened for April 2015 in Paris to “touch base of the commitments adopted, make [our] demands even more precise and come up with a code of good conduct.” In April, the meeting was held, along with the French association of Internet Access Providers. Google, Microsoft, Facebook

---

129. Cassini, S., & Rauline, N. (2015, February 23). Bernard Cazeneuve en Californie pour convaincre les géants du Net. Retrieved February 26, 2018, from [https://www.lesechos.fr/23/02/2015/LesEchos/21883-091-ECH\\_bernard-cazeneuve-en-californie-pour-convaincre-les-geants-du-net.htm](https://www.lesechos.fr/23/02/2015/LesEchos/21883-091-ECH_bernard-cazeneuve-en-californie-pour-convaincre-les-geants-du-net.htm)

Apple and Twitter announced that they would contribute to training law enforcement officers to help them understand the US legal framework for which they had to abide for surveillance requests made outside of “Mutual Legal Assistance Treaty” (MLAT) procedures. A “permanent point of contact between the Ministry and the providers” was also announced.<sup>130</sup> Headed by the “cyberprefect”, its aim was to allow for a sustained dialogue.

According to one of our interviewees – a French executive of one of these US companies who have attended the meetings this “group of contact” –, since mid-2015, the group has been convening roughly every trimester. On the issue of surveillance, one of its main tasks has been to update law enforcement officials about the launch or update of new products and services that might have consequences for their work, to training sessions regarding the applicable legal framework and corresponding procedures within the legal teams of the companies, to provide law enforcement with “model forms” based on US law to streamline surveillance requests that are compatible with US law and therefore do not require going through the complex and time-consuming MLAT procedures.

Despite the bellicose rhetoric of Cazeneuve, of other French politicians and law enforcement officials, this form of cooperation may have played a role in the sustained growth in the data handled to French administrative and judiciary law enforcement in the past years. In the first semester of 2013, Google was served with 2,011 requests by French authorities (it complied with 49 % of them); Facebook 1,547 requests a (39 % compliance rate). In the first semester of 2017, Google was served with 5,661 requests by French authorities (it complied with 63 % of them); Facebook 4,700 requests a 74% compliance rate). That makes for a 360% and 570% increase in the number of requests for which some data was produced, respectively.

**Fostering privatised censorship:** Like in the US, a key goal for French authorities was also to accelerate the takedown of terrorist-related content on the platforms of large online providers. During his trip in California February 2015, Cazeneuve praised these actors for their cooperation, insisting that “they now take content down more rapidly and efficiently than before.”<sup>131</sup> Their “reaction time” upon notice from public authorities was then said to be of the order of 15 minutes against months some time before.

The visit coincided with the adoption of an implementation decree that opened new avenues for the administrative takedown of online terrorist propaganda, by forcing cooperation of hosting and access providers with sanctions of up to one year imprisonment and a \$75 000 fine.<sup>132</sup> The second report of the member of the French Data Protection Authority tasked with the supervision of this administrative censorship, released in Spring 2017, points to the rapid development of this system, with a two-fold increase in the number of items taken-down by hosting providers (a category which includes social media and search engines) and a three-fold increase in the number of websites blocked by the French police.<sup>133</sup>

---

130. Cassini, S. (2015, April 23). *Terrorisme : accord entre la France et les géants du Net*. Retrieved April 23, 2015, from [http://www.lesechos.fr/journal20150423/lec2\\_high\\_tech\\_et\\_medias/02124922454-terrorisme-accord-entre-la-france-et-les-geants-du-net-1113723.php](http://www.lesechos.fr/journal20150423/lec2_high_tech_et_medias/02124922454-terrorisme-accord-entre-la-france-et-les-geants-du-net-1113723.php)

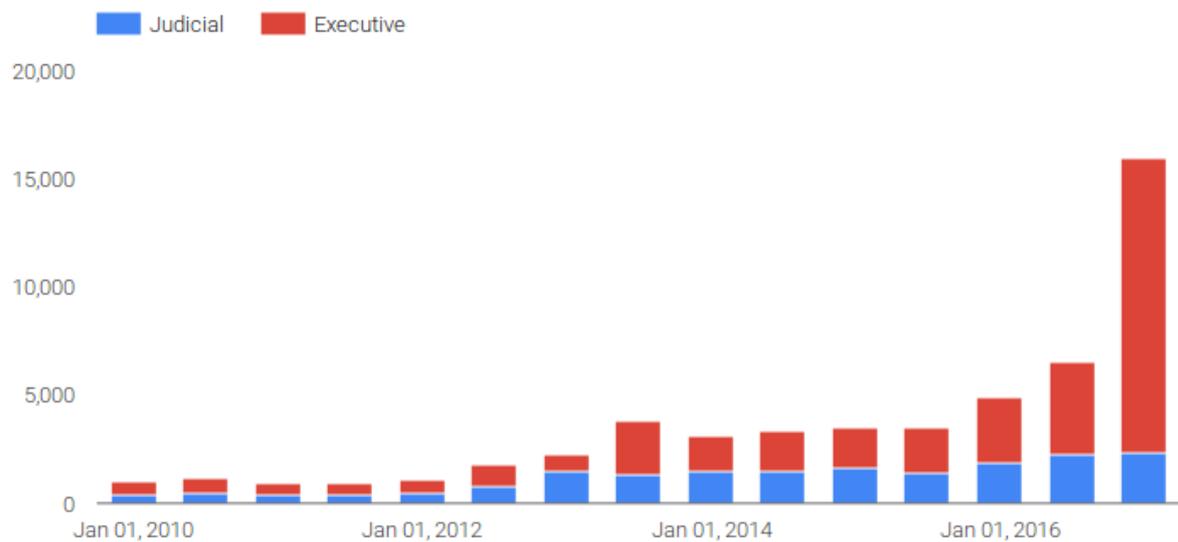
131. Idem.

132. Décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique. <https://www.legifrance.gouv.fr/eli/decret/2015/2/5/INTX1502813D/jo/texte>

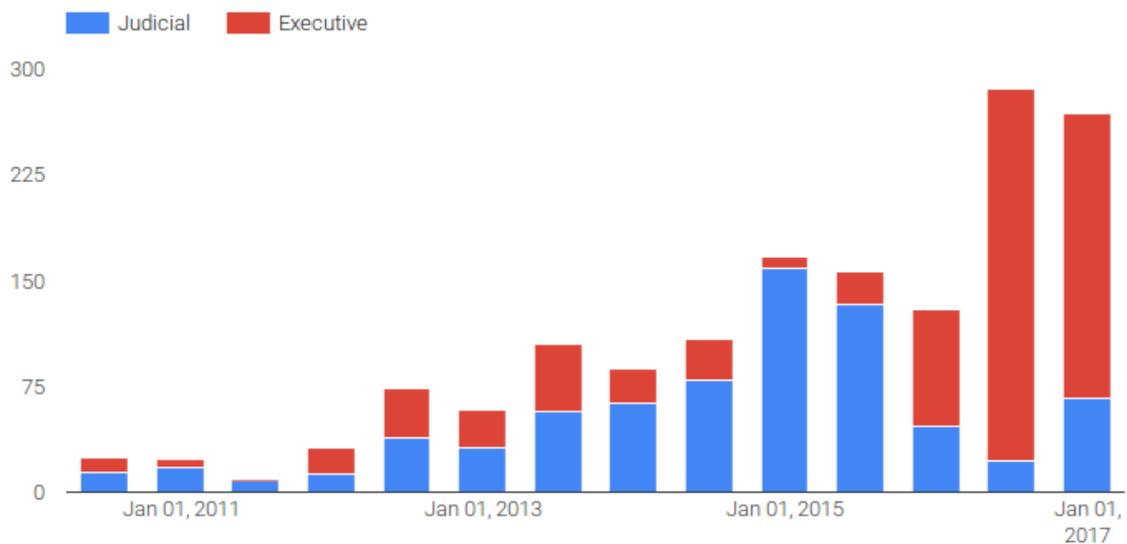
133. Linden, A. (2017). *Rapport d'activité 2016 de la personnalité qualifiée prévue par l'article 6-1 de la loi n° 2004-575 du 21 juin 2004 créé par la loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme (mars 2016-février 2017)*. Paris: CNIL. Retrieved from

But besides these legal avenues that are much criticized but still inscribed in a legislative framework, the forms of cooperation between the French Ministry of Interior and US tech companies regarding censorship can also be based on the private law of the firm's terms of service. This trend that is reflected in the transparency reports released by firms like Google, but the latter fails to make clear what is the legal basis for the takedown when it is mandated by the executive branch.





(a)



(b)

Figure: Number of takedown orders sent by public authorities either judicial (blue) or executive/administrative (red) at the global (a) and French ((b) levels (source : Google's Transparency Report).<sup>134</sup>

Since 2015, France and the UK have been the European leaders of this push toward privatized censorship, the institutions of the European Union have also been accompanying these trends.<sup>135</sup>

134. [https://transparencyreport.google.com/government-removals/by-country/FR?country\\_item\\_amount=group\\_by:branches;authority:FR&lu=country\\_request\\_amount&country\\_request\\_amount=group\\_by:branches;authority:FR](https://transparencyreport.google.com/government-removals/by-country/FR?country_item_amount=group_by:branches;authority:FR&lu=country_request_amount&country_request_amount=group_by:branches;authority:FR)

135. See, e.g.: Commission initiative with social media platforms and civil society shows progress. (2017, June 1). Retrieved June 2, 2017, from [http://europa.eu/rapid/press-release\\_IP-17-1471\\_en.htm](http://europa.eu/rapid/press-release_IP-17-1471_en.htm)

Fioretti, J. (2016, December 5). Web giants to cooperate on removal of extremist content. *Reuters*. Retrieved from <http://www.reuters.com/article/us-internet-extremism-database-idUSKBN13U2W8>

UK looking to increase pressure on internet firms over extremist material: minister. (2017, May 28). *Reuters*. Retrieved from <http://www.reuters.com/article/us-britain-security-manchester-technolog-idUSKBN18O0BT>

The European Commission and Europol have indeed convened regular meetings and pushed large online platforms to sign a code on hate speech in 2016.<sup>136</sup> In its report on the activity of its “Internet Referral Unit” created in 2015 to weed out extremist content online, Europol makes clear that these censorship activities are conducted outside of any legislative framework:

“A referral activity (meaning the reporting of terrorist and extremist online content to the concerned online service provider) does not constitute an enforceable act. Thus, the decision and removal of the referred terrorist and extremist online content is taken by the concerned service provider under their own responsibility and accountability (in reference to their Terms and Conditions).”<sup>137</sup>

The oversight of these activities is plagued with important shortcomings from a human rights perspective,<sup>138</sup> but they are gaining increasing importance as the French and British approaches to cooperation seems to be replicated at the EU level.<sup>139</sup> This process is still ongoing. In November 2017, the French government tasked its “Digital Ambassador,” David Martinon, with negotiating with US companies for the takedown of illegal content.<sup>140</sup> More recently, the French Prime Minister Edouard Philippe announced that platforms should aim at taking litigious content down within one hour open publication,<sup>141</sup> and in 2017, Germany adopted the “NetzDG law” which gives platforms a 24-hour deadline to take down hateful speech upon notice when it is deemed “obviously illegal.”<sup>142</sup>

These moves, which are sometimes but not always backed by the force of law like in the German

---

136. Hern, A. (2016, May 31). Facebook, YouTube, Twitter and Microsoft sign EU hate speech code. Retrieved June 8, 2016, from <http://www.theguardian.com/technology/2016/may/31/facebook-youtube-twitter-microsoft-eu-hate-speech-code>

Monroy, M. (2016, June 29). New Europol regulation due to enter into force from May 2017 – oversight is likely to remain superficial. Retrieved July 15, 2016, from <https://digit.site36.net/2016/06/29/new-europol-regulation-due-to-enter-into-force-from-may-2017-oversight-is-likely-to-remain-superficial/>

137. Europol. (2016). *EU Internet Referral Unit - YEAR ONE REPORT* (p. 11). Retrieved from <https://www.europol.europa.eu/content/eu-internet-referral-unit-year-one-report-highlights>

138. Baker, J. (2016, July 4). Europol’s online censorship unit is haphazard and unaccountable says NGO. Retrieved July 4, 2016, from <http://arstechnica.com/tech-policy/2016/07/europol-iru-extremist-content-censorship-policing/>

Monroy, M. (2016, June 29). New Europol regulation due to enter into force from May 2017 – oversight is likely to remain superficial. Retrieved July 15, 2016, from <https://digit.site36.net/2016/06/29/new-europol-regulation-due-to-enter-into-force-from-may-2017-oversight-is-likely-to-remain-superficial/>

139. Computer support to analyze IS propaganda. (2017, April). Retrieved March 8, 2018, from <https://www.europol.europa.eu/publications-documents/computer-support-to-analyze-propaganda>

Disruptive efforts by industry and law enforcement force jihadist sympathisers to seek new platforms to disseminate terrorist propaganda. (2017, September 15). Retrieved March 8, 2018, from

<https://www.europol.europa.eu/newsroom/news/disruptive-efforts-industry-and-law-enforcement-force-jihadist-sympathisers-to-seek-new-platforms-to-disseminate-terrorist>

EU law enforcement joins together with Facebook against online terrorist propaganda. (2018, January 18). Retrieved March 8, 2018, from <https://www.europol.europa.eu/newsroom/news/eu-law-enforcement-joins-together-facebook-against-online-terrorist-propaganda>

Europol coordinates EU-wide hit against online terrorist propaganda. (2017, May 7). Retrieved March 8, 2018, from <https://www.europol.europa.eu/newsroom/news/europol-coordinates-eu-wide-hit-against-online-terrorist-propaganda>

Europol coordinates fifth joint operation to flag online terrorist content. (n.d.). Retrieved March 8, 2018, from <https://www.europol.europa.eu/newsroom/news/europol-coordinates-fifth-joint-operation-to-flag-online-terrorist-content>

140. Eschapasse, B. (2018, April 2). David Martinon : « Le monde est en état de cyberguerre froide permanente ». Retrieved April 10, 2018, from [http://www.lepoint.fr/high-tech-internet/david-martinon-le-monde-est-en-etat-de-cyberguerre-froide-permanente-02-04-2018-2207326\\_47.php](http://www.lepoint.fr/high-tech-internet/david-martinon-le-monde-est-en-etat-de-cyberguerre-froide-permanente-02-04-2018-2207326_47.php)

141. La France prête à pousser l’UE à légiférer sur les contenus terroristes. (2018, February 26). Retrieved February 26, 2018, from <http://www.contexte.com/numerique/briefing/2018/02/26/#briefitem-83434>

142. Aleksandra, K. (2017, November 30). Phantom Safeguards? Analysis of the German law on hate speech NetzDG. Retrieved from <https://www.law.kuleuven.be/citip/blog/phantom-safeguards-analysis-of-the-german-law-on-hate-speech-netzdg/>

case – but most often with the mere threat of new legislation –, represent an important challenge considering the sheer volume of third-party content posted on these platforms: 300 hours of video are posted on YouTube every minute;<sup>143</sup> on Facebook, 510,000 comments are posted, 293,000 statuses are updated, and 136,000 photos are uploaded every day.<sup>144</sup>

On the part of the platforms, these efforts have led to significant investment in tools based on “Machine Learning” systems aimed at spotting terrorist-related content in order to make them inaccessible. In September 2017, taking some time away from the UN General Assembly in New York, Emmanuel Macron, Theresa May and Paolo Gentiloni, then Prime Minister of Italy, convened a meeting with the tech industry to renew their demands (with a new takedown reaction time of 2 hours upon notice). According to Theresa May:

“Industry needs to go further and faster in automating the detection and removal of terrorist content online, and developing technological solutions which prevent it being uploaded in the first place. We need a fundamental shift in the scale and nature of our response – both from industry and governments – if we are to match the evolving nature of terrorists’ use of the internet.”<sup>145</sup>

An unidentified British official also explained to the Guardian the state of mind behind these calls:

“These companies have some of the best brains in the world. They should really be focusing that on what matters, which is stopping the spread of terrorism and violence. We want them to break the echo chambers.”

Monica Bickert, Vice President of Consumer Operations at Facebook, says

she often gets asked “when is AI going to save us all?” But, she says, “we’re a long way from that.” To make a determination of whether a given content abides by the terms of service of these platforms, a human intervention remains essential to look at context of a given post or a community. According to Bickert:

“There are some areas where technical tools are helping us do this job. But the vast majority, when we’re looking at hate speech or we’re looking at bullying or we’re looking at harassment, there is a person looking at it and trying to determine what’s happening in that offline world and how that manifests itself online.”<sup>146</sup>

Accordingly, we are seeing a significant increase in the number of staff mobilized on content moderation. In 2017, Facebook moderation team grew from 3000 to 7500 people in only eight months,<sup>147</sup> while Google’s YouTube announced even more ambitious plans.<sup>148</sup> According to YouTube CEO Susan Wojcick, “[Google] will continue the growth of our teams, with the goal of bringing the total number of people across Google working to address content that might violate our

143. <https://fortunelords.com/youtube-statistics/>

144. <https://zephoria.com/top-15-valuable-facebook-statistics/>

145. Hope, C., & McCann, K. (2017, September 19). Google, Facebook and Twitter told to take down terror content within two hours or face fines. *The Telegraph*. Retrieved from <https://www.telegraph.co.uk/news/2017/09/19/google-facebook-twitter-told-take-terror-content-within-two/>

146. Madrigal, A. C. (2018, February 7). Inside Facebook’s Fast-Growing Content-Moderation Effort. *The Atlantic*. Retrieved from <https://www.theatlantic.com/technology/archive/2018/02/what-facebook-told-insiders-about-how-it-moderates-posts/552632/>

147. Idem.

148. Beavers, O. (2017, December 4). Google to appoint staff of 10,000 to weed out extremist content on YouTube [Text]. Retrieved December 5, 2017, from <http://thehill.com/policy/technology/363242-10000-google-staff-set-to-weed-out-extremist-content-on-youtube>

policies to over 10,000 in 2018.” Most of these content-moderators are in fact hired by subcontractors in low-wages countries and face serious issues regarding social rights (Roberts, 2016).

Rather than putting public money in the justice system to allow it to catch up with the surge in speech, states are pressuring private companies who have developed large technical infrastructures and amassed enormous financial power to do it. Counting on the ability of these firms to develop technical solutions to the political and legal problems tied to online speech, they place hopes in the development of “Artificial Intelligence.” So far, this has not delivered expected results, and this means that huge numbers of low-wage workers need to be recruited to populate what are, in effect, privatized censorship bureaucracies.

During a conference in February 2018, Neil Potts, a public policy manager at Facebook, emphasized the similarity between the censorship role played Facebook and that of governments:

“We do really share the goals of government in certain ways,” he said. “If the goals of government are to protect their constituents, which are our users and community, I think we do share that. I feel comfortable going to the press with that.”<sup>149</sup>

But this growing alignment between large online platforms and states, as we have seen, often escapes appropriate legal frameworks. To some extent, this gives more leeway both to the states and to companies with regards to these censorship activities. A key issue for the US companies is to protect their status as “neutral” hosting providers which give them a liability exemption, and which many policy-makers are willing to undermine to increase pressure on these platforms.<sup>150</sup>

**Economic cooperation and provider-customer relationships:** A last instance of cooperation between US tech companies and the French state is their business relationship. Many US companies, from CISCO to Microsoft, are important bidders of public tenders issued by public administration in the field of public and cyber security.

Despite the efforts of many players to ensure “digital sovereignty” by favouring French and European competitors, the alleged superiority of US companies’ products and services give them a significant appeal. The contract between Microsoft and the French Ministry of Defense have for instance come under harsh criticism on the basis of “digital sovereignty.”<sup>151</sup> In 2016, US company Palantir has also teamed up with the French Internal Security Intelligence Agency (DGSI by its French acronym) through a €10 million contract, when the agency failed to cope with the vast amount of data seized during the house raids and digital seizures conducted under the state of emergency, which was in force in France between November 2015 and October 2017.<sup>152</sup> Other

---

149. Madrigal, A. C. (2018, February 7). Inside Facebook’s Fast-Growing Content-Moderation Effort. *The Atlantic*. Retrieved from <https://www.theatlantic.com/technology/archive/2018/02/what-facebook-told-insiders-about-how-it-moderates-posts/552632/>

150. For an overview of recent debates on intermediary liability in the EU, see e.g.: Greenfield, H. (2018, March 1). New EU Recommendation on Illegal Content Online Undermines Online Rights and Harms Europe’s Tech Economy. Retrieved March 9, 2018, from <https://www.cccanet.org/2018/03/new-eu-recommendation-on-illegal-content-online-undermines-online-rights-and-harms-europes-tech-economy/>

151. Open Bar Contract between Microsoft and the French Ministry of Defense: April Calls on Senators to Support a Motion for the Creation of an Investigation Committee. (2017, October 18). Retrieved March 9, 2018, from <https://www.april.org/en/open-bar-contract-between-microsoft-and-french-ministry-defense-april-calls-senators-support-motion>

152. Tesquet, O. (2017, January 27). Palantir, l’encombrant ami américain du renseignement français. Retrieved January 27, 2017, from <http://www.telerama.fr/medias/palantir-big-data-renseignement,153229.php>

prominent figures of the French intelligence community have voiced their scepticism towards this partnership. But it also speaks to the superiority of US tech companies and the seemingly irresistible appeal for their services and products even for the French national security field.

US tech companies are also international investors that help maintain the competitiveness of the French digital economy, or can even be a substitute to public policies. In 2015, Cisco and the French government signed \$200 million partnerships. According to Cisco, the company is:

“committed to accelerating the digital transformation of France through a series of investments totaling more than \$100 million. This involved training individuals for the new digital economy, investing in innovative start-ups, developing national network infrastructure, researching smart cities, and broadening cyber security expertise.”<sup>153</sup>

In part, these investments lead to joint-ventures with large firms or startups in the French digital economy. For instance, in October 2015, the management of CISCO and Thales announced a common “sovereign” co-innovation proposal to protect critical infrastructures against cyber-threats. IBM has also recently partnered with Engie, a French multinational electric utility company, to help it develop Big Data solutions.<sup>154</sup> More recently, in the field of Artificial Intelligence, Facebook and Google have announced major investment in their French R&D centres.<sup>155</sup> US tech companies like Cisco, Microsoft or Google are also increasingly investing in training programs in French universities and schools.<sup>156</sup>

**Revolving doors between EU administrations and these “essential partner”:** These various forms of cooperation show the strong interdependencies that unite US tech companies and the French state, and help explain the softer tone of the 2017 SGDSN strategic review compared with the one adopted two years before. According to the document, the digital ecosystem leads to “the rise of new private actors, who impose themselves on the international scene as a challenge to the sovereignty of states but also as sometimes essential partners.”<sup>157</sup> They also need to be understood in the wider context of the “revolving door” between French and EU administrations and US tech

---

According to the former Director of the DGSI, Patrick Calvar, «*les entreprises françaises qui développent des systèmes ne sont pas encore capables de répondre à nos besoins, alors que nous devons acquérir ce big data immédiatement. Nos camarades européens sont dans la même situation. Le choix n’a pas encore été fait mais, en tout état de cause, la solution sera temporaire. Tout ce que nous développons se fait en relation directe avec la DGSE, afin d’éviter les doublons, et la plupart de nos ingénieurs en charge de ces questions viennent de la DGSE. La moindre perquisition nous permet de récupérer des milliers de données. Nous avons donc besoin d’outils de big data pour répondre immédiatement à nos besoins.*” Audition de M. Patrick Calvar, directeur général de la sécurité intérieure par la commission de la défense nationale et des forces armées. (2016, May 10). Retrieved March 9, 2018, from <http://www.assemblee-nationale.fr/14/cr-cdef/15-16/c1516047.asp>

153. Chambers, J. (2015, February 24). How France is Embracing Digitization of Everything. Retrieved March 9, 2018, from <https://blogs.cisco.com/news/how-france-is-embracing-digitization-of-everything>  
Cisco drives the digital acceleration of France through innovative investment, partnership and programs. (2015, October 8). Retrieved March 9, 2018, from <https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1721329>

154. Filippone, D. (2016, July 26). Avec IBM, Engie monte d’un cran dans les smartcities. Retrieved December 21, 2017, from <https://www.lemondeinformatique.fr/actualites/lire-avec-ibm-engie-monte-d-un-cran-dans-les-smartcities-65501.html>

155. Google, Facebook Target Paris as a Center for AI Expansion. (2018, January 22). *Bloomberg.Com*. Retrieved from <https://www.bloomberg.com/news/articles/2018-01-22/google-facebook-target-paris-as-a-center-for-ai-expansion>

156. See, e.g.: Hérard, P. (2018, February 25). Google et Facebook formateurs au “digital” de chômeurs et d’étudiants : que fait l’Etat ? Retrieved February 25, 2018, from <http://information.tv5monde.com/info/google-et-facebook-formateurs-au-digital-de-chomeurs-et-d-etudiants-que-fait-l-etat-222637>

157. Secrétariat général de la défense et de la sécurité nationale. (2018). *Revue stratégique de cyberdéfense*. Paris. Retrieved from <http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/>

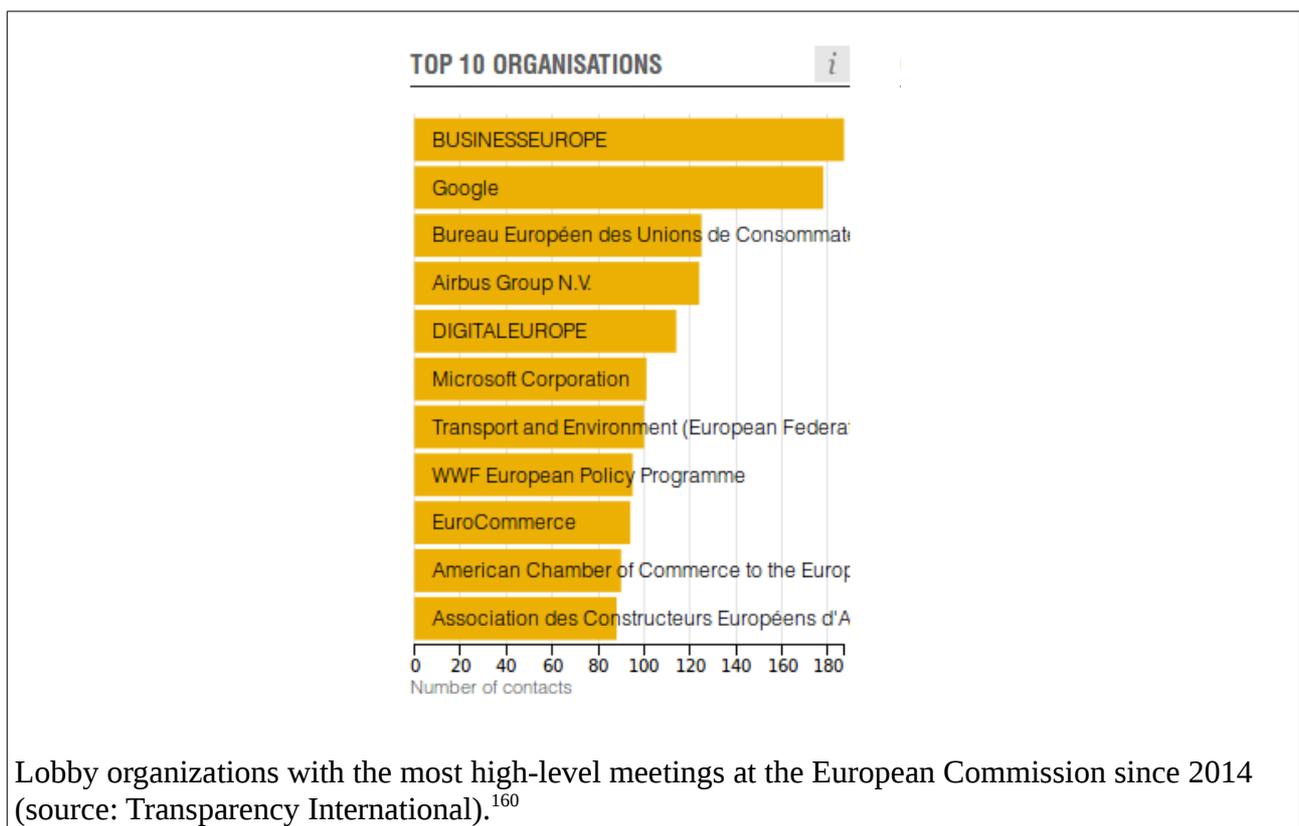
companies. In 2016, the Google Transparency project has for instance documented:

“at least 80 revolving door moves between Google and European governments over the past decade as the company seeks to boost its influence in the region and head-off antitrust action and privacy regulation.

Google, now part of Alphabet Inc., has hired at least 65 government officials from all over the European Union since 2005. Those included Tomas Gulbinas, a former ambassador-at-large for the Lithuanian government, and Georgios Mavros, an advisor to a French member of the European Parliament, to name two recent examples. Google hired both officials as lobbyists in 2015.

During the same period, 15 Googlers have been appointed to government positions in Europe, gaining valuable contacts at the heart of the decision-making process. Those included Baroness Joanna Shields, a former managing director for Google, who was appointed the UK’s Minister for Internet Safety and Security at the Department for Culture, Media and Sport; and Google’s executive chairman, Eric Schmidt, appointed by British Prime Minister David Cameron to his business advisory council.”<sup>158</sup>

Google and Microsoft for instance declare spending between €4,25 million et €4,5 million annually to lobby EU institutions, and this translates in frequent meetings with EU commissioners.<sup>159</sup>



French data journalist Alexandre Léchenet has also stressed the importance of the phenomenon at the French level, with at least 23 hires from the public sector for major US tech companies in

158. Google’s European Revolving Door. (2017). Retrieved February 13, 2018, from <https://googletransparencyproject.org/articles/googles-revolving-door-us>

159. <https://github.com/alphoenix/donnees/blob/master/lobbies-gafamut/lobbies.csv>

160. <http://www.integritywatch.eu/>

France and many high-level meetings.<sup>161</sup>

---

161. Léchenet, A. (2017). *L'influence tentaculaire des géants américains*. Retrieved from <https://github.com/alphoenix/donnees> (Original work published December 2016).

## 4. Conclusion: Changing Bureaucracies, Security & the Rule of Law

In concluding this deliverable, we would like to go back to our main research questions and gather key takeaways from our case studies.

First, regarding the strategies of major Internet firms in navigating debates on state surveillance, despite a lack of extensive data on this issue, our research suggests that these strategies are handled and decided upon at very senior levels within the companies – in some extreme cases, Chief Information Security officers might not even been aware of the companies decision to comply with a given and contentious surveillance order. Besides the management of sensitive information, this can also be seen as a way to shield the governance of national security issues from internal dissent within these companies.

With regards to the factors determining the behaviors of these firms in the resistance-cooperation dilemma, our hypothesis seem to be validated by our case-studies. We initially found important differences depending on the considered country: in the US, overt resistance was staged in a prime instance of double-dealing, whereas in France such double-dealing was immediately called out by government officials leading to much less intense and much more discreet forms of resistance. But overtime, from 2015 on, the influence of the human rights field withered along the media attention to state surveillance issues. The agenda became dominated by the terrorist threat and similar trends towards greater cooperation materialized on both sides of the Atlantic – especially regarding the issue of the monitoring and takedown of terrorism-related content on online platforms –, suggesting strong transnational field effects not only from technology multinationals but also from security professionals (Bigo, 2016).

As a consequence, while we sometimes observed important variations in the processes depending on the countries under consideration – variations that can be explained by the greater proximity of US firms with the US government and the existence of existing public-private alliances in Europe where these firms economic and cultural capitals do not hold the same value in the administrative or security fields where they face strong private competitors –, these processes eventually aggregate in coherent mechanisms and produce similar outcomes overtime.

### **Data governance as a new bureaucratic paradigm**

As our case-studies show, these shifts in public-private assemblages for communications surveillance purposes need to be inscribed in a broader context of changes in modern bureaucracies.

In her work on neo-liberal bureaucratization, Béatrice Hibou have shown how, from the 1970s on, the logic of management migrated from the private realm to state institutions, and how the spread of these private rules and procedures meshed, contributing to the blurring of traditional public-private distinctions (Hibou, 2012). But through the imperatives of “efficiency”, of “cost-effectiveness”, of “flexibility” and practices of “auditing”, of “benchmarking”, bureaucratic practices within public administrations were increasingly perceived as alien to the values of the public sector and to its relationship to the social world. The abstract principles of neo-liberal democracies and the old

precept of abstract and general rules was pushed so far as to give way to a “manufactured unicity” of the social world, leading to aggravated forms of depoliticization.

As Zuboff (2015) and others as well as our own research on the security field suggest, the large technology firms on which we have focused in this report have nurtured a new bureaucratic paradigm based on “data governance.” In 2014, Eric Schmidt and Jonathan Rosenberg, a former Senior Vice President of Products at Google, co-wrote *How Google Works*.<sup>162</sup> Adding to the doctrine already forged by Google’s Chief Economist Hal Varian regarding “data extraction and analysis”, “new contractual forms due to better monitoring”, “personalization and customization”, and “continuous experiments,”<sup>163</sup> the authors documented the business management lessons from Google, an experience that led them to “relearn everything” they knew by exploring data-intensive models, expanding the “new spirit of capitalism” with a horizontally-driven and creative workforce. Some years before, some self-proclaimed Internet theorists like Jeff Jarvis had also called on emulating Google across society.<sup>164</sup>

It these models that Schmidt is today helping spread at the Pentagon through the Defense Innovation Board. In France too, the debate on the “reform of the state” has moved from the premisses of the New Public Management described by Hibou to data governance. By referring to concepts like the “Startup Nation” or the “platform State”,<sup>165</sup> today’s reformers are re-modelling bureaucracies and decision-making processes around the need to produce data, make it available and usable, maintain its integrity and feed it to powerful data-processing tools that will be used to optimize bureaucratic outputs. Even when these discourses claim to be opposing the hegemony of US tech companies, they are in fact assuming the superiority of this model and diffusing them across public administrations. It is an instance of “mimetic rivalry” (Girard, 2002), where what Evgeny Morozov has termed *solutionism* serves as a new technocratic utopia (Morozov, 2013).

### **Public-private security assemblages in the age of data governance**

Similar trends towards technical, managerial and technological responses to security challenges have of long been sweeping the security field (Abrahamsen & Williams, 2010; Bonelli, 2010). But today, public-private hybridization – especially when it comes to monitoring and controlling information flows – are also increasingly focused on data governance.

Faced with the challenge of adapting surveillance and censorship practices to the challenging digital environment – which was supposed to undermine state sovereignty and law enforcement –, national security professionals have increasingly resorted to alliances with private actors who master new forms of management, have the technical know-how and operate communication infrastructures. In today’s digital economy, that means not only dealing with large, “home-grown” firms (sometimes former state monopolies) whose relations to the state are long-established, with long-running forms of cross-socialization between public and private security professionals, but also with newcomers to the field like tech firms who came to dominate the digital economy in recent years.

---

162. Schmidt, E., & Rosenberg, J. (2015). *How Google Works*. London: John Murray.

163. Varian, H.R. (2010). Computer Mediated Transactions, *American Economic Review* 100(2): 1–10. Varian, H.R. (2014). Beyond Big Data, *Business Economics* 49(1): 27–31.

164. Jarvis, J. (2011). *What Would Google Do?: Reverse-Engineering the Fastest Growing Company in the History of the World* (Reprint). New York; Enfield: HarperBusiness.

165. In France, see e.g.: Algan, Y., & Cazenave, T. (2016). *L’Etat en mode start-up*. Paris: Eyrolles. Bertholet, C., & Létourneau, L. (2017). *Ubérisons l’État ! Avant que d’autres ne s’en chargent*. Malakoff: Armand Colin. Pezziardi, P., & Verdier, H. (2017). *Des startups d’État à l’État plateforme*. CreateSpace Independent Publishing Platform.

The large tech firms on which this deliverable has focused are – because of the structure of their technical, economic and organizational capitals – a prime locus to observe these trends. We have seen that, despite the fact that conflicts are being staged, and under the conditions where their capital is gaining the upper hand across the administrative field, new cross-socialization spaces are being created, alliances are being formed between these actors and public security professionals. In periphery of these new cooperation avenues, conflict remain. Such is the case for instance when state officials use securitization discourses, the threat of legal sanctions or denounced the double-dealing of tech companies to “force” cooperation in security matters, or when the personnels of these companies stage their resistance to the security policies and demands of the state. But as we have seen, they can in part be attributed to the actors’ strategies, determined by various constraint structures, as they progress towards greater cooperation in a field that is by its very nature a competitive space, reaped with power relations and struggles.

Although these emerging public-private security assemblages tasked with managing information flows are particularly visible when they embark large tech companies used daily by billions of Internet users, these large online service providers are hardly the only private actors involved in such assemblages. Old tech and utility companies in the transportation or energy sectors are also increasingly investing in Big Data analytics (partly as a result of cybersecurity public policies), sometimes in partnership with their US competitors, and getting closer to the security field. Many small companies specialized in data analytics or vulnerabilities are also partnering with intelligence agencies to sell their products and services (Deibert, 2013).<sup>166</sup>

For these two later types of companies, who can also count on a kind of technical-organizational capital currently sweeping the administrative field, resorting to “revolving door” hires with people coming from intelligence agency is usually easier.<sup>167</sup> For the most part, they also have the luxury of not being engulfed in the sort of public scandal that large consumer-facing companies like Google, Apple, Facebook and the like had to deal with during the Snowden disclosures, thus decreasing the likelihood of resistance. Even when they are, like for instance Orange and Qosmos in France, their internal corporate culture and their already completed inclusion in public-private security assemblages mean that they are more likely to just keep a low-profile rather than stage resistance, while relying on the support of “deep state” officials. Finally, because of their business operation and the nature of their products, these companies will typically not face the sort of regulatory stakes – and in particular conflicts of law and judicial cooperation mechanisms – which, as we have seen,

---

166. See e.g.: CIA hackers’ favourite suppliers. (2017, March 22). Retrieved March 13, 2018, from <https://www.intelligenceonline.com/grey-areas/2017/03/22/cia-hackers--favourite-suppliers.108226984-art>  
Paris wises up to darknet data leaks. (2018, February 14). Retrieved March 13, 2018, from <https://www.intelligenceonline.com/surveillance--interception/2018/02/14/paris-wises-up-to-darknet-data-leaks.108294132-art>

NSA, GCHQ look to private sector for cyber-offensive firepower. (2017, June 21). Retrieved March 14, 2018, from <https://www.intelligenceonline.com/government-intelligence/2017/06/21/nsa-gchq-look-to-private-sector-for-cyber-offensive-firepower.108250738-eve>

167. See, e.g.: FedData recruits at NSA, its special customer. (2017, May 24). Retrieved March 14, 2018, from <https://www.intelligenceonline.com/corporate-intelligence/2017/05/24/feddata-recruits-at-nsa-its-special-customer.108235644-bre>

Former spy chief turns to new cyber-security role in the private sector. (2017, October 26). Retrieved March 14, 2018, from <https://www.thesun.co.uk/news/4768235/spy-boss-robert-hannigan-who-quit-due-to-ill-health-lines-up-lucrative-private-deals/>

Guibert, N. (2014, January 14). L’ex-M. Grandes Oreilles de la DGSE part dans le privé. *Le Monde.fr*. Retrieved from [http://www.lemonde.fr/economie/article/2014/01/14/l-ex-monsieur-grandes-oreilles-de-la-dgse-part-dans-le-privé\\_4347510\\_3234.html](http://www.lemonde.fr/economie/article/2014/01/14/l-ex-monsieur-grandes-oreilles-de-la-dgse-part-dans-le-privé_4347510_3234.html)

further complicate the dealings of US platforms with the state officials of the countries in which they operate.

### **Overcoming the digital challenge at the price of the rule of law?**

In concluding this deliverable, we would like to tie our findings to some of the hard-pressing questions regarding the rule of law and human rights in the digital age: What are the political consequences of the emergence of data governance as a new bureaucratic paradigm and the corresponding reassembly of public-private assemblages in the security field?

The alliance of traditional state power with the reach and depth of the digital infrastructure mastered by a handful of companies has turned mass surveillance into a practical reality. In the arms-race to amass and process data, these new “Big-Data security assemblages” are now implementing automatic, preventive, preemptive and/or predictive policing approaches. There are reasons – and growing evidence – to doubt that the new “regimes of truth” established by modern surveillance will in any meaningful way provide long-term solutions to security issues (e.g. Aradau & Blanke, 2015; Ferguson, 2017). Like New Public Management, technological solutionism in the age of data governance, bolstered by marketing discourses coming from the private sector, might only be recreating a veil of illusion of technocratic control, while putting evermore distance between bureaucracies and the social world they wish to make more orderly.

In the process, these socio-technical assemblages charged with the surveillance and censorship also take our political systems further away from the rule of law. Legal norms and principles, once programmed into computer code governing algorithms, become diluted, invisible and therefore hard to challenge (Rouvroy, 2012). Indeed, when Google or Facebook develop algorithms aimed at ensuring the speedy removal of allegedly-terrorist content, who is able and allowed to make sure that this piece of code works as intended, safeguard protected speech, etc.?

In the course of the ongoing negotiations regarding online censorship between private companies and government officials, the latter seems all too content to re-establish effective mechanisms to control the vast amount of public expressions flowing on the Internet while doing away with the need to invest resources in their police and justice system to do so, let alone to escape some of the “old safeguards” that our legal systems have developed overtime to protect freedom of expression but which make them ill-suited to process the surge in communications entailed by digital technologies (Tréguer, 2017b). In this regard, these new public-private assemblages governing data flows are an illustration of what some have called a “hybrid rule,” that is “a set of practices deployed by political elites that rely on the private sector to shield national security activities by expanding state power while constraining democratic accountability” (Hurt & Lipschutz, 2015). The line between the public and the private might be increasingly diluted, but the resulting arrangements have strong structural effects that need to be inscribed in the genealogy of modern state power.

## References

- Abrahamsen, R., & Leander, A. (2015). *Routledge Handbook of Private Security Studies*. Routledge.
- Abrahamsen, R., & Williams, M. C. (2010). *Security Beyond the State: Private Security in International Politics*. Cambridge University Press.
- Aradau, C., & Blanke, T. (2015). The (Big) Data-security assemblage: Knowledge and critique. *Big Data & Society*, 2(2), 2053951715609066. <https://doi.org/10.1177/2053951715609066>
- Assange, J. (2014). *When Google Met Wikileaks* (1ST edition). O.
- Ball, K., & Snider, L. (2014). *The Surveillance-Industrial Complex: A Political Economy of Surveillance*. Taylor and Francis. Retrieved from <http://www.scopus.com/inward/record.url?eid=2-s2.0-84906009380&partnerID=40&md5=aa053badcfba61421cd51546a352e42c>
- Barbrook, R., & Cameron, A. (1995). The Californian ideology. *Mute*, 1(1), 44–72. <https://doi.org/10.1080/09505439609526455>
- Barlow, J. P. (1996, February 9). A Cyberspace Independence Declaration. Retrieved from [https://w2.eff.org/Censorship/Internet\\_censorship\\_bills/barlow\\_0296.declaration](https://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration)
- Barty-King, H. (1980). *Girdle Round the Earth: History of Cable and Wireless*. London: William Heinemann.
- Bauer, M., Lee-Makiyama, H., van der Marel, E., & Verschelde, B. (2014). *The Costs of Data Localisation: Friendly Fire on Economic Recovery* (ECIPE Occasional Paper No. 12). Brussels: European Centre for International Political Economy. Retrieved from [http://www.ecipe.org/app/uploads/2014/12/OCC32014\\_\\_1.pdf](http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf)
- Bigo, D. (2016). Sociology of Transnational Guilds. *International Political Sociology*, 10(4), 398–416.
- Bigo, D., Jeandesboz, J., Martin-Mazé, M., & Ragazzi, F. (2014). *National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law* (Study for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs No. PE 509.979). Brussels: European Parliament. Retrieved from [http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/509979/IPOL-LIBE\\_ET\(2014\)509979\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/509979/IPOL-LIBE_ET(2014)509979_EN.pdf)
- Black, E. (2012). *IBM and the Holocaust: The Strategic Alliance Between Nazi Germany and America's Most Powerful Corporation* (Expanded Edition edition). Washington, DC: Dialog Press.
- Boltanski, L., & Chiapello, È. (1999). *Le nouvel esprit du capitalisme* (Essais). Paris: Gallimard.

- Bonelli, L. (2010). Les modernisations contradictoires de la police nationale. In *L'État démantelé* (pp. 102–117). La Découverte. Retrieved from <https://www.cairn.info/l-etat-demantele--9782707160195-p-102.htm>
- Bourdieu, P. (2014a). *On the State* (1 edition). Cambridge Malden, MA: Polity Press.
- Bourdieu, P. (2014b). Séminaires sur le concept de champ, 1972-1975. *Actes de la recherche en sciences sociales*, (200), 4–37.
- Brito, J., & Watkins, T. (2011). *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy* (Working Paper). Mercatus Center, George Mason University. Retrieved from <http://mercatus.org/publication/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy>
- Brust, R. (2012). Letters of the Law: National Security Letters Help the FBI Stamp out Terrorism but Some Disapprove. *ABA Journal*, 98, 56.
- Casilli, A. A. (2017). Digital Labor Studies Go Global: Toward a Digital Decolonial Turn. *International Journal of Communication*, 11(0), 21.
- Chander, A., & Lê, U. P. (2015). Data Nationalism. *Emory Law Review*, 64(677), 678–739.
- Charbon, P. (1991). Genèse du vote de la loi de 1837, origine du monopole des télécommunications. In C. Bertho-Lavenir (Ed.), *L'État et les télécommunications en France et à l'étranger, 1837-1987* (pp. 11–22). Genève: Librairie Droz.
- Christakis, T. (2017). *Data, Extraterritoriality and International Solutions to Transatlantic Problems of Access to Digital Evidence. Legal Opinion on the Microsoft Ireland Case (Supreme Court of the United States)* (SSRN Scholarly Paper No. ID 3086820). Rochester, NY: Social Science Research Network. Retrieved from <https://papers.ssrn.com/abstract=3086820>
- Coleman, G. (2011). Hacker Politics and Publics. *Public Culture*, 23(3 65), 511–516. <https://doi.org/10.1215/08992363-1336390>
- Deibert, R. J. (2013). *Black Code: Inside the Battle for Cyberspace*. Random House LLC.
- Doyle, C. (2015). *National Security Letters in Foreign Intelligence Investigations: Legal Background*. Washington, D.C: Congressional Research Service. Retrieved from <https://fas.org/sgp/crs/intel/RL33320.pdf>
- Easton, D. (1957). An Approach to the Analysis of Political Systems. *World Politics*, 9(3), 283–400.
- Ferguson, A. G. (2017). *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: New York University Press.
- Flichy, P. (1991). *Une histoire de la communication moderne : espace public et vie privée*. La Découverte.

- Foster, J. B., & McChesney, R. W. (2014). Surveillance Capitalism: Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age. *Monthly Review*, 66(3). Retrieved from <http://monthlyreview.org/2014/07/01/surveillance-capitalism>
- Fuchs, C. (2013). Political Economy and Surveillance Theory. *Critical Sociology*, 39(5), 671–687. <https://doi.org/10.1177/0896920511435710>
- Fuchs, C., & Trottier, D. (2015). Towards a theoretical model of social media surveillance in contemporary society. *Communications-European Journal of Communication Research*, 40(1), 113–135. <https://doi.org/10.1515/commun-2014-0029>
- Gasparin, A. de. (1837). Exposé des motifs et projet de loi sur les lignes télégraphiques présentés par M. le ministre de l'Intérieur. In *Procès-verbaux de la chambre des députés* (pp. 189–196).
- Girard, R. (2002). What Is Happening Today Is Mimetic Rivalry on a Global Scale. *South Central Review*, 19(2/3), 22–27. <https://doi.org/10.2307/3189861>
- Glaser, B., & Strauss, A. (1999). *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Aldine.
- Goldsmith, J., & Wu, T. (2006). *Who Controls the Internet?: Illusions of a Borderless World*. Oxford University Press, USA.
- Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology*, 51(4), 605–622.
- Harris, S. (2014). *@War: The Rise of the Military-Internet Complex*. Boston: Eamon Dolan/Houghton Mifflin Harcourt.
- Headrick, D. R. (2012). *The Invisible Weapon: Telecommunications and International Politics, 1851-1945* (Reprint). OUP USA.
- Hibou, B. (2012). *La bureaucratisation du monde à l'ère néolibérale*. Paris: La Découverte.
- Hurt, S., & Lipschutz, R. (Eds.). (2015). *Hybrid Rule and State Formation: Public-Private Power in the 21st Century* (1 edition). Routledge.
- Jacomy, M., Girard, P., Ooghe, B., & Venturini, T. (2016). Hyphe, a Curation-Oriented Approach to Web Crawling for the Social Sciences. In *International AAAI Conference on Web and Social Media*. Köln, Germany: Association for the Advancement of Artificial Intelligence. Retrieved from <https://hal.archives-ouvertes.fr/hal-01293078>
- Kuner, C. (2015). Data Nationalism and Its Discontents: A Response to Anupam Chander & Uyê P. Lê. *Emory Law Journal Online*, 64(2089). Retrieved from <http://law.emory.edu/elj/elj-online/data-nationalism-its-discontents.html>
- Lécuyer, C. (2007). *Making Silicon Valley: Innovation and the Growth of High Tech, 1930-1970*. Cambridge, Mass.: The MIT Press.

- Levine, Y. (2018). *Surveillance Valley: The Secret Military History of the Internet*. PublicAffairs.
- Levy, S. (2001). *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age* (1st edition). London: Penguin Books.
- Lyon, D. (2015). *Surveillance After Snowden*. Polity Press.
- Manes, J. (2015). Online Service Providers and Surveillance Law Transparency. *Yale Law Journal Forum*, 125, 343.
- Mattelart, A. (2010). *The globalization of surveillance*. Polity.
- McChesney, R. W. (2013). *Digital Disconnect: How Capitalism is Turning the Internet Against Democracy*. The New Press.
- Mills, C. W. (1959). *The Power Elite*. Oxford University Press.
- Mitchell, T. (1991). The Limits of the State: Beyond Statist Approaches and Their Critics. *The American Political Science Review*, 85(1), 77.
- Morozov, E. (2013). *To Save Everything, Click Here: The Folly of Technological Solutionism*. New York: Public Affairs,U.S.
- Mosco, V. (2014). *To the Cloud: Big Data in a Turbulent World*. Boulder: Routledge.
- Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press.
- Peoples, C., & Vaughan-Williams, N. (2010). *Critical Security Studies: An Introduction*. Milton Park, Abingdon, Oxon ; New York, NY: Routledge.
- Pohle, J., Hösl, M., & Kniep, R. (2011). Analysing internet policy as a field of struggle. *Internet Policy Review*, 5(3), 426–445.
- Poupard, G. (2016). Towards European Digital Sovereignty. *The European Files - Cybercrime, Cybersecurity and Cyberdefense in Europe*, (40), 36.
- Powers, S. M., & Jablonski, M. (2015). *The Real Cyber War: The Political Economy of Internet Freedom* (1st Edition edition). Urbana: University of Illinois Press.
- Project, B. C. (2016). “Don’t Panic”: Making Progress on the “Going Dark” Debate. Cambridge: Berkman Center for Internet and Society. Retrieved from <https://cyber.law.harvard.edu/pubrelease/dont-panic/>
- Roberts, S. T. (2016). Commercial Content Moderation: Digital Laborers’ Dirty Work. In B. M. Tynes & S. U. Noble (Eds.), *The Intersectional Internet: Race, Sex, Class, and Culture Online* (pp. 147–160). Peter Lang Publishing.

- Rogers, M., & Eden, G. (2017). The Snowden Disclosures, Technical Standards, and the Making of Surveillance Infrastructures. *International Journal of Communication*, 11(0), 22.
- Rouvroy, A. (2012). The end(s) of critique : data-behaviourism vs. due-process. In *Privacy, Due Process and the Computational Turn*. Routledge. Retrieved from [http://works.bepress.com/antoinette\\_rouvroy/44](http://works.bepress.com/antoinette_rouvroy/44)
- Rubinstein, I., & Van Hoboken, J. (2014). Privacy and Security in the Cloud: Some Realism About Technical Solutions to Transnational Surveillance in the Post-Snowden Era. *Maine Law Review*, 66(2), 488–533.
- Schiller, D. (2000). *Digital Capitalism - Networking the Global Market System* (Reprint). MIT Press.
- Schiller, D. (2014). *Digital Depression: Information Technology and Economic Crisis* (1st Edition edition). Urbana, Chicago: University of Illinois Press.
- Schulze, M. (2017). Clipper Meets Apple vs. FBI—A Comparison of the Cryptography Discourses from 1993 and 2016. *Media and Communication*, 5(1), 54–62. <https://doi.org/10.17645/mac.v5i1.805>
- Siokas, E. (2018). Network Analysis of EU-Funded R&D Collaboration in the European Security Research Programme: Actors and Industries. In *The Emergence of EU Defense Research Policy* (pp. 221–245). Springer, Cham. [https://doi.org/10.1007/978-3-319-68807-7\\_12](https://doi.org/10.1007/978-3-319-68807-7_12)
- Tilly, C., & Tarrow, S. (2015). *Contentious Politics* (2nd edition). New York: 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. Presented at the 7th Biennial Surveillance & Society Conference (SSN 2016): "Power, performance and trust". Retrieved from <https://halshs.archives-ouvertes.fr/halshs-01306332/document>
- Tréguer, F. (2016b, October 26). French Constitutional Council Strikes Down “Blank Check Provision” in the 2015 Intelligence Act. Retrieved October 27, 2016, from <http://verfassungsblog.de/french-constitutional-council-strikes-down-blank-check-provision-in-the-2015-intelligence-act/>
- Tréguer, F. (2017a). Intelligence Reform and the Snowden Paradox: The Case of France. *Media and Communication*, 5(1), 17–28. <https://doi.org/10.17645/mac.v5i1.821>
- Tréguer, F. (2017b, November 2). *Pouvoir et résistance dans l'espace public : une contre-histoire d'Internet (XVe -XXIe siècle)* (phdthesis). EHESS - Paris. Retrieved from <https://halshs.archives-ouvertes.fr/tel-01631122/document>
- Wagner, M. (2009). Warrantless Wiretapping, Retroactive Immunity, and the Fifth Amendment.

*George Washington Law Review*, 78, 204.

Webb, J., Schirato, T., & Danaher, G. (2002). *Understanding Bourdieu*. SAGE.

Weinstein, B. (2015). Legal Responses and Countermeasures to National Security Letters. *Washington University Journal of Law & Policy*, 47, 217.

Williams, M. C. (2010). The Public, the Private and the Evolution of Security Studies. *Security Dialogue*, 41(6), 623–630. <https://doi.org/10.1177/0967010610388210>

Zuboff, S. (2015). Big Other: Surveillance Capitalism and The Prospects of an Information Civilization. *Journal of Information Technology*, 30(1), 75–89. <https://doi.org/10.1057/jit.2015.5>

# Appendix 1: Roundtable “The Internet, Private Actors and Security Challenges” (CERI, October 9<sup>th</sup>, 2017)

## Programme

In the first of three conferences to be held over the next year, Didier Bigo (CERI-Sciences Po), Laurent Bonelli (ISP-Paris-10 Nanterre) and Sebastien-Yves Laurent (CMRP-Bordeaux) from the ANR project UTIC are bringing together representatives of major online service providers for a high-level experts roundtable.

Participants will look at the ways in which technology firms engage with policy-makers and law enforcement agencies to address today's major security challenges: How did their relationship with intelligence and law enforcement agencies evolve amidst heated post-Snowden debates on surveillance and privacy? What are the main legal hurdles faced by online service providers to protect the rights of their users, and what changes in legislation are called for? How do these companies adapt their business practices to help address today's security challenges?

By looking at these important issues at the intersection of policy, law and technology, the roundtable will analyse public-private relationships in the fields of surveillance and security, offering an opportunity for a much-needed discussion between key international stakeholders and researchers.

To facilitate the discussion, the roundtable will be divided in two parts during which representatives of leading Internet companies will share their insights in interaction with researchers. The audience will have an opportunity to join the discussion during Q&A sessions.

### Participants:

Acadia Senese – Google, Legal Counsel, Law Enforcement & Information Security

Nicole Jones – Google, Senior Law Enforcement & Security Counsel

Marc Mossé – Microsoft Europe, Director of Government Affairs

Gail Kent – Facebook, Director for global cybersecurity, surveillance and law enforcement

Maud Sacquet – Computer & Communications Industry Association, Senior Manager for Public Policy

### 14h00-14h30: General introduction

Alain Dieckhoff, Director of CERI-Sciences Po and Didier Bigo, Sciences Po-CERI, UTIC Coordinator

### 14h30-16h15: Roundtable discussion (first part)

In the first part of the discussion, representatives of leading Internet companies will share insights about how post-Snowden controversies on surveillance have impacted their work and relationships with other stakeholders, and what changes in their business practice ensued

Chair: Olivier Chopin, Deputy Director of the Reims campus, Head of Academic Affairs

Discussant: Félix Tréguer, Sciences Po

Q&As session

### **16h45-18h30: Roundtable discussion (second part)**

In the second part, we will focus on today's key legal priorities for Internet companies, who have to face a fragmented legal environment and strike a balance between competing interests. What are today's main legal hurdles and what are the opportunities for reform?

Chair: Alex Mcleold, UQAM-Montréal

Discussant: Joris van Hoboken, University of Amsterdam

Q&As session

### **18h30-19h00: Concluding remarks**

Ronald Deibert, Citizen Lab, University of Toronto

Thierry Delville, Ministerial Delegate for the Security Industries and the Fight Against Cyber Threats

## **Draft transcription by Barthélémy Michalon**

Introductory words by Alain Diekhoff, director of the CERI

Good afternoon and welcome to the centre for international studies which I have the pleasure to head for some years now

It's my pleasure to welcome you to this conference on the Internet private actors and security challenges. So this conference is the first of three conferences to be held over next year. It's part of the ANR UTIC which is coordinated by Didier Bigo, Laurent Bonelli and Sébastien-Yves Laurent. Didier is professor here in Sciences Po, Laurent Bonelli is at the university of Paris-Nanterre and Sébastien-Yves Laurent is in Bordeaux.

This ANR (national research project) is this afternoon bringing together representatives of major online service providers and we'll start the discussion on things which are of course important nowadays, which are the security challenges brought by the tremendous development as we know, sometimes unfortunately I would say, of the Internet.

Anyway I am happy to welcome all those people here on this round table for the whole afternoon. We have several distinguished chairs and also discussant which will be introduced by Didier in a moment inspired. I am pretty sure that you will have a good start today for the first conference and very fruitful debates for the whole afternoon. Very briefly, for those who don't know CERI: it is the largest research unit here in Sciences Po, with about sixty full-time researchers and professors (I do not go into the details of the status which are quite different and complex for non-French and even for French sometimes I would say). The centre is dealing with very different issues of course: [boundary?] studies, international relations, international political sociology, the question of defence, the question of security, which are different matters of course have always been quite important here at CERI and I must say that Didier has played a very important role in the last at least 25-30 years in this field and I see that with this conference he's going on with his deep involvement in Security Studies.

Without taking more time, I will give the floor [to Didier] and he will introduce the analysts and the whole project maybe this afternoon.

[APPLAUSE]

[3'30 - Didier Bigo]

I will try to be very brief also, but just in a nutshell, to give you an idea of what is this project called UTIC or RESO: Renseignement, Espionnage, Surveillance, Obéissance, or in English Intelligence, Espionnage, Surveillance and Obedience (RESO, Network and ISO for norms, technical norms and how they work). What do we want to do? We began this project in 2015 and it will continue until 2019.

As Alain said, it involves three universities, so we have here Sciences Po with the CERI but we have also Nanterre and Bordeaux but we are also a lot in touch with all the universities around the world, we have contacts with a lot of people working in Germany, in the UK, also in Canada and we will see that with also the people arriving and I think it is important because it cannot be addressed as a national question.

This is sometimes one of the problems of the framing of the research because we have a lot of projects. We are by far not the only one to work on that but what we have seen is that most of the questions, especially in the US, are organised regarding the national security of the US. Or the connection with the so-called GAFAM and the way they are organised together and it turns a little bit as if by definition there is a centre and there are the margins. Maybe we have to think more transversally and to try to understand what are the relations at the transnational level between all these different aspects.

So the first point that we wanted to analyse is really to review today's communications surveillance technology and the transformation brought by new computing capacities, integration platform or the so-called big data analytics because here of course you have a lot of research and very good historians who have done research about specific agencies: the history of the NSA, the history of the GCHQ, a little bit less about DGSE (we have good historians nevertheless in the room), and also about the other intelligence services, what are the connections between the ones which are not specialised in signal intelligence or on the Internet but in other activities anti terrorism, policing, law enforcement and how they are connected.

What is certainly important is to try to understand how Internet has modified or not - and that's really a question - the logic of surveillance: is it just an acceleration, an intensification, or do we have to reframe our reasoning when we speak about the Internet if we compare let's say with what is now an old story - which is not so old - about Echelon and the signal intelligence communication? So this is one of the elements and of course we have a lot of discussion about what does it mean to collect data in bulk. I suppose that we will come back to this discussion at some point.

The second is to understand the variation of the relation to technology among and between law enforcement agencies and their respective countries as well as the justification underlying surveillance practice. Also, to be very simple, just in a way of introduction: a lot of people consider that because technology can do it, it's done and so in some way a lot of NGOs also want to be activists, with sometimes very good reasons, have the tendency to accept that: because it's possible it's done. So what are the social use of Internet? What are the social use of the Internet by intelligence services? How far do they go into this question?

[9'06] And the third is certainly to try to analyse how this question of what they call national security and claims to secrecy is connected now with the question of the global nature of Internet. So it looks like it really turns around security studies but that's not what we want to and that's crucial. Because if we analyse the question through the perspective of security studies we immediately introduce a major bias which is to take the position of one actor as if it was the central actor and that this actor are the different states or the interstate relations and not to look at the different agencies, the relation and competition there are between them and also to understand that in many cases they are not at all in a position of controlling everything, that they may on some point but it's not just, let's say, this kind of vision where you have a state surveillance of an Orwellian kind and its diffusion: it's certainly more complex than that, it's more horizontal.

[10'37] But at the same moment you have lot of inner resistance at all levels. And typically with the question of if national security government is about the fear, the anxiety of the [...?], of global insecurities, one of the questions has been: what is the solution? National security, [versus] global insecurity. An international collaboration of states and agencies regarding what they call themselves sensitive information on suspect groups? Yes, it looks like a solution but if you have the acquisition of information globally, if you have links between the relevant information and if you want policies of prevention, you arrive to a second major tension: national security, shared secrets but at the national level [versus] acquisition of information on suspects at the global [level]. So your national security is purely national arrived at what? A form of egoism, a form of incapacity to regulate nationally. So, what's going on? If it's seen as insufficient you have to have a belief in technology, you have to consider, and that's maybe one of the frame which has to be discussed, that, for most of them, technology will resolve what political judgement can not. In that case, they focus their attention on what the technology is regarding mobility of people, mobility of capital and, centrally, mobility of information.

[12'43] And then, what happened was that the focus of many intelligence services has been toward the Internet as a source of organising their new activities and the old ones with different methods. That's why, certainly beyond signals intelligence, investigating the Internet has become a key element of this logic. But the management of data is done by private actors, so what are the relations? These actors have been put in a situation of constraint, to be obliged to deliver some data, through changes in the legislation. They have tried (and there the category of private actors [encompasses] a lot of different companies) and they did not have all the same reactions (it will be interesting to discuss about that). How

to comply to legislation but how also to give to your consumers forms of protection, security about their own rights?

[14'13] So a lot of companies who were in charge of managing data have been more and more included into different stories about what kind of relations we may have with our public, but this public has privacy rights, they are citizens, they are citizens and foreigners, they live somewhere but they use Internet to be connected... So what is the logic of rights and what are the forms of resistance?

[14'51] I will stop here, because I don't want to "destroy" the discussion by imposing some views. On the contrary, I think what is important is just to be ready to deconstruct some categories we spontaneously have (the state, the private actors, the others...) and to blur the lines. All of these actors and the relations they have. So I will leave now the floor but I will first ask the president of the first round table to introduce our different partners. I really appreciate that you have accepted to come.

[15'45 - Olivier Chopin] Thank you Didier. [...] My name is Olivier Chopin, I am member of Sciences Po and the academic director of the Reims Campus, so for the undergrad programme in Sciences Po. My personal research deals with intelligence studies and surveillance and I thank Didier Bigo for asking me to chair this first round table today.

[16'20] I am very thrilled to introduce the first discussion and a lot of high level representatives of leading Internet companies will share with you today their insights and their reflections on how controversies that happened after Snowden's revelations affected their works, their relationships between themselves, with the judiciary, with governments and all the different actors involved in the story, even of course the general public and the audience. We would love to have a real dialogue, not only a discussion but a dialogue between yourselves: how it affected and changed your business or your representation of your own activity.

[17'20] Félix Tréguer will be your discussant in a few minutes: he will listen to everything you say and will have a discussion with you here within the panel and will keep around 30 minutes to have questions with you [in the audience]. Of course do not hesitate to prepare your questions and to ask questions later.

[17'44] As we have enough time, maybe we can start with a personal presentation by yourselves, so I will leave you the floor for two minutes each of you to present yourself and give maybe some background and some context about your activity and how it will impact your discussion in a few minutes.

[18'06 - Acadia Senese] Good afternoon everyone and thank you so much to the centre for having us here this afternoon. We are just so thrilled to be able to participate in the discussion in this topic which is near to me. I'm attorney in the information security team, advising Google on data disclosure requests from around the world and as part of my work I also support the policy team for the work they are doing globally to update and reform surveillance law. Prior to joining Google I was a federal prosecutor within the Department of Justice and so working for law enforcement with working cases I used to be on the requesting end, sending requests to companies to obtain data so I now have an interesting vantage point being on the receiving end of those requests, having to balance conflicting laws across the world and in advising Google on their data disclosure obligations.

[19'12] But I think you know as an opening remark we very much agree that surveillance reform is a transnational question, it's not one that particular to any one country and it is really going to require agreement of nations to reform our surveillance laws. We're doing quite a bit of work and updating, er, insisting that the US Congress updates laws that allow companies to be able to respond to demands from other requesting nations (and I will talk a little more about that) but it's certain and we agreed that in an era where technology has proliferated in our everyday lives where there are real security threats to individuals but also a real interest in privacy that the law needs to be updated to reflect all of those things. Anyway, thanks very much, looking forward to having a discussion with my fellow panelists and all of you today.

[20'18] I am Marc Mossé, from Microsoft Europe. Hi everyone, thank you, just a few words about who I am: I am working at Microsoft, I am leading the Government Affairs team in Brussels. Prior to that I was the government affairs and legal director for France, for about ten years, and before I was an attorney at the Paris bar association and I used to work with Robert Badinter, the former Chief Justice in France. I worked with him for five years. So I have some appetite from this time on civil liberties, fundamental rights, and all these topics we are covering today, aside of technology. And just to add one sentence on what you have said: all these topics should be treated through a transnational approach, for sure.

[21'24] I am Gail Kent from Facebook and apologies for being slightly late since I have come from Brussels. I lead for Facebook globally on security, law enforcement and surveillance which means three things in practice: when we are developing new products I look at what the likely impact is going to be on law enforcement, both from how people might use these products but also what details and what information law enforcement are likely to be asking us. I also provide advice to our colleagues around the world and I think we are going to talk a lot about the transnational elements

of surveillance today, when there are new legislations proposed in any country and then lastly I contribute to the debate on some of the huge issues that we're talking about today, whether that's encryption, whether that's about mutual legal assistance reform, whether that's what cybersecurity looks like in 2017 and onwards.

[22'34] The two things I draw from doing that and doing my current role are 20 years I spent in London in law enforcement in the UK as part of the National Crime Agency, leading on international operations and lately on international cybercrime operations that included a lot of working transnationally, including with Europol and Interpol and also I think now 5 years in academia, I had the great joy of landing in Stanford on a Fulbright Fellowship the day after Snowden [matters?] revelations: looking at transnational data sharing and MLAT reforms, that was quite a leak from, you can imagine, UK law enforcement and the civil service and to Stanford at the height of the Snowden revelations.

[23'28] So I am very much looking forward to enter this discussion today and I will definitely echo what both Microsoft and Google have said - and I suspect you won't disagree with each other quite a lot - but I think there are two things we have to think about here, or three things probably: One is that it is absolutely a transnational problem and I was in the US last week and the same issues I am sure we are discussing here today were discussed there. Secondly that there has to be greater transparency in these discussions: I think it is incredibly surprising the lack of transparency that exists in most countries around the world about what surveillance legislation looks like and even within Europe there are a lot of countries that are not transparent about how they carry out surveillance, even what they call surveillance. And then the last thing, and I think it is one of the reasons I am so happy to be here today, is that this can't just be a conversation only between governments or a conversation between companies, this also has to involve everyone talking together and a key part of that is academia and the NGO community because we can't do any of this unless we're clear that we've got to have the right human rights frameworks. Thank you very much.

[24'46 - Olivier Chopin] Thank you Gail, you anticipated my first question which would be the day after Snowden but first let's welcome Maud Saquet, who works in the Computer and Communications Industry Association in Brussels.

[25'07 - Maud Sacquet]. Exactly. Well, It's the CCIA for short, which, if you want the story, used to be known as the Communication Industry Association and after a few weird phone calls to the CIA, the actual real CIA asked us to change our name, to add another letter. Officially now it's the CCIA, so it's a trade association that represents tech companies in Washington and Brussels. On my side I am based in Brussels and work, I would say, mainly now on content issue and availability of online intermediaries, so content removal, copyright, audiovisual, etc. but I follow also from a slightly greater distance all the surveillance and law enforcement issues that are happening in Brussels, mostly because of my background, because prior to joining CCIA I was working for Yahoo! here in Paris and during those five years I was handling law enforcement relationship with French authorities so practical experience into what it means to receive a data request and then decide what kind of data should be handed over to law enforcement.

[26'22] There is no much I can add to what has already been said in the introduction: the transnational aspect of the discussion has been highlighted and transparency as well. This is something CCIA has been fighting for for a long time: I mean having offices both in Washington and Brussels gives us quite a unique opportunity to work on those matters on both sides of the pond and try to co-ordinate what is being done between Washington and Brussels on these matters so that is indeed very close to our heart on these issues.

[26'50 - Olivier Chopin]. Thank you very much. My first question will be what you record from the day after Snowden, at the beginning of June 2013, revealed that he had a lot of classified information proving that the NSA had been able to tap directly into Verizon, first, and the day after The Washington Post and the Guardian revealed that the secret program called PRISM gave the NSA the ability to access servers from the biggest us tech companies, and especially apple Google and Microsoft. So that was like a thunder, of course, those moments were recorded: you may know the documentary "Citizenfour" by Laura Poitras or even some fiction movies have been made about Snowden's life, so it was really a turning point in the history of surveillance. We of course as specialists could suspect a lot of those surveillance activities but then there was public proof of all those activities. So our first question is very simple and maybe even a personal one: Do you remember the moment - although you have already said a little bit about that - when this information was released? Were you already working on those issues: surveillance, civil liberties, the probability that some day the surveillance capabilities would be revealed to the general public? How did it impact you at the time? Maybe we can start with you, Acadia.

[28'43 - Acadia Senese]. Sure: I was actually still with the government when the Snowden's revelations hit, so I can't speak about what Google was feeling or thinking at the time, although I understand from my colleagues who were living and breathing these Snowden revelations at Google that there were 1) surprised by the revelations but 2) also frustrated because the portrayal of the revelations was not always necessarily accurate, so there was frustration with the government for its failure to correct and fix the inaccurate portrayals of some of the programs that were being discussed. But then on the other side of that, there were already ongoing efforts at Google to 1) deploy SSL across Google systems 2) to engage for example into digital due process coalition and to argue for surveillance reform and 3) to educate our

users about security, like using two-factor authentication. So Google didn't necessarily make any changes, although it certainly accelerated ongoing efforts that already existed at the time in terms of security, assistance [?] and educating its users.

[30'06 - Marc Mossé] I tried to remember what I was doing this day - you told me before the panel that you would ask this question, so I tried to figure out where I was. In fact I was reading the book, which is not a George Orwell book, but is a book maybe less well-known and I would recommend you to read it: it is "Le Palais des Rêves" (The Palace of Dreams), by Ismail Kadaré. It's a very interesting book because the main character of this novel is a guy with a very precise role, which is to monitor the dreams of people at night and come through the secrecy of life of everyone until the day he realises that on the list he will be the next whom the dream would be checked and monitored. So he realises that this day you are monitoring the dreams of others but one day it could come to your dreams. It's not just an anecdote because it was true, I was reading this book at that time, a very short novel and I would recommend you to read because it's a very nice way to think about where we are going today.

[31'39] On the technologic side, as Microsoft we were already working on the security and we had made at this time already a lot of investment and one entity which is called Digital Crime Unit because cyber security as a whole is very important for the company we were working on this and on the law and the general framework on the access to data which is not only surveillance but also the judicial requests because everyday as a telecom operator we get a lot of requests on investigations on the web. So we were already working on this and of course we accelerated, we sped up on this topic because immediately, and this is my immediate, I would say, feedback to these days, in addition to Ismail Kadaré's book, it was the questions from the customers and how trust is so important in the use of technology and in particular in a time when technology would be everywhere. The question of trust really went on the top of the discussion with the customers, with the government (not only the agencies but also the policy-makers), because at that time they realised that this question of trust could impact a lot the development of technology across the world.

[33'18]. If I had to summarize these days, I would say, first, read the book because it's a really nice way to think about the importance of fundamental rights at any time, the principles and the values are timeless and second how trust is important in the technology world.

[33'46 - Gail Kent] So I had just landed in California and I had come from the UK government so I don't know how many of you worked in European civil service but you can imagine that they are much more rigid than in California. In California in itself it was a bit of a shock and it was very very different from the Home Office and the National Crime Agency, where I was in London, to arrive in Stanford. And I was working with Jennifer Gaskell - sorry, for Jennifer Granick<sup>168</sup> - who was one of the people that really strongly pushed for reform on the basis of the Snowden revelations, so I had gone from working for a conservative (with a large and small "C") government to be with one of the most reformers - or advocates for US surveillance reform, so it was a huge cultural shock. I think I can say that it was one of the things that absolutely came out in my time at Stanford was realising that one of the most important things that we need to do - and I think you will hear me say this a lot today - is to try to understand different perspectives.

[35'05] But if I go back a bit to what I was thinking and what was Facebook thinking: obviously, I wasn't in Facebook at that time because it happened another two years before I joined but exactly the same as Acadia Senese has said: looking back into our understanding of a lot of details now, there was a lot of shock and surprise and the fact that these allegations were being made and the fact that the US government was not correcting them. Exactly the same as the other companies, the three things that Facebook started doing was making sure that we doubled on our own security - that is the most important thing to us: you cannot be the steward of two billion people's personal data without absolutely having to look after it properly and saving things securely. Pushing for reform and looking at what those standards would be - I'll come back to that - and then again working on who could be or who were the different groups that we could work with to do that. Another one [endeavour?] was to ditch the processes of the "Reform Government Surveillance"<sup>169</sup> alliance, which all of our companies are part of and which looks to or pushes to clear standards and surveillance reform around the world.

[36'30] I think for me Snowden was not just about that this absolute shock personally and understanding this sort of clash of these two worlds, it's also been known for how it has meant, positive and not so positive, over the last four years. I think we have to remember that wasn't just one moment in time, since we have seen safe harbour in the discussions around the privacy shield, which is very much what can be the impact of US surveillance outside of the US, then the 702 debate<sup>170</sup> which is still going until [it terminates? 37'12] will be renewed this year. For those of you who don't know that, this is the part of the US legislation that allows US law enforcement to make requests on companies like Facebook, Google or Microsoft for non-US citizens' information.

---

168. <http://cyberlaw.stanford.edu/about/people/jennifer-granick>

169. <https://www.reformgovernmentsurveillance.com/>

170. <https://www.justsecurity.org/31098/702-reform-debate-heating/>

[37'30] And just as this genuine need for greater transparency: what we saw through Snowden was a reinforced need to discuss what actually was happening and further to be going for a better clarity and we saw that in the US, we also saw the impact on the other Five-Eyes countries, so the UK was obviously in the discussion around the Investigatory Powers Act<sup>171</sup>, New Zealand, Canada and Australia have also had their own debates. But I think one of the things that we just don't see enough are those sorts of debates within countries.

[39'09] Whilst there is a lot I can disagree with in the Investigatory Powers Act - one thing the UK did do was have an hopeful / awful lot of reviews and trying to get there and try to listen to... at least let a number of different voices talk in that discussion. I think that's something we certainly would like to see even more of, in these discussions we were listening to other groups but also, more importantly, understanding the impact of legislation in one country on another. That's not just directly on companies like ours, but what happens if a country that's less democratic copies legislation from a democratic country: what does that mean? What is the impact of surveillance legislation on Human Rights is not just privacy and freedom of speech but what impact does it have on people's ability to connect as well. I think that is something that we really need to be, sort of, moving towards having. I think it does come a break because of Snowden, these discussions about what actually surveillance means for all of us from all these different perspectives.

[39'22 - Maud Sacquet] For my part, I was still working at Yahoo! at the time of the revelations. Something I mostly remember is a lot of shock, a lot of e-mails, a lot of phone calls, from colleagues, from friends asking "what is it exactly you're doing?", perhaps a weird look from other teams saying, "well, what is legal doing actually, on the fifth floor?". So, a lot of questions, I will try to perhaps to be too much, but try to understand where it was coming from, and especially trying, struggling to reconcile what I was reading in the press and what I was actually doing.

[40'12] For me on my day-to-day work I was doing my best to be helpful to law enforcement, to explain how things work, to be available, to help them in their investigations while at the same time protecting our users' rights and privacy, for example by interpreting as narrowly as I could a data request, to only hand in the strict necessary level of data [that I should?], which seemed the right balance I would say. So I was quite struggling to reconcile what I was hearing and what I was doing and then trying to explain it in a way that make sense to friends and family, actually wondering what my job was, suddenly. So that's perhaps the personal aspects of these revelations.

[40'56] From a purely perhaps policy side, and tech association policy side, so obviously I wasn't working there at the time but I also asked my colleagues about how they lived those revelations and what it changed for them in Washington mostly at the time. What was interesting from their feedback was that for them it was not new, in the sense that especially US surveillance reform had been something they had been working on for years, I mean since the adoption of the PATRIOT Act it has always been something that the tech industry was lobbying, I would say, in Washington and trying to rein in those kinds of programs as much as they could and partnering with academics, with NGOs, to try to feed a bit the discussion on those topics already pre-Snowden. One example again, so it comes back to Yahoo! (I think it will be the last example about Yahoo!), but that was following the Snowden revelations: Yahoo! was able to communicate on the fact but they were actually fighting against the US government in 2007 as far as I remember, calling some amendments of the surveillance program and fought indeed before the Foreign Intelligence Surveillance Court (FISC) because they thought that those amendments were overbroad and unconstitutional but [42'20] they lost but following these revelations they were able to declassify some of the proceedings of that Court. So it's just an example to show that really from a legal and policy perspective those facts were already happening before the Snowden revelations - I think that's the really first thing that my colleagues highlighted to me - while it was less visible at the time perhaps.

[42'40] The change that the Snowden revelations did for my colleagues was that suddenly those topics, which were part of a long list of topics we were covering, were pushed front and center, and that US surveillance reform suddenly became one of the main priority, the legislation we were working on and most of their lobbying efforts were being directed toward that topic.

[43'07 - Olivier Chopin]. Thank you. My next question will be a follow-up to Maud's answer: if now you look back to the four years that have passed since that shock and revelations, would you say that you learnt a lot of things about government surveillance, or did you have confirmation of things you know about because tech companies are involved, as you just said, in the process of collecting data, or did you revise your perception of what global surveillance from a government or from many governments can mean at some point? What did you learn, actually? Did you learn things and what was the most intriguing or most important thing that you discovered when Snowden did that revelation? Or maybe nothing at all? Who would love to answer first?

[44:16 – Gail Kent]. I think that what I learnt is what country you do not know anything about, so you now have a lot of information on what the US does, I mean you can argue you did not have enough, but we have all the Snowden

---

171. <http://www.independent.co.uk/life-style/gadgets-and-tech/news/investigatory-powers-act-bill-snoopers-charter-spying-law-powers-theresa-may-a7503616.html>

revelations themselves, we have the various abuses that have taken place most notably under the privacy and civil liberties, boards that we had to beat in Congress, we've had companies pushing for greater transparency, we still have ongoing cases that the companies continue to raise, pushing for [exacting the amount of thing? – 44'58], for making sure the US government is able to get the minimum and correct amount of information.

[45'09] France has also had a discussion around terrorism legislation, I think what is shocking here are the large number of countries that we genuinely do not understand what their legislation actually means. I see this in somebody whose job is reading this: there is a huge amount of opaqueness in surveillance legislation, often it is, I think Hungary, Polish laws, both of whom have had discussions in the last eighteen months, there we are looking at different layers of legislation on top of each other and try to understand what it means. I am not talking [specifically?] about those countries now but where there is a generic constitution you can almost do what you want for national security reasons.

[46'09]. That's why for me I am surprised there hasn't been more of a discussion and even within Europe, if this is in your interest I recommend you all read the Fundamental Rights Agency report on surveillance in Europe because that also shows you that even within the member states there is a huge variety of openness about what different countries do.

[46'38]. On top of that I think we still are grappling with the issue, again something that I continue to learn as a result of the Snowden revelations: there are no standards for what good surveillance legislation looks like. And I speak and unapologetically believe there are times in which law enforcement should gain access to information: I have investigated cases, whether they were rapes, or murder, or people trafficking where I absolutely believe the companies have the responsibility to work with law enforcement in a Human Rights framework to help protect the Human Rights of the victims of these crimes but there still isn't clarity, even I think within Europe, let alone internationally, about what good surveillance legislation looks like.

[47'34 – Acadia Senese]. To follow up on Gail's comments and also on Mark's, I think one of the biggest revelation from the Snowden disclosures was, frankly, a lack of understanding of what legislative landscape looks like, both in the United States and outside the United States with respect to surveillance laws. That lack of understanding – to Mark's earlier point – deeply contributed to a lack of trust among users. For companies like Google, users trust is critically important and one of the ways that we help users gain our trust [?!] is to be transparent with them about how we respond to government demands for user data. So in the wake of Snowden and this again is ongoing work, we have been fighting against the government to allow companies to be able to talk about the requests that we have been receiving, to disclose the number of requests, for example FISA requests and national security letters.

[48'36] That took lawsuit to do against the government to be able to disclose, in aggregate, the volume of requests that we are receiving, and we do that in the transparency report. But also it took lawsuits and ongoing lawsuits, some of which are still not public, to be able to describe to the public and the users what those requests look like, what the requests entitle the government to, how the companies define those requests and how the companies map those requests to the types of data that the companies may be able to disclose.

[49'10] So there's a common understanding among users and companies about how it is that we define metadata, how it is that we define content and how companies behave when they receive a request on those categories of data. So transparency is so important to us, it's important to the debate on surveillance reform but it's also important so that there is a common understanding about what it is we are discussing, what are the reforms we are working towards and so we can work together to drive coalitions to reform these laws.

[49'48 – Marc Mossé] Just a few words on this. In fact this is a very complicated issue because it's not only about surveillance, it could be about criminal investigation: we get requests every day from the authorities, I would say every [GOs?], every country. So it's very complicated stories and we absolutely need to frame the story in a way which is understandable and that we can fix with a concrete solution.

[50'21] Just a few comment here: as Google and Facebook we have a transparency report twice a year to give information on these requests. You get the statistics and you can access online to these reports: this is a first sign because, as you have said just now, it's a very important point to ensure transparency on this issue. Second aspect, and maybe the most important, is the rule of law. I do not want to be provocative but the question of public safety, privacy and fundamental rights is not a new topic, it's not a new debate. For years we had this, with our telecom (surveillance on your phones), even before the mobile phones we had this discussion about surveillance and access to data: it's not new. So because the debate is not new the values we are using are not new either. When we are talking about freedom of expression, privacy, freedom of communication, all these values are still valid and these are timeless values. It's not because technology is new that the values disappeared and the rule of law is critical here: yes, we give access to some data, only when the request is done according to the rule of law of the country where we operate. This is super important to consider.

[52:13] And I would love to give you one example because this is a post-Snowden story and maybe we'll talk about it

during the second round table this afternoon: The case we have today against the US government. Two years ago we had a request, a warrant from the US government, to have access to data stored in Europe and we refused to defer to this warrant. We went to the Court, we won before the Court of Appeal of New York and now the case may be taken by the Supreme Court: we'll know this in the coming days. It was critical for us because it was to set the US government. Of course you can ask us to access to data but only if you go through the rule of law. As a company, as [part of] the private sector and, I would say, as a citizen, it should be the North star. Principles and rule of law. Because, again, technology will not change the principle.

[53'30 - Maud Sacquet] There is not much I can add, to be honest. Perhaps just one point on what we learnt following the Snowden revelations. From a very Brussels perspective, I was wondering "what is actually the US doing?" We need to know, we need to understand and following a few years of debates, of reform, now the actual narrative in Brussels on those issues is: we know more about the US surveillance system than we do about the European ones. And that's an issue. Speaking for the Commission or Brussels institutions. And that's not normal. And so again, maybe (let's see how things evolve in the next few years), but maybe then the focus of the EU institutions will actually shift to what is actually being done within our borders rather than what is being done in the US, because we have now a clear understanding of what is happening over there. So that's really the change that we are seeing now, and that very striking, I would say.

[54'30 - Olivier Chopin] Now we are going to begin a series of more precise questions, but following up what you have just said: you talk about general principles and you publish transparency reports. That's maybe more for the general public than for your users or customers. How did your companies manage to restore confidence and trust, as a provider, to customers on a day to day basis? Because I believe not everyone who uses a Gmail account has read the transparency report from your company. So it's a general discourse. So how did you face the question of distrust between your customers and yourselves?

[55'18 - Gail Kent]. So I think the first thing that Facebook did was coming out straight away after the Snowden revelations and Mark Zuckerberg made a statement saying [that] we never have offered any government access, not to the US government or any [other] government to our servers. And that remains exactly the same today. So I think it's also us being transparent. I can't agree more with what Marc has said about trust as fundamental: if you lose the trust of your users. then they stop using your services and also, worse than that, they stop trusting the internet. And if we lose the trust people have on the Internet then we lose all the amazing benefits that we all gain through the access to connectivity that we have. So it's about being transparent, it's about people understanding when we do give over data, so we all publish those transparency reports and we also publish - the same as Google, Microsoft as well and a lots of companies - very clear guidelines for when we do provide data and what data we do provide to law enforcement. So it's being clearer now, maybe every user isn't look at the transparency reports and isn't looking at the amount of data their own country is asking for, but if they do want this information, it is available and it is there. We obviously do panels like this, where we are trying to talk as much as possible about what we do and to provide information. I think that, lastly, the most important thing we are consistently fighting for (both in Courts but also when there is new legislation and discussion like the Commission one on e-evidence) is the ability to notify our users if we are asked to provide their data. Now, something that we believe as incredibly important so when law enforcement comes and asks for any of your data, that we can say: "you know what, law enforcement has asked for those data". So we give the users themselves the ability to challenge that.

[57'48 - Olivier Chopin] That was not the case before Snowden's revelations, you came to that...

[57'54- Gail Kent] I am trying to remember whether it was the case in the US because I think it's actually part of... it comes under US law and again it's something we're [stumbling upon?] about just not knowing very much about the EU. One thing the e-evidence process has thrown up [?] is that user notification really varies from country to country, so there are some countries where it's obligatory, or [in as in most countries] obligatory unless it's going to undermine the investigation, they often can ask a prevention of a company notifying the user until the investigation reaches a certain point. Some countries do not mention it, some countries make it an offense in itself to notify the users, which is undermining due process. And I think that shouldn't be the case. One of the principles of government surveillance is the ability to tell a user that their data is being requested.

[59'03] We all see a huge variety of requests everyday, most requests that Facebook get are ones I think what most people in this room would agree with we should be providing that data. But they are ones where we definitely don't want to be providing that data or where we believe the user should have the right to contest them.

[59'30 - Acadia Senese] We have been similarly advocating for the ability to notify our users when we receive a request and I think here is an example where US laws are a little bit better on this point in the sense that we aren't prohibited under US law from notifying our customers of the existence of a request, unless it's accompanied by a specific non disclosure order. So in the United States unless we are prohibited from doing so we do notify our users and some of them go to Court and challenge the request. And that challenge happens while the company stays on the sidelines and

waits for the litigations to play out. So there is that avenue in the US and interestingly some of the states - California being one of them - require the law enforcement officers themselves to notify the users when they make a request to a provider. So even if a provider didn't notify the customer, law enforcement would be required to do so themselves. At least on that front we've made headway with respect to being able to provide notice to our users, to tell them not only that we have received a request but in some cases being able to provide a copy of that request so they can make a challenge in Court.

[1:00'50 - Marc Mossé] Very briefly, because most has been said. First, we reiterate the fact that we don't give access to all data. It's clear. We just provide access to data when there is a request compliant with the rule of law. It's super important. And even in this case, as you have just said, first we have the law enforcement department to go to the customer, first. It's really the principle. And if not we ask to be transparent with the customer and we won the case with the Seattle Court - I don't know if you are aware of this one - because the law enforcement agency refused that we disclose the request to the customer and we won this case. It's a really important point. I am sorry to be repeating myself here but, to understand how we work in this question of trust, we also go back to the rule of law.

[1:02'00] It's not our decision, this is really in the respect of the law, in the US but it could be as well in other countries, such as in Europe. We had a lot of discussion, even with the French government, to work on a framework which is really respectful of the principle.

[1:02'20 - Maud Sacquet]. Perhaps a few things. First on the possibility to inform the users whose data have been requested, I remember indeed when this concept was discussed at the European level, within the [countries?] of Europe at least, where US colleagues were surprised that we didn't have a ready answer as to whether we could disclose the data request to the users actually because it was very complicated to figure out, especially in national law, because it was not something that was taken into account when the law was written and so something that we could easily answer. So it stirred a lot of debate about what was actually possible under European law or French law.

[1:03'13] From a more "policy" perspective, this issue of transparency reports and of disclosure of the type and number of requests was something that was key. In our lobbying in Washington for US surveillance reform with the adoption of the USA Freedom Act a couple of years ago, more transparency, especially regarding the types of requests that we were receiving and the possibility for companies to disclose this request, that was one of the elements of the reform of US surveillance. That's something that the companies and the industry as a whole fought for, to include more clarification and more transparency on that point.

[1:04'00] The other and last interesting reform of US surveillance (and maybe that will be discussed later) is that the US government also adopted what is called the Judicial Redress Act, adopted at the beginning of 2016 if I am not wrong, in which the idea actually was to go back to the idea of trust. Well, how do we ensure that all European users and European citizens actually trust the US government and US service providers, that we are not going to do a mass collection of their metadata in surveillance programs like the one that Snowden revealed? Through this piece of legislation now Europeans have the right to review for inaccurate data to be corrected to [by?] US federal agencies [?], they have the right to challenge the fact that their data were shared by the government [companies, instead?] with US federal agencies. They have the right to challenge their own agency and US federal agency if their data wasn't fully disclosed [??]. I mean: there has been again some measures that were adopted at the US level to try to address the trust issue and to give European citizens similar rights than the ones American citizens can enjoy in the US on that matter. That was something really important that we fought very much for in Washington.

[1:05'37 - Olivier Chopin] Could some of you explain if (or not) you have some relations with advocacy centers for civil rights or privacy, or civil liberties. Did you interact with organizations like ACLU<sup>172</sup> or FIDH in France? If you did, how? Could you give some examples of how you managed to access to them or work with them in order to advocate more for that trust with the government?

[1:06'10 - Gail Kent] Sorry for jumping in so quickly. As I said at the start, understanding all the different perspectives is really important and especially understanding what are the Human Rights implications of surveillance. It means talking to people who spent their time thinking about this in a huge amount of detail. So we have regular conversations with a lot of different NGOs who were thinking about this through a number of different perspectives. What I would say is these are things that we are also thinking about ourselves. This is not that we go to Human Rights groups to get the Human Rights perspective because we aren't capable of thinking about it. We absolutely are. One of the reasons why I joined Facebook was because of the mission Facebook has and because of the idea that we could connect the world and we can do that in a way that is connecting the world safely and taking into account Human Rights. I would say that possibly one of the misconceptions that people have is that the companies are all about power - and we'll talk about that later [...].

---

172. American Civil Liberties Union.

[1:07'44] It's really important to be understanding what we are doing from all the different perspectives. Part of that is talking with people at the UCLA, the Electronic Frontier Foundation, CDT<sup>173</sup>, the Government Information Technology<sup>174</sup> [?], Privacy International... and trying to get all those different perspectives. One thing I would like to say and that Maud was mentioning earlier is that there is a lot of debates in Europe around privacy, it's incredibly important to us as Europeans (I can still see that I'm a European at the moment, as a Brit).

[1:08'30] What I have found is that there isn't as much conversation around surveillance and what European governments are doing, so there is a slight vacuum compared to what is in the US for NGOs talking about this sort of issues. But when they exist I am really really happy to have those conversations, to make sure we can understand their perspectives and be given a different way of looking through things that we haven't thought through that already.

[1:09'02 - Acadia Senese] NGOs are critical components of the debate and the conversations that we're having between and with companies and the governments and the NGOs talking about surveillance reform, you know, RGS<sup>175</sup> being one of the groups that Google participates in. I think one of the main reasons why the coalition and those working groups are so critical is the education that occurs when you're in those conversations and you are talking as a company to an NGO, to a government official about where the pinpoints are, what the needs are, what the concerns are, and trying to move towards consensus on what reform could be like, reform that includes basic human rights standards, due process of law, privacy protections... Then each one can bring something very different to the table but it's in those conversations, with all three groups in the room, when really (in my opinion anyways) the progress is being made.

[1:10'05 - Marc Mossé]. I would same the same: NGOs and citizens are critical in this process. It's a multi circular approach and the dialogue is not only between the Tech industry and the government, it's really the NGOs and the citizens involved in these discussions. If I look at the New York case, the one I mentioned earlier, we have seen in the Court of Appeal a lot of Amicus Briefs, a kind of intervention (which it is not exactly the case in terms of procedure) from the NGOs. You can go to our website, digitalconstitution.com<sup>176</sup>, and you will see all the briefs from these NGOs, they brought their arguments in the case to the Court. Here are the principles at stake and as part of this ongoing dialogue or, I would say, conversation, we absolutely need to have the citizens and the NGOs involved.

[1:11'09]. I just remember one thing ... Some years ago, when I was leading the French team, I have been heard by the National Assembly committee in charge of one of these reports on Fundamental Rights in Internet and we had a lot [of such reports?]. I have been questioned by the MP saying "in France and in Europe we are taking a lot of care of privacy and they have no interest in this in the US". I said "no, you're wrong" because at that time (I am talking about maybe 8 or 9 years ago, it was a report issued by Patrick Bloche and Jean-Yves Warsmann<sup>177</sup>), at that time the civil society, the NGOs in the US were much more involved and active on this topic than in France. Because often we consider that in France and Europe we are much more active but I've been impressed of that time by how the NGOs and the citizens were really involved on this topic in the US. And it came to my mind at this time that this story could go a little bit further if really, across the world, NGOs and citizens worked together.

[1:12'25] It's not EU against the US, it's how we build a bridge between our common values because in fact if you look at the reality of this question, it's about values that are largely exactly the same. They can be interpreted in different ways, we could have in the US, I would say, a more consumer approach to privacy rather than a Fundamental Rights approach in Europe - we can discuss this - but at the end of the day the principles are the same, the values are the same and what we have to build is a common approach on this question of principles.

[1:13'04 - Gail Kent] Can I just add something that is really really important? One thing I have seen a lot of is particularly (I think we'll come in the second half to discuss Mutual Legal Assistance Reform and I think we have already mentioned some of the reforms in the US Congress) EU groups complaining about US surveillance because that's not fair and US groups complaining about EU surveillance because that's not fair, which does sort of put companies very much in the middle, rather than, exactly as you said, a much more cross-cultural distinction about what would "good" look like. Because at the moment we can't be in a position where US groups can say "all this is OK in the US but you Europeans can't gain access to any data" or European groups saying "It's OK what's happening in Europe but you, US are really really bad and you are spying on everyone. It looks like they were talking past each other<sup>178</sup> and we absolutely do need that, I would say, conversation about what that does really look like in reality and what that look like for all of us.

---

173. Center for Democracy and Technology - <https://cdt.org/>

174. <https://www.gov.uk/government/collections/ict-strategy-resources>

175. Reform Government Surveillance.

176. <https://blogs.microsoft.com/datalaw/>

177. Probably <http://www.assemblee-nationale.fr/13/rapports/r4326.asp>

178. Talking past each other is an English phrase meaning two or more people talking about different subjects, while they believe that they are talking about the same.

[1:14'28 - Marc Mossé] If I may just add one point, because it's a very important aspect in the discussion. Some years ago, we had in France a bill on surveillance, some could remind this, and at that time the entire Tech industry, maybe for the first time ever, all the business association and IT association worked together to lodge an Amicus Briefing to the attention of the Conseil Constitutionnel (because it was seized, at that time) and one of the important parts of the brief from the industry was to say "OK, whatever you decide on this bill, the most important is to go to the principle in a way to build this bridge with the US" because at that time we had the decision on *Riley vs. California* in the US, we had this case on the way on the warrant I mentioned earlier and the idea in this memo from the industry was to say "OK whatever you decide, your decision should pave the way for such a way for a dialogue with the US and a dialogue across the world".

[1:15'57] I have to say, with the decision of the Conseil Constitutionnel, maybe we have not been totally followed but it was a first step thanks to the Quadrature du Net and others the Conseil Constitutionnel has been able to give more details on some points but it's an ongoing dialogue, for sure.

[1:16'19 - Maud Sacquet] Perhaps a last point, more generally, on the cooperation between the industry and NGOs, which is indeed a key one, as I had highlighted before. It's also fascinating, for me working and representing the industry in Brussels and working with NGOs. It's indeed perhaps a bit more done in the US than it is at the European level. And also there is, I would say, a friend/enemy relationship where we agree on some issues and we *absolutely* [emphasis] disagree on other issues. So it's often a question of "you are working with this NGO" - I say: "Yes, of course" - "But they hate you on that one" - I say "Yes, but we are also friends". So it's really weird sometimes, this kind of relationship that we can have, but at least on many issues we are able to cooperate, for example right now on content issue and copyright reform, which is, actually, crucial for fundamental rights, I could talk about it later I think, but it's about content removal.

[1:17'20] But on many issues such as surveillance, intermediary liability, content issue, etc., there are many areas where there is a lot of cooperation possible between NGO and industry and that's where, I think, we are the most powerful, heard and relevant. But it's not the case on all issues. Perhaps the main problem that we would have at the EU level compared to the US is that there are NGOs in Brussels that are covering European issues but many NGOs are actually national and it's not easy for them to be, even by financial means, to be aware of everything that is happening in Brussels, to come in Brussels and be heard, so they often work with different groups, associations that will represent several NGOs but that limits perhaps the number of representatives that you can have in Brussels and perhaps they are less heard than they could be or should be on those issues. This is a concern, it's improving honestly, year after year, but that may be the main difference between the US and the EU policy on how this kind of cooperation is done.

[1:18:37 - Olivier Chopin] Maybe to focus on one of the points you have just addressed a few seconds ago, this question will be for Gail, Acadia and Mark first, and I'll have another one for you, Maud, in a few seconds. That's because it's about collaboration between companies. I am kind of struck by the kind of consensus you reach here on those issues: you are different companies and sometimes in a kind of competition on the market. So can you explain: do you interact with each other after Snowden's revelations? Did you come to talk to each other about how you should respond, what the proper attitude would be towards the revelations, or how do we push for new legislation in Europe, in the US? Is there some kind of coordination between the companies or not? We'll have a kind of reverse question for Maud in a few seconds.

[1:19:30 - Acadia Senese] Maybe I think the companies align on issues in a very similar way because we have very similar difficulties, for instance responding to government demands for users data from all over the world where there are conflicting laws, where, as Marc said, we are law-abiding companies, where we all respond to lawful demands or requests but we have to navigate conflicting laws to be able to do so in an accurate way. So many of the pinpoints that Google has, for example, are shared with Microsoft and Facebook.

[1:20'11] So we do align on many issues, even if it's not so much a planned collaboration or coordination but we land on the same spot. With Microsoft for example as Marc has mentioned, the litigation in the US involving the government's ability in the US to use a search warrant to compel the production of data that may be stored beyond the borders of the US. Unsurprisingly, Google had similar litigation after the Microsoft case proceeded to the Appeal Court and Microsoft there filed an Amicus Brief in one of Google's cases. So we do have, and we joined with Amici with Facebook on other matters as well, so there is collaboration, even if not so much coordination, but certainly, I think, from Google's perspective, there is great value in identifying as an industry some of the reforms that are needed, bringing a common voice to the table when we are drafting with government and NGOs so that we can move forward.

[the other speakers approve the idea]

[1:21'42 - Olivier Chopin] So, to Maud, as a policy officer based in Brussels and working for different companies, did you feel that at some point the Snowden revelations were a turning point in the way companies reacted or coordinated maybe more closely and even the relations between legal and tech guys within the companies working for solutions ...

Do you feel there was a collective reaction and maybe that's not the same in Europe and the US...

[1:22'20 - Maud Sacquet] That's an interesting question from a trade association perspective because by default all members, all companies we represent have to coordinate within the association to agree on common position that the association will put forward publicly. So there is always coordination and I can guarantee that the companies are clearly competing against each other because sometimes it's a nightmare to actually get a common position that you can go and advocate for.

[1:23'00] On surveillance, specifically, I would say the coordination is perhaps slightly easier than on other topics because of the principle, because of actually, there are not hundreds of ways to approach that issue compared to content, telecom policy... So it's perhaps a bit more clear in that area, it's easier to get coordination. It's also interesting to see coordination between trade associations and between the different sector' representatives you can have. Often time [?] even though you could also argue that tech associations compete against each other as well, for additional members and for leadership on certain issues. So we are definitively competitors but it's well recognized that we are often more powerful if we act together, so in many issues, including surveillance, you will see a lot of coordinated action, common joint letters, for example signed by the entire tech sector in Brussels advocating for reform and that we ask for coordination between trade associations and within companies to agree on that messaging, so it can be common event, it can be associations replacing each others at working groups meetings if some can't make it that day but we have to be there...

[1:24'28] So it's also a close-knit community, where we try to act as the best as we can and to have a unique voice on those issues.

[1:24'39 - Olivier Chopin] Thank you. Two last questions before I leave the floor to my colleague. After the Snowden disclosure of all the secret information coming from secret agencies in the US, people asked for a new notion of digital sovereignty in Europe. There was a push for that concept and a way to securitize personal data in Europe, legally and technically maybe stronger than it was or it is possibly in the US. How did your organizations react to that notion? Was that taken into account in the development of your technologies and services you provided? And the final question: are you worried that it could lead to some kind of new economic protectionism if we enter into the notion of digital sovereignties around the world? I know it's a complex question...

[1:25'58 - Gail Kent] I think that one thing Snowden certainly brought to light was the importance of protecting your data. It's something that is important to us anyway but the idea that any government can be trying to gain access to, I think it has been really focused by Snowden. One thing that is absolutely clear to us increasingly as there are a lot of debates around access to data around the world and you see numbers of different countries, from Russia through France, UK, South Africa, Uganda... All passing different types of surveillance laws that we cannot just rely on the rule of law to protect our data. So that has to be done through using the very best technology - and we haven't talked about encryption yet but it is a really key part of that because as we all said trust is exactly what we are about, and showing our users that they can absolutely trust us with their data. For us it does not matter where you are in the world, we should provide you with exactly the same service. It doesn't matter if you are in the EU, the US or subsaharan Africa, we should keep your data at the same level of security, but we should also enable you to access quickly and efficiently.

[1:27'32] So for us it's not about where the data is, it's about how we can protect and enable people to gain access to it. We also understand that for some people or companies, knowing that their data is in jurisdiction at a level of confer (?), that is not the way that the Facebook model works, we are about connecting people and making sure you've got access to data. So one of our concerns is that you do end up, through a misplaced surveillance policy, looking at data localization model which would undoubtedly have an impact on economic benefits. There are number of countries (Russia the most obvious one) that are really pushing for that at the moment. We've been mistaken if we think that's only being done for security reasons, I think there is an economic driver behind that as well.

[1:28'36 - Acadia Senese] I think that what we call data localization efforts are the pendulum swinging in the complete opposite direction as where we think it should land post Snowden revelations. Data localization arguments, such as if you keep the data in a country, in a specific jurisdiction for example, in the context of the Snowden revelations, is outside the reach of US surveillance. But that's actually a misguided understanding of how US surveillance laws work: to put data outside the US is in some ways losing the restrictions on US government's ability to get that data - or any other government's ability to get that data.

[1:29'22] So data localization is not the answer to the security of the data. That comes with tools like encryption, with users understanding how the data works and certainly for Google and other companies that offer the services it offers in a way that is fast and efficient and reliable is to do so in a way where the data is free flowing. That is why, and we'll talk about I think in the second half of the panel, most of the advocacy work we're doing in terms of legislative updates, the touchstone for the reform is not the location of the data but instead the location of the user. And that's the user location that should drive the protections in the law and should dictate which law applies to the handling of that data.

[1:30'16 - Marc Mossé] It's a very difficult question in fact. But I would say sovereignty means two things. It means a lot, but at least two things: first, it's the ability for the citizens to choose their government and [second] the role of the state is to protect its citizens. This is what sovereignty means, in more than a nutshell, in very few words. So if you go back to the topic of today, I would say the question is not about border. Sure, sovereignty is very important, we should not underestimate its importance. It resonates a lot to the citizens and even with technology, with internet, with the clouds, the Artificial Intelligence, sovereignty is still a cornerstone of the relationships between the states and between citizens. However, it doesn't mean protectionism. It means, or it goes back to the question "how do we protect the most efficiently the rights of the citizens? And as it has been said, the question is more how we can protect the data wherever they are rather than to force the companies to locate the data in every country. It's really important.

[1:31'45] If you look at Microsoft's data centers in Europe, in the Netherlands, in Ireland, in France, in Germany, in other countries at the same time we are totally in favor of free flow of data because it's part of how we can build a very dynamic and healthy ecosystem with the internet. So it's a balance between all these aspects but at the end of the day sovereignty should go back to one crucial point which how to protect the rights of the citizens. This is really the key aspect of this.

[1:32'30 Maud Sacquet] Digital sovereignty is, well, a very complicated concept. I think, again as a trade association, our mission statement is to advocate for open market, open networks and free competition. So, by default I would say protectionism or sovereignty is not something I would stand for. One example is we know that Europe wants to be a leader in privacy regulation and so impose its sovereignty around the globe on privacy. Again, I am not a specialist on that matter but I do not believe that there are many countries that have actually implemented similar privacy regulation as to what Europe has developed. So that is perhaps something the EU should think about.

[1:33'19] More specifically on data localization, that has been an important topic of debate in Brussels. The Commission published mid-September a proposal on free flow of data, which is the idea of free flow of non-personal data within the EU to try to fight against those calls of data localization. One example, which we use quite often is that in Germany actually, per law a company can't store accounting data outside Germany. What's the reason? Why can't you store them in a server in Denmark for example? That's the kind of trend that we see more and more in many countries and that this proposal tries to address so that we can have free flow of data, non personal data, that could then be organized in a way that makes sense and that is more efficient, a safer way that a company can offer to its customers. That why I think we would not go for [in favor of] sovereignty.

[1:34'29 - Marc Mossé] I want to react to your point because beyond this discussion on the digital sovereignty which is, somehow, a physical question, which is not only the relationship between the private sector and the government, it's also the relationship between each of us - the citizens - and the technology, which is the very old debate on whether the technology will dominate the human. The real question of digital sovereignty is this one and it means that we absolutely need to give to each of us the capacity to control the technology. This is really crucial and having the government controlling the technology will not help on this question of digital sovereignty. The same with the companies of the IT sector. You made the point on education earlier this afternoon, and I think this is one of the key point. Education is really important because we are talking about a lot of questions: the rule of law, the US law, the European law... at the end of the day we have to be conscious that it's a question of education, how people will be able to control the technology, to understand what is at stake with the use of technology. If we don't go this way and invest in education, on how people can understand and manage the technology, we can do a lot on the legal side / framework but we'll miss one of the important point, which is really about the core of sovereignty, which is how people can control their environment.

[1:36'18 - Olivier Chopin]. Thank you. With that vertiginous perspective I will now leave the floor to Félix Tréguer, my colleague, who will act as a discussant for this panel and ask you some extra questions and come back to different dimensions you mentioned.

[1:36'40 - Félix Tréguer] Just a few points, I'll try not to be too long because we want to save room for the discussion. One is to thank you for this very transparent discussion, it's very interesting and were grateful to have all of these very expert insights on surveillance and controversies around privacy in the digital age. Although the topic of the discussion was a bit broader, because we talked about security challenges we focused so far at least on surveillance. My first question is actually to complement the various topics that we have addressed so far before going back to what you said.

[1:37'26] About the challenges in your relationship with governments, because I think that in the past years you've been navigating in ambivalent and contradictory environment or context in that respect because on the one hand you have seen greater demand for privacy rights and transparency and very dense and tense legal debates and on the other we've seen terrorist attacks and security policies creating a lot a pressure on your companies to cooperate with law-enforcement agencies. So, what are the biggest changes in the way you communicate and interact with public authorities and in particular law enforcement authorities? I remember, a few weeks after the Charlie Hebdo attacks in

2015, French minister Bernard Cazeneuve, Interior Ministry at the time, went to the Silicon Valley and discussed with some of the executives of your companies and maybe you could talk a little bit about this process and how you interacted with policy-makers in that respect.

[1:38'44] Then, to go back to some of the things you said, it's interesting that you've mentioned – and we will talk about encryption in the next part of the discussion – but you talk about technological fixes and encryption in particular as the first reaction of your companies to the Snowden disclosures and Acadia said these efforts were already under way at Google at the time, that those disclosures only accelerated that process... I am still wondering: the web 2.0 concept was introduced in the mid 2000s, then it would become the cloud and the idea that Internet users could defer the protection and the handling of their data to online service providers and one of the marketing arguments in the second half of the 2000s was the fact that these companies were better suited than average users to protect the security of the data. My question was why did it take so long, until the Snowden disclosures, for relatively basic encryption measures to be deployed on your products and, maybe that's not the case but I would be very interested in having your intake on why did internet users had to wait until 2013 to have SSL encryption for instance on some very widely used online services.

[1:40'20] Then, one last point, or maybe two. One would be the ability of your companies to resist in engaging this debate on surveillance in a way that, maybe... resisting some of the proposals made by policy-makers and people coming from law-enforcement agencies and in this respect I think there is one interesting example and I just want to talk about it and maybe have your feedback and impression on it: it's the case of Yahoo! Because Yahoo! was one of the last... you know, there was this very famous slide about the PRISM program, where you have the dates at which different companies started engaging in the PRISM program, which is, basically, data request coming from Intelligence, the FBI and the NSA (or the FBI I think) to Internet companies. Yahoo! was said to have resisted the participation to the PRISM program and was even threatened apparently by the FBI to be fined 250,000 dollars a day if they did not comply. I was sort of puzzled by this and I was wondering whether the explanation for that resistance at the time was the fact that Yahoo! had suffered what was then probably the biggest scandal ever for a giant company, which was the Shi Tao request in China in 2005 where Yahoo! complied with an order from Chinese authorities to release data on a Chinese dissident and there was a big controversy in the US and there were public hearings in the US Congress where the leaders of Yahoo! were summoned by Congressmen to plead for forgiveness to the family of Shi Tao, they were called moral pygmies, something quite violent for the leaders of this company.

[1:42'23] So I was wondering whether that scandal maybe prompted Yahoo! to devise internal procedures that would allow them to maybe... something that would explain why their participation to the PRISM program was delayed for some years. But at the same time in the post-Snowden context we see Yahoo! [cooperating]... last year the press agency Reuters publish a report saying that Yahoo! had been served with an order to install a scanning device on US-based servers to scan the e-mails of Yahoo! users and apparently the chief technology officer of the company was not even aware of this order to which other executives complied, the board of the company apparently. So that also begs the question of the evolution in context and the fact that the company might be able and willing to resist to illegitimate practices or things that would fall out outside of the rule of law or such a definition of it and why in some other contexts a few years later they would not. So my question would be whether the Snowden scandal led to changes in the way, maybe within your companies, you might handle these... I don't know, something similar to whistleblower protection, internal to your companies? Are there things that were devised and that would allow the legal team and people working on privacy issues to talk more with engineers? Have there been some changes internally since 2013?

[1:44'20] The last question, also going back to the issue of differences between countries and the debate around data localization is the fact that we saw in Europe very harsh language coming from leading politicians against your companies. I remember in France in 2013 there was a first attempt at legalizing access to metadata and I remember a minister pushing very strongly against the criticisms of NGOs saying that users gave away their data to private companies and they shouldn't be worried about the state because at least there is a sort of democratic control over the state and really using Internet Service Providers as a scapegoat in a way, at least something that would justify the practice of the French state in terms of surveillance. At the same time I remember also that then president Obama talked about data protection in Europe as a form of economic protectionism, so what do you make of these discourses that sort of, on the one hand, you see European politicians being very critical of US companies and on the other, that's probably a separate question, about the way privacy is handled in Europe, and you underlined the fact that we make a lot about the differences and the fact that privacy is well protected in Europe whereas it is not in the US, and that might not be true. Do you think that sometimes data protection is used by European authorities as a way of escaping a debate on their own practices and also a way of protecting European companies with respects of some of your competitors on digital market?

[1:46'45 – Acadia Senese] I will start with your very first question and we'll go from there. I think you asked how do we navigate our relationship with the government post Snowden. I think I can illustrate that for you just by describing you how an average day in my life looks like because on one hand in any single given day I can be advising Google to disclose data to assist in emergency like terrorist attack and an hour later I can be drafting a brief to be filed in Court to

sue the government about being able to notify customers about the existence of a request. So I think we can be both advocating for a reform and pushing the envelope about how the law can be improved while at the same time being good stewards of the data recognizing real threats to the society and doing our part where the law allows it, to disclose for example data where to do so over an emergency. So it's not an incongruent thought to think that we can be both doing our part to protect but also doing our part to advocate for privacy and security. So I do – it's a very common day for me – on one hand I am fighting the government and I have very heated phone calls with the government official about a demand that they are making that Google thinks is unreasonable and inappropriate and on the other hand I might have another phone call from another government official who needs an information because there's an imminent threat in Paris for example. So that's very common for me and I think that dynamic is very good because companies can come to the floor and say "look what we are doing when there are threats". I think all of us have emergency disclosures processes that we staff 24 hours a day, every day of the week, every day of the year, where we are responding to emergencies around the world, no matter the country and on the other hand litigating and pushing for legislative reform. These two things actually pair very well together to say the companies are in a unique spot, where we have a vantage point where we see conflicting laws and are trying to navigate through those and have solutions or suggest a solution in a way that moves forward. So that's the first question, I forgot what the second one was but I'll appoint [?]

[1:49'25 – Marc Mossé] As you have just said, we have the process to answer for emergency calls and if I remember the Charlie Hebdo attack, we were asked by the French government to provide some information. We have been able to provide the data in 45 minutes while the terrorists were still active, and it has been done according to the US law in case of emergency when people could be killed or there is a risk for the life of people you can give access to data in certain circumstances we have been able to provide this data in 45 minutes so there is an efficient way to collaborate and at the same time to respect the due process of law.

[1:50'24] When the Bataclan attack started I was at home and my older son came to me and said "something is happening, I don't know what". I turned on the TV and I looked at the events and I called my colleagues, well, in fact at the highest level of the company and I said "something is happening in Paris, I don't know what, it could be extremely serious and we have to be ready to answer the questions that could come from the law enforcement department". I know that you have done exactly the same in your respective company. We have been able to provide information in no more than 90 minutes during this attack. So there is way to collaborate in respect of the law and it's important to remind it because, again, I do not see any opposition between public safety and privacy, and it's not new because of technology. We had to solve this question for years and if you go through the jurisprudence of the Conseil Constitutionnel or even the Conseil d'Etat, the Court has always tried to find a right balance between this fundamental right. There is no hierarchy in the fundamental rights framework, they are at the same level and we have to find the right balance between this. The question with the technology is that the principles are not new, the values are stake are not new but the way they can be impacted is new. We have to think collectively on how to find this balance in this new era and how we can modernize a law in ways that we can apply these principles in an efficient way.

[1:52'34] I remember the second question, you mentioned GDPR (General Data Protection Regulation): I don't know if we have a consensus here, maybe not on this very point, but I tend to think this is now one of the standards for the world and we have to agree on this. It's very important because, again, we have to consider this regulation on privacy as a starting point to build this bridge I mentioned earlier between our countries. What has been built through the GDPR is something that really puts privacy on the top of consideration and it's something that could help us to build this trust I mentioned at the beginning of my intervention. Even for the US it will be an important step that it could benefit from, in order to build something that could help a trustworthy computing era. But I don't remember the third question.

[1:53'52 – Gail Kent] The question I remember – you had about hundreds in there – was about how our relationship matured and changed with governments and how has our responds to security matured. I don't think it has changed but both have matured. If you look at four years, at the age of the technology computing it's a huge amount of time. It's a third of Facebook life, so the importance of data protection has always been there but, as with every single technology company, we know that there have been developments that have enabled us... I think we're going to talk about encryption next, but I think we are always at the forefront of those technological and policy discussions so we have been putting even more emphasis on that, just as you have seen around the world, cybercriminals becoming better and better so we know that we have to do even more in order to protect ourselves. I don't think that was a result of Snowden, that was already in place, but it has undoubtedly changed and developed just as I don't think that our relationship with governments in it [has?] this sort of complexity that Marc and Acadia have talked about has necessarily changed, I think that it is just sort of managing that complexity on both sides has matured, so I think governments – if I put myself back of my law enforcement hat on – the relationship with law enforcement authorities is a very straightforward one, particularly in countries where the main landline providers had once been owned and run by the government, you know, it's a very straightforward relationship.

[1:55'55] If you look at the companies whose origin is in California that's a completely different mentality. One of the things that really hit me when I first entered it in 2013 was just how true it is to the idea of California being at the frontier and feeling so far away from government, and this belief that you can do anything, that is something that is just

so different from a civil service mentality. Therefore, by default there is a very different relationship anyway. If you had asked any of my colleagues in 2013 if there is any place in Facebook for terrorists, they would have given you exactly the same answer as I give you today, in that there is no place, as in any of our companies, there is zero tolerance. What has changed is that we need to be talking about this, to be overt about it, particularly after Snowden and to be very candid. There was a real concern talking about anything you were doing that was stopping something the government also wanted to stop would be misinterpreted, as a worker in the government it was I think naïve that we understand that we need to talk exactly about what we do to keep all sorts of bad actors of our platforms and also an understanding of the fact that we just talked about how we use technology to do that and being incredibly transparent in doing that.

[1:57'42] Other ways in which our relationship has developed with governments is through things as, you talked about the Bataclan, aside from providing data, how can we help? The Bataclan was the first time we turned on the Facebook safety check as the result of a man-made incident as opposed to natural disasters. I know that was something that the French government has talked us about before we turned it on, it was agreed it was a very positive thing to do and hopefully was helpful. The other thing that changed since Snowden in terms of relationships with the government is what we are all here talking about: the need to get some more systematic framework, that they can't just sort of be ad hoc, we need to be working on what does good look like, what's the framework for whether it's content, removal, whether it's about alerting governments about terrorist content or whether about providing data on an international level. That's another sure sign [?!] of the maturity of the companies.

[1:59'00 – Maud Sacquet] Perhaps I can take the last two questions I noted. One of the questions was: were you speaking hard towards this proposal from policymakers and you mentioned Yahoo quite often in that example. I was not involved in any of those issues at Yahoo! at the time when I was working there. Why was Yahoo! the last one to comply? With this issue, I have no idea, I think the fact that we knew now [?!] that Yahoo! challenged some amendments in 2007 in front of a Court might explain that delay and as far as I know all the proceedings are now available online, so that quite could be an idea. I know as well that following that situation in China, Yahoo! was the first company to implement a program that was a Human Rights program, so you had a department within the company where you would have called some people that were hired to review a lot of the policy decisions on data, on surveillance, some on advertising, depending on the exact scope, to think about all those issues from a Human Rights angle in a systematic way. That can perhaps explain some of the things you mentioned but that's mostly really guess from me as to why companies reacted differently. Yahoo was the oldest Internet company at the time, so perhaps went through a couple of issues first that the others experimented perhaps at a later time. That was the point I had on Yahoo!.

[2:00'40] How to resist proposal from policy-makers more on a broad perspective? For me, it's all the work you do as a lobbyist. As an industry representative, it's how you convey publicly your opposition to the proposals that are being made by the government and explain, as an industry, why this is relevant or less relevant, or why they go in the wrong direction or in a slightly better direction. I think that's the entire purpose of the work and you do that by talking with company to understand the product and the exact position and then you try to finalize and to mount campaigns and also simply persuade governments because most of the time people are not experts on the issue we work on every day and not aware of the some of the issues that are actually raising, and that's the virtue of just talking with everybody just to try to have everybody on the same level of understanding. Actually it's only how you try to do that.

[2:01'52] The last point that I remember you mentioning was about a kind of state control, company control and the way a European politician would criticize US companies to try to avoid facing some of the issues that they have to deal with nationally. This is where as a trade association I have a bit more freedom to give my opinion than a company on that one but this is one of the huge debate that we're having in Brussels right now. The European Commission has launched, about three years ago now, what we call the digital single market, so it's a broad area of reforms in every direction and tech issue we can think of. We've been bombarded with this proposal in every possible way. Let's just say very simply that the tech industry is extremely critical of most of this proposal. I think perhaps there is merely one or two I would think of which I could agree with, more or less. Instead of creating a digital single market, you are actually going backwards on many of those issues. Because of that, most of the narrative today in Brussels is the Europeans vs. the US companies, all of that is forged to try to trap a few American companies and it won't do anything to enable European companies to grow within the European market.

[2:03'19] Is that true or not, publicly all of them [Commission officials?] will say “no it's not the case, it's not protectionism, we are not going after US companies, it's for everybody”, if it's true in practice, I would say that at least there is a part of truth in that narrative.

[2:03'35 – Olivier Chopin] Thank you very much to all of you. So we have some time for a few questions from the audience, so please raise your hands to ask your question.

[2:03'54 - Amish]. Thank you for this very good talk, my name is Amish. It's definitely true that all of you to some extent are in the same boat, navigating a quite difficult line between cooperation with the government and a duty to your audiences and towards the citizens. I want to ask you whether or not there's a kind of understanding in the field that

you're operating that a relationship with no cooperation may eventually lead to a relationship or coercion. And perhaps at some point, do you have an understanding that if you were to give ground and have a relationship of cooperation, it's in order to avoid or prevent more of a relationship of coercion? My main example, thinking about that kind of happening would be that earlier in the UK we had an attack outside of our Parliament and it was very big on the newspapers calling the killer the "WhatsApp killer", because of two-way encryption, meaning that it was for a society's security that perhaps it could lead to forceful move against WhatsApp. After this, as for a relationship with the government is sort of more established, that it becomes a sort of normalization with this kind of relationship that expands over time, particularly with the use of big data... Big data is so vast, unimaginably vast, that sometimes you don't really know what you are looking for in the data intel you have access to and it even leads to some critics of big data who worry about privatization of big data because you don't necessarily know what you are looking for and the government does not necessarily know what to ask for until they have access, until they can apply filters and can really dive into it. The final point I really wanted to ask is because of this sort of privatization of big data, that hasn't really been discussed today, until the same extent, is on the other side, the issue of trust with the consumers and it's a second front where I know that Uber has had a big PR problem with the relationship with the consumers and it becomes sort of creepy because you've had a privatization of big data with the rise of experimental rationalities with behavioral economics, which means that you've also got another front of trust between what the company itself does with this big data. Thank you.

[Comments by Didier Bigo about having all the questions, then the answers and finally a well-deserved pause]

[2:07'08 – unnamed person] I am just interested in an answer to the Yahoo! question from you three because it puzzles me also: how come that it was only Yahoo! who was in this legal debate in the US and the other big data actors weren't. So somehow Yahoo! was facing this problem and the others just were agreeing... Was there also this big demand for data for the other companies? The second question I have concerns a little bit the boundaries of data provision, so rule of law was somehow framed by Marc as a boundary where you provide data but now in France we see that with the state of exception some rule of law gets overcome, like there are problems with the rule of law in France at the moment I would say. How do a Tech company deal with it? I just take France as an example but you could name thousands of examples I guess in countries... Is there a Human Rights or moral guideline for you for providing data to governments?

[2:08'48 – unnamed person] Thank you. I have two specific questions. The first one is about the Privacy Shield. One of the consequences of the Snowden revelations was the invalidation of the Safe Harbor and then the adoption of the Privacy Shield. Currently this agreement is under review, well the adequacy decision is under review, I would like to have your position on the implementation of this Privacy Shield and for instance some comments on the functioning of the ombudsperson mechanism. The other question is about some current negotiation with regard to the access to e-evidence at the European level. We eluded it at some point, I would like to have your comments about the position of your respective companies with regard to access to e-evidence for public authorities in the context of criminal proceedings and how it can be compatible with your stance with regard to strong encryption, end-to-end encryption for instance. Thank you.

[2:09'55 – Olivier Chopin] Thank you very much. As this question will be addressed specifically in the second round table I think maybe you can answer to the first two questions.

[2:10'13 – Gail Kent] If I can draw a theme between, you mentioned your first question is about coercion, around the rule of law and also is relevant to the e-evidence part. Facebook certainly feels that there are cases in which we absolutely should be providing data. It's not that we believe that we should never provide data to government. If you are thinking about domestic violence cases, terrorist cases, rapes, murders... there are a lot of cases where governments, to Marc's point, are protecting the citizens and we're all safer because they're doing that. In terms of sort of what there is [??] we have a three-pronged approach to when we believe we should be answering those requests for data, and I know for being in various panels with Microsoft and Google that the same is true for them as well. The first is that we have to... whether it is a conflict of law - we haven't talked a lot about conflict of law today but it's relevant I think to the question about the rule of law: which laws do you apply? As a US company we have to comply with US law and often what you find is that there is a conflict of laws. So US does not allow us to provide content outside of US jurisdiction and that's one of the issues being debated in Congress at the moment. That means that if any other country is asking us for content – I'm talking about when we have the content, so not WhatsApp, where we do not have and never have the content – we cannot provide that unless the US legal processes follows up. It basically means mutual legal assistance treaty. But we do have basic subscriber information and in some cases additional metadata.

[2:12'13] So the three-pronged approach that we follow when it comes to when we should provide information is 1) we need to have the legal process of the country that is requesting, the jurisdiction cannot just ask us, they have to follow their own legal process, 2) that user has to be within the jurisdiction of that country and 3) the request has to be human rights compliant. So that means it cannot be a request pretending to be murder when it's actually for political activism. Speech issues are particularly problematic but we look into every single request to make sure that we are complying with all of that. And that's very much the debate in a lot more details than we've been having with the Commission on

e-evidence – as you said, we are going to talk more about that. But that's our way in terms of trying to do with the conflicts of law.

[2:12'20] In terms of coercion, what we found so far... and we can talk about what's happened in the UK government, a particular case of interest of mine, where it comes down to trying to explain to the UK government exactly what data we do have and what we can comply and what we can't provide. This doesn't break end-to-end encryption, it doesn't require us to retain data that we have got no business need to. And not only explaining what that does look like in reality but explaining to them what we think the downside of them changing our business model, not just for what it causes to ourselves but for the overall ecosystem. I will talk at length about encryption but it's about trying to have that conversation so we never get to the point where they think they have to force us in Court to do something, which we think will severely undermine the security of our users but also the security of the ecosystem as a whole.

[2:14'45 – Olivier Chopin] Thank you so much. In the name of Didier and everyone here, a warm thank you for your candid answers and your dialogue, for talking about those tremendous issues today. Thank you very much.

[APPLAUSE]

Didier Bigo specifies that some face-to-face discussion can take place during this long break but after the coffee.

[2:46'20 - Alex Macleod, chair of the second roundtable): Just one thing before we start: I come from the perspective that Didier said we were not coming from, which is security studies and IR theory, which does not mean that I don't think that we now have to adapt because this is the great thing I think about this [...] second roundtable, is bringing a stack to reality.

[2:47'11] One of the things I tried to do myself is teaching. I am teaching a course on the cinema and security, which go from Cocoon, to Fourteen Days to Snowden, which, believe me, is an interesting way of looking at it. So I will not say anymore about that, because you are here to listen to other people.

[2:47'34] This second part of the roundtable is about the legal debates. And as you know, there has been a lot of questions raised about the legality of the interventions of the various companies, of the way governments handle it, of the way legal systems handle these questions very differently, the fact that [these governments] have tried to pass through what we call Mutual Legal Assistance Treaties to try and bring some sort of order into the whole situation. So first of all, a question which I've been asked to pose which is on approaches to surveillance reform. As you know, in both the US and the UK, your companies have been involved in legislative reforms aimed at protecting privacy, especially the question of encryption, and other things we will come to in a few minutes. The first question is to Acadia about the changes in the Patriot Act in 2015 and whether you think it achieves better protection for the privacy of US persons. What are the perspectives for non-US persons, and in particular the FISA Act Section 702, on which are based the NSA's broadest capacities, such as the programme Upstream?

[2:49'06 - Acadia Senese] Just to clarify, which changes to the Patriot Act are you referring to?

[2:49'11 - Alex Macleod] I've got absolutely no idea. I have just been given these questions.

[2:49'14 - Acadia Senese] So whoever asked the question so we're clear on what we're discussing.

[2:49'18 - Alex Macleod] Anyone is clear on that? I am sorry, I didn't write the question.

[2:49'25 - Félix Tréguer] It was referring to the fact that the NSA and the FBI have deferred the retention of data to private companies.

[2:49'34 - Acadia Senese] Okay so the Patriot Act is up for renewal again this year...

[2:49'43 - Félix Tréguer] It's about the USA Freedom Act of June 2015 that we talked about earlier.

[2:49'50 - Acadia Senese] Let me try to get to a broad answer here. Part of the Patriot Act authorizes the US government through FISA requests - which are judicially-ordered requests, although by special courts in the United States - to authorize the US government to seize electronic communications of non-US citizens. As part of the collection, or as part of the production in response to FISA requests, the content of communications belonging to US citizens might be included in those productions. One of the things currently up for debate, in the US, is whether protections will be afforded to the contents of the communications belonging to US citizens. At the moment, a production made pursuant to a FISA [request] does not also require the government to obtain a US search warrant in order to also seize that data.

[2:50'54] So there is a debate in the US now ongoing about even if the government can seize content of communications - again judicially authorized by a special court - for a non US-citizen, can also as a corollary keep the content of communications that belongs to US citizens. That's now being debated, Google and others advocating for the need for a warrant for that other types of data as well. We've seen improvements in the law, that I talked about earlier, including the reporting of the number of requests that companies receive, both national security letters and FISA. So, there are some improvements, although I think it will be all up for debate what we see come with this Congress at the end of this year.

[2:51'44 - Alex Macleod] Thank you very much. The second question will be to Marc. It's about Silicon Valley companies working in France. They seem to be less vocal regarding surveillance laws adopted in France in 2015 to legal surveillance capacities that had previously been adopted with very little legal basis. Is it true or do you believe that it is more difficult for these Silicon Valley companies to intervene in France?

[2:52'19 - Marc Mossé] I could say that we are not in Silicon Valley. We are from the North of the West Coast. I'm sorry I will answer for you, from the Silicon Valley. On this, I can say for Microsoft, we have been involved in discussions with the government at the time. We have been heard in the National Assembly by the rapporteur. We have made our point. And as I mentioned earlier at the beginning of the afternoon, when the Bill was under scrutiny by the Conseil Constitutionnel (the kind of Supreme Court in France, although it is fact much more complex in France, where we have three supreme courts), the entire IT industry, and beyond the IT industry the business ecosystem, lodged an intervention to the Conseil Constitutionnel to make its point. Of course with the clear view that we need to fight terrorism - there is no discussion, it's a no-brainer, of course - at the same time it should be done in full compliance with [higher legal] principles. It was in a nutshell the sense of this memo. This memo is still available on the Web, so you can easily find it and read it. What was interesting in this memo if I may - it's another way to answer your question - is that as part of the introduction we had several paragraphs to say: "this topic should not be fixed only in France. This question requires a transnational cooperation, because the Internet is not a national question, it's an international question".

[2:54'35] And we, when I say we, the entire industry was calling for a set of principles that could be part of the constitutional heritage of our nation. I'm not fully sure that the Conseil Constitutionnel went on this path with its decision on the surveillance bill, but we have seen after on different cases brought to the court by La Quadrature du Net and other NGOs that the Conseil Constitutionnel, like the Conseil d'État, have made some moves opening the door to further evolutions. So to answer on this question, I would say yes we are developing our point to the government in a very transparent way. When we have to say something, we say it in a transparent way. And yes, the French industry - not the Silicon Valley in France but the French industry, including I would say companies such as Dassault System or others that are member of this association - brought this amicus curiae, this intervention, to raise some points. Again, not [against the idea] to fight terrorism - again we are totally aligned with this idea to fight terrorism - but to find the right balance between fundamental rights and how to work in a way [through which] you still protect public safety and you still protect privacy and fundamental rights. It's really important to keep in mind that we need a balance between both dimensions.

[2:56'21 - Alex Macleod] Thank you. This time it's for Gail, and it's about Great Britain and the Investigatory Powers Bill in the UK. What has been the attitude and the way of evaluating on the part of Facebook and other Internet companies over the debate on the Investigatory Powers Bill?

[2:56'45 - Gail Kent] I've said in the first panel: one of the things that was very positive about the Investigatory Powers Bill was, I think as the result of the Snowden revelations, there was an understanding that none of this could be done in secret anymore. And I think that that in itself was huge step. I will bore you all a little bit about my own background: I joined, over twenty years ago, what was then the National Crime Intelligence Service, then Serious Organised Crime Agency and then the National Crime Agency. And all of these agencies had the sole UK non-terrorist responsibility for interceptions of communications. Which means that it was the only agency that can intercept telephones or other data on behalf of UK police forces for non-terrorist related incidents.

[2:57'46] One of the jobs I did was running the suite that carried out the interceptions. And this is relevant because I had people in that suite whose funerals I have been to - not related to working for me, they died of old age - who never told their partners what they did for a living. So they were involved in [countering] drug trafficking organizations, or people trafficking, or money laundering, or serious murders or corruptions cases. These are people who spent their lives protecting UK nationals from terrible crimes, and they never revealed what they did to their partners. So that amount of secrecy was embread to people and so we all know about these posters of the war with "loose lips costing lives": It was an incredibly secret environment. And I think that, to have gone from that - and for this I think Snowden definitely does get credit - to get to the point where we are now talking more is a fantastic step forward, and I think the Investigatory Powers Act really took that on front and center.

[2:59'09] It had three reviews. One by David Anderson QC - who was Independent Reviewer of Terrorism Legislation

at the time - and it's written in an incredibly witty tone. Anyone who is really interested in this area I would advise you to read it<sup>179</sup>, or at least its recommendations and its summary, because it goes into, probably better than anything else I've read, the different perspectives of the stakeholders. Because it's something it took very seriously, he was speaking to everyone he could to understand [...] the perspectives of the civil society community, of the intelligence community, of the police community, of Internet companies, of politicians in terms of what they were trying to achieve on surveillance reform.

[2:58'58] Secondly we had, the Royal United Service Institute had a panel of eminent - probably a very sort of French model in fact - public intellectuals, again looking and debating this: they had ethicists, they had philosophers, law professors on it, they had previous heads of two intelligence agencies and senior police officers, again to grapple with these issues.

[3:00'28] That was the second review and the third review was the own UK Members of Parliament and Members of the House of Lords [from the] intelligence and security committees. They debated this as well. All of those three reviews went into what the legislation should look like. It was a very public review. I think that sort of process in itself was a very positive one. Whether we ended in exactly the right place is probably a different matter. But certainly as part of that, Facebook and the other companies and all the different stakeholders were asked to contribute publicly during review, and were able to have as many conversations as we wanted with people who were reviewing. So from that perspective it was very positive.

[3:01'24] The other part that ended up in the right place is the part on understanding conflicts of law. Understanding the impact that one country's legislation has on other people. I think that in itself was a second positive step: understanding that we're a global community we have to work together. I think the one part where undoubtedly the UK government failed and I think it could have done a little better is that the legislation is not necessarily any more transparent - though on this I am not an expert - than the previous legislation was. And that is a disappointment. And David Anderson himself has said that what one thing he wanted to achieve was that an informed reader could make sense of the law. And I think that isn't the case. And I worry that ambiguity doesn't benefit anyone because it allows people on both sides to over-interpret legislation. So we haven't got to encryption yet but it means that there is often over-interpretation of the what the law currently allows in terms of removing encryption protections. I certainly see some exaggeration in the press coverage about what the UK law allows you to do, and again it gets interpreted during the road of "the UK is removing encryption, we can do the same".

[3:02'54] But equally, and Marc said this at the start, that we have to look at what do we think about surveillance legislation: If that it is turned upon ourselves. I think that ambiguity can also mean that, are we 100% sure that the law enforcement officers and the judges, and the oversight commissioners who are interpreting that, are interpreting it in the way that it was written, and will they continue to do that in a five or ten years time? I know my previous colleagues and I believe they made the right decisions, but can I see that the law offers them that clear framework? I'm not 100% percent sure of it.

[3:03'38 - Alex Macleod] Thank you. And the question for Maud is about the EU Charter of Fundamental Rights. Would you agree with those that say that the surveillance activities of US-based law enforcement agencies is not always enough to respect the Charter? And the other question, which is closely connected, is: What is your view on the Privacy Shield as a way to protect those rights which we see are not so well protected when it's used by the US law enforcement?

[3:04'15 - Maud Sacquet] So on your first question, I've less worked on purely US legislation so my understanding is perhaps a bit more high-level. Is current US surveillance law respectful of the Charter of Fundamental Rights? I would have difficulty saying yes or no. What I know is that the adoption of the USA Freedom Act, while not perfect, and we recognized as an industry that it's not perfect, is still the first time that the US surveillance regime was reined in, at least somewhat, in the past few decades. And that is the first time that, we, we'll come for that, I would say, it's better oversight over new programs, it's not perfect, my understanding is that there are still some bulk collection of some foreign data, which we would of course like to see removed. We also think there could be better and potentially stronger oversight, but at least it's a first step in the right direction and this is something we should welcome and then continue to improve as much as possible.

[3:05'30] On your second question regarding the Privacy Shield, that's a very interesting issue: when the Privacy Shield [in fact she is probably referring to the Safe Harbor instead] was struck down by the European Court of Justice, actually stakeholders were currently negotiating to try to update the framework. What we ended up with was a text... first, we were happy that we ended up with something since it was important to have a framework to enable personal data transfer between Europe and the US. Without that it would have been a lot more complicated to operate. Again, it's not

---

179. [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/434399/IPR-Report-Web-Accessible1.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/434399/IPR-Report-Web-Accessible1.pdf)

perfect but we still think there has been an improvement between the two versions. In this new version we have the annual review of the Privacy Shield, [while] it wasn't the case of the Safe Harbor, but now we can potentially tweak the agreement every year in light of modifications of laws or what's happening and return of experience as well or development of new systems so it's a lot easier to do tweaks and try to adapt the framework as best as possible.

[3:06'48] We have also the ombudsperson who is there to review European complaints, that is also why it was important that the US adopted the Judicial Redress Act which also gives some guarantees to European citizens that they could challenge US federal agencies based on the data that these agencies would have. So I think broadly speaking on your two questions I would not say that both texts are perfect, certainly not, but it's the first improvement perhaps that we have seen on that field for a long time and that's something to encourage and to continue to talk with stakeholders to improve it as much as we can.

[3:07'30 - Alex Macleod] Thank you. I would like to follow up the question I have just asked because this is a much more general question that I think is very important: we sort of touched the first part of the roundtable, and that's the question of different legal systems and how you can really compensate for the differences between legal systems, work between them, how for example, for Europeans you get around the first and the fourth Amendments which of course have all sorts of restrictions, especially in the Fourth Amendment for what counts as evidence. I mean, if you are getting evidence which would be considered to be illegal according to the US and law enforcement agencies and especially the courts, it obviously does create problems for the agencies in Europe. So I think that's a first question I'd like to ask you is: How do you see the possibility of reconciling these legal systems... it has already been done through the so-called Mutual Legal Assistance Treaties but I am sure there is more to eat than that.

[3:08'43] Another question that I'd like is to come back to what Marc said earlier about the question of sovereignty. I think it was a fairly short definition of sovereignty but we are in an age where people claim that Internet was supposed to be global, etc. but what do you do (and that's something I would like to ask Acadia in particular) when certain very important countries like China say "we will not accept access to this type of information", especially for example on questions of Human Rights in China or Taiwan independence, I think those are questions which now the Chinese would not allow their own citizens to access and not even, if I've understood rightly, get to them through VPNs (apparently you can also control that). So there's a huge question there that sovereignty is being exercised in the first question that is the legal system, because each legal system is very different (the French one if different from the British one and the British from the American) and then, second, of course, is what you do when certain states say "this sort of information is not going to be available for our citizens, period". So what do you say to those who say "Oh, but we have the global internet"?

[3:10'14 - Acadia Senese] I'll take the first question first and I'll talk about what's going on in terms of removals. In terms of resolving conflicts of laws, Google is an American company so we are compelled to comply with US law but we're also a global company and that means that to the extent that we're permitted to do things under US law we do so. That for example means that we comply directly with French law enforcement requests that are served directly on Google and because US law permits Google to respond to those requests directly and provide non-content information we voluntarily do so.

[3:11'00] In parallel, we are working with other companies, NGOs, the governments to advocate for MLAT reform, and part and parcel of MLAT reform, that is reforming the system by which countries formally engage with one another. That is France, for example, formally engaging the United States to make a request on behalf of the country of France to US company. That system is broken in terms that it can't handle the volume of the requests that are coming through it. It is a manual process requiring human review and processing that we can't, as we say in the Valley, scale to a place that it needs to scale to.

[3:11'48] So in parallel we are working to update the Stored Communications Act, which is the US law that prohibits the disclosure of content to France, for example, and so all of these things need to happen together. Congress needs to update the Stored Communication Act to allow the disclosure of content to a non-US governmental entity, in parallel we need a framework that exist [?] either bilateral agreements between, say, US and France, that would allow France to come directly to the US [companies] or multilateral agreements which would contemplate multi-state membership, so long as those states meet basic Human Rights standards, that there is a due process of law and that there are privacy protections. Those multilateral frameworks based on the location of the user would then facilitate and enable this cross border data request in a way that's clear (there's a clear legal framework for it) and can meet the demand for those requests.

[3:13'00] About China, I am not a content-removal expert, I don't pretend to be one, so to the extent to which we are talking about censorship of content based on the country where a person resides, that is not my area of expertise. Companies handle disagreements with content censorship in various ways: one of the ways that it can be handled is by not doing business or offering certain services in certain countries because companies aren't willing to assume the obligations that come with offering a service in a particular jurisdiction. Another way that IT companies handle this is

by removing content and I think some others will probably speak to that as well but it varies by jurisdiction, it varies by companies it varies by what the business needs are and it varies by the demands are being asked by the posting jurisdiction.

[3:14'05 - Marc Mossé] Maybe I will talk a little bit about the cooperation between the governments and the conflict of law. I would love to spend a few minutes, maybe a few seconds, on the New York warrant case, which is a case I mentioned during the first roundtable. Just to explain the situation: it was a warrant issued under the SCA (Stored Communication Act) requesting that we provide content data from one of our customers, stored in our datacenters in Ireland. We declined to do so. Of course we had a strong disagreement with the US government about this, we didn't have the same reading of the SCA and we went to the Court, the second Circuit Court of Appeal of New York and in 2016, July 14th, we won this case. It was a little bit surprising for some but we won this case with two questions, and these questions are very important, because it was about the conflict of law but, beyond it, it was about privacy and sovereignty, the two questions at stake.

[3:15'43] After the decision of the Court of Appeal of New York, the government of the United States had the opportunity to stop, to maybe try to modify the legislation (the SCA) or to go to the Supreme Court. They have made the choice to go to the Supreme Court. And the Supreme Court, as you may know, can decide to take or not the case. And the Supreme Court will decide tomorrow or next Tuesday, October 16th, to take or not this case. If the Supreme Court decides to take the case [...], we will have this debate at the high level of the juridical system in the US and it's really a case that opens the debate on these different aspects.

[3:16'45] Again, on this case we are not against the investigation, it was not our position. It was not terrorism but it was about narcotraffic. We didn't [...] on the investigation. The question was really about the principle. The data were stored in Ireland, it means in Europe, and it was about privacy. If the Supreme Court takes the case, it will be an opportunity, not only for us to defend our position, but also for some maybe to intervene and to give their opinion. We mentioned the possibility for NGOs to be active on this kind of topics. As I mentioned earlier during the procedure before the Court of Appeal we have seen some NGOs lodging, filing an Amicus Brief, maybe some will do the same at the Supreme Court level. We could see as well other companies, of course, but we can see governments making their point which is not supporting Microsoft or not, which is really mainly about the principle.

[3:18'03] It would be interesting because we often talk about the question of building a bridge between the US and Europe, building an international framework, revising, modernizing the law in digital era and here we really have an opportunity, through this multi circular approach, to push this point of view. What should be modern law in digital era to both protect public safety and privacy? I don't know what the government will do, I don't know what the French government will do on this but they have the opportunity to make their point and to lodge an Amicus Brief. If I go a little bit further, beyond this New York warrant case, we have at the same moment the discussion in Europe (it was the last question just before the break): the e-evidence discussion.

[3:19'00] As you know, or if you don't know I will tell you, there is a discussion at the European level to build a sort of new framework still to access to e-evidence in a way which is compatible with both: public safety protection and privacy. Even between European governments it's not so easy. So the Commission is working on a regulation that could be issued on the coming months or year but it's extremely important because it will create this framework on having a possibility to access to data when an investigation requires it and protecting the rights of the citizens in a modern era.

[3:19'53] If I make a link between the two stories, the New York warrant case and the e-evidence regulation under discussion, you can see that there is some opportunity to build this bridge I mentioned earlier. Because if the Supreme Court takes the case and decides that the Court of Appeal was right, which means supporting the Microsoft position, it would mean that the US government will have to either modify its law or enter in discussion with other governments (why not the EU) to frame this international legal system. It would be even easier if at the same time the EU has a new framework, the e-evidence framework for cooperation between member states, one system, and this system could help to build this bridge with the US.

[3:21'05] I am drawing a sort of ideal scenario, of course, but it's really about what we have discussed during the first round table: how could we build this new legislation in the digital era? It's extremely concrete. And this is a way to not be trapped in this discussion opposing public safety and privacy. We don't have to oppose both. We have to work in a way that we find a right balance between two constitutional rights, two important principles, that citizens care about. And here, with the New York warrant case, if the Supreme Court decides to take it, and with the e-evidence discussion which is under way in Europe, we have two pieces of a puzzle that could help us to build this bridge, because, again, as I think, there is a worldwide constitutional heritage with the same values that we could really integrate in something that could build the future of internet.

[3:22'24 Gail Kent] So you started by asking how do you make these different laws match up and I do think we should not underestimate the difficulty of that. Surveillance laws are some of the oldest in the world. Most of them in Europe

were drafted in the 80's or 90's. Last week in India I was looking at their laws: 1885, they drafted the Telegraph Act. On top of this there is the fact that the laws are so old and need to be reformed for a digital era. You also have, you can put it on top of that, not just what the law says, because what I definitely learnt in this job is reading a law, even if you understand the language it does not actually tell you that much, you need to understand the culture that comes with it, the history of whether the law is even made for implementation or not because there are a lot of countries around the world where to pass a law is the same as having done something because there is nothing like being policy-maker, politician and proving that you've done something by passing a law, because you've done something but whether that ever get implemented can often be a different question altogether.

[3:23'44] I think all of that put together means that there is a layering of secrecy on top of it, it means that these are not laws that sort of naturally fit together and they were never meant to, because they are about national security so they are not part of harmonization of EU member states or anything that should be generally covered by any UN Convention in any sort of details, so it's a really really difficult area. Having said that, I completely agree with you that we are now at a critical point where we have to do something because the pressure on companies is great, but more importantly, the voice that we don't often think about, though we often think from a users and Human Rights perspective, we do not often think about the victims of crime and what it means when you try to do an investigation and you are not getting data that might help prove that somebody is innocent or might help get resolution for a victim of crime.

[3:24'55] All of this means that we absolutely have to do something and as Marc said there is the e-evidence project, it could for the first time in Europe come up with a framework that helps provide a structure for what good surveillance legislation looks like within member states. There is also the pressure for US reform, there is the Microsoft case and there is the "Internet and Jurisdiction" project, which is right here in France, which is looking at that from a much more global scale. But all of that will require countries to think about their legislations as well, because the two parts I see in terms of resolving this issue is building the bridge between how does France request information from the US - that's the agreement part of it - but it's also making sure that French legislation can be explicitly recognized as good legislation by the US. We see this in the US reform debate at the moment - if you are really interested in this it's worth watching the Congressional discussions around access for other countries to data that's held by US companies so it can give you a sense of how strongly Congress feels the responsibility, partly because of things such as the Yahoo case, to make sure that data isn't being given inappropriately to other countries. But US Congress certainly takes the responsibility of not just thinking that data could be handed over to anyone.

[3:26'40] So what does good surveillance legislation look like? I think that's going to be one of the very difficult bits of the e-evidence project is making sure that explicitly every member state have clear human rights safeguards. Every member state will argue that they already implicitly have a [good] legislation because of signing up to the European Convention of Human Rights but is that enough if it's not going to be explicit in here? I do not think it's going to be easy. Having said all of that, I am really surprised how far we've come in in four years. When I first started research in this, nobody was talking about it and there was what was called the MLAT problem and we just had to assume that it would be there forever.

[3:27'31] Now I feel that we've got reform in front of Congress, you've got a case that will possibly go to the Supreme Court which would mean that we would get an extra level of attention, the Commission is taking this very seriously, not just for the sake of us but because it believes it's a key part to solving part of the terrorism issues, and you also have countries like India and Brazil really pushing for this as well. So I think that if there's a time that we can manage to put all those different legislations together, that's now.

[3:28'09 - Maud Sacquet] There is not much I can add because I think everything has been perfectly covered. perhaps still a couple of points. First with one practical example. I remember being on the phone with a French police officer and explaining to him that I couldn't hand him any of the data because it was data this was data only available to the US companies, so he had to go through the MLAT process to be able to receive it. The answer I got was "OK, go to the US, no chance, case closed, request in the bin" I put on the phone. It's his decision obviously but I wouldn't have liked, as a private citizen, to see may case handled that way. I think that was the time I realized that what we did [indeed?] before was clearly necessary, especially for the MLAT process.

[3:29'08] From a policy perspective, again, nothing I can really add. What we are focused on as an institution both in Washington and Brussels is, indeed, reform of those processes. My colleagues in Washington are working on the International Communication Privacy Act where we think it still can be refined but it's an interesting area of progress in those issues. There is also discussion around bilateral agreements between the US and [some big?] countries such as the UK, again it's an interesting way to look at it but there's always questions about which country, which crimes, which data, how, etc.? It's an extremely complex issue to settle and so we are working on those issues.

[3:30'02] From a Brussels perspective there are two things that can be done by the industry broadly speaking: first, communicating with the European stakeholders, explaining to them what's happening in Washington, what is actually moving there and asking them to support the different efforts by the US government to try to improve the situation

because of more feedback, the most constructive discussion that we can have between Brussels and Washington on these issues is important, as the role as an industry that we can play. Then there is the own European process on e-evidence, where again we can contribute to working groups and trying to create that framework which is indeed necessary. We have to think of cooperation regarding data request between two European countries, a bit the same way we would think of it between France and the US: the German police authorities would have to go through the French authorities before the French authorities can hand over data requests to the company based in France. So then you as a company you have questions and you're trying to clarify the scope of the request or the scope of the investigation, then you call the French police officer who has absolutely no idea what that request is really about, he has to go to the German colleague to try to figure that out, with the language issue you can just imagine what's this look like. So even within Europe basically there is progress to be made and that's why the e-evidence program is so interesting right now and we welcome it. While we can see some issues, my understanding of the e-evidence framework right now is that the Commission is looking at many different options as to what exactly could be done and that the proposal should come out normally early next year at some point but that's really under discussion. So that might change.

[3:32'05 - Marc Mossé] Very quickly, because I do not want to be see too optimistic or jumping into wishful thinking, but I was reading a quote by Justice Breyer, a member of the Supreme Court, francophile and francophone. In his book "The Court and the world" that has been issued in 2015<sup>180</sup> - a very interesting book I recommend you to read, in addition to "Le Palais de Rêves" [mentioned earlier] - he says something which is very interesting: our world is increasingly interdependent and questions about overseas application of American law and how our Constitution should apply in the modern age cannot be avoided .

[3:32'58] Again, we are at a moment when we are crossing the path and sometimes there is some momentum like this where people can mobilize to try to draw the new framework. Honestly, not being too much optimistic here, I am seeing a lot of signs that maybe we'll go in a positive way for the fundamental rights.

[3:33'35 - Alex Macleod] This ought to be the last question but I think this is a very important one that has already been raised, which is the encryption question. It was raised of course by the San Bernardino attack and involved a company that is not present [today], Apple. It raised an extremely important question about how far states can go to demand that encryption should be handed over so the police could at least have access to what they consider to be possible vital information. Now I think all the companies and organizations involved on this panel have had at least something to say about it, so I would turn to you and say: how do you see it now?

[3:34'25 - Acadia Senese] So, the Apple-FBI unlock debate touched all our companies, it certainly touched Google. In that particular case it was framed as an encryption issue but actually it was really a file about really antiquated law. In the Apple-FBI case the government tried to use a law that was passed in the 1800's, called the All Writs Act and they tried to use that law which was basically a law that authorizes a court to issue an order if necessary to effectuate an already issued order by the court. So in this case the concept was that the court had issued a search warrant, and ancillary to the search warrant the court then issued an All Writs Act order to Apple requiring Apple to do something that it wouldn't otherwise do in the normal course of business. In the case of the San Bernardino matter, what was at issue there was that the order compelled Apple to write additional code that didn't already exist so that the government could gain access to the device.

[3:35'52] So the debate was not so much about encryption and what was regulated / not regulated did apply here, but rather could the government compel a company or third party to do something that it currently didn't have the capability to do and did not otherwise have a business need to do, when it otherwise wasn't connected with the crime at issue. So that was the debate there. Google brought in an Amicus there saying "no, you could not use the All Writs Act in that way" and the debate fizzled out because the government otherwise gained access to the phone, through other means, and didn't pursue the case any further in court and so with respect to providing access to phones that conversation has largely gotten away in the United States, and may be surfacing again, but there hasn't otherwise been a challenge to the All Writs Act.

[3:36'44] So with all of that sort of backdrop to Google's position with respect to encryption, which is "yes, companies should be able to encrypt their data and to give users the ability to encrypt their data and that should be a choice, that encryption should be there when it makes good business sense to do so, when it makes sense for the service, when it makes sense for the user. But otherwise it shouldn't be regulated, no. Of course, recognizing that there is no panacea for the real true legitimate concerns and needs of the government to be able to investigate crimes. But also, on the other end, the need to balance the true need for privacy and security in the data at issue. So I leave it there, I know others are trying to get at the end [?] but that was the framing of the San Bernardino debate.

[3:37'35 - Alex Macleod] I just want to be fair and let Maud intervene without having her thunder stolen by the others.

---

180. <https://www.nytimes.com/2015/09/20/books/review/stephen-breyers-the-court-and-the-world.html>

[3:37'42 - Maud Sacquet] That's a shame because that's actually the question I know the less about, so this time I cannot really say "Oh, I have nothing else to say". My Washington colleagues at the time that were on the San Bernardino case actually were quite vocal about [it]. As industry we think that end-to-end encryption is key but also was somehow the reaction of some of the privacy concerns that a lot of our users had. I think in that debate - of course the main debate is terrorism vs. privacy, most of the cases are terrorism, that comes first - it's actually some debate that was already existing in the 1990s (in my understanding) in the US as well when we started to think about encryption and third-party keys and all of those things. The debate was already there and the arguments from law enforcement and industry were actually the same already at the time.

[3:38'52] As industry position, it's very simple: we think encryption is good, we do not think that backdoors should be implemented... I mean, perhaps it could be a solution in some cases but if you look at all the damages that it would cause, we do not think, if you have to balance security and privacy, this is the concern that should win. Very simple because, if any criminal knows that these backdoors were implemented, they would simply use other services, less well-known services where companies potentially would not be as law-compliant as the main communication services that we use today. So we think it could actually damage law-enforcement activities there. Then, if you think broadly about trust, that we were talking about at the beginning, we are actually starting to regain trust, we have done a lot of efforts to maintain the trust of our users in tech services, and having, especially the US government implementing those backdoors, then all that work, all the transparency work that has been done would simply again fall apart.

[3:40'04] It could also have a chilling effect on the speech of dissidents for example, again using a lot of our services and knowing that encryption can protect them, especially in countries where the current regime is perhaps not as democratic as it should be. That's also a big concern, as industry, that we want to raise. In short, we know there are concerns but still think that in most cases privacy concern should perhaps take the lead, that law enforcement should often look at the many of the other options they have to actually solve the case. In many many cases, those cases were solved without really having potential access to that data, so that's something to take into consideration.

[3:40'57] Broadly speaking then in Europe the encryption debate has been raised quite a lot, more recently I think by letters from the French and German governments, all of this this summer if I am not wrong, saying that after the French and German elections the issue of encryption should be tackled at the European level, while at the same time we have a Commissioner, Ansip<sup>181</sup>, in Brussels, who has said very clearly that he is for encryption and doesn't want to see any backdoors implemented there. So that's the kind of political fight that we are starting to see at the Brussels level and that we follow very carefully and closely.

[3:41'39] To finish, my understanding as well is that there should be a Communication on encryption<sup>182</sup> at the end of the year...

[3:41'45 - Gail Kent] ... Maybe next week

[3:42'47 - Maud Sacquet] next week, perfect... We will be looking at it very closely when it's released.

[3:41'57 - Gail Kent] So obviously, as WhatsApp is one of our companies and WhatsApp is end-to-end encrypted, this is a debate that we have thought a lot about. It's also interesting coming from the law enforcement perspective. One of the frustrations - that had been my career for such a long time - I have when looking at this debate around the world is you very much see the same pattern: you see cybersecurity experts and people that are looking at data protection consistently emphasizing the importance of encryption and of increasing and getting better encryption particularly when we look at, I mean every week there is a different name that you can throw at it: Equifax (the breach of the moment)... We are witness to an increasing number of breaches to huge numbers of data. And we all know that encryption is key to protect access to data.

[3:43'00] You see cybersecurity experts and policy-makers emphasizing this, as you said, like Commissioner Ansip and then you will see, usually in the back of a terrorist attack, and understandably caused by frustration for not being able to gain access to a piece of data, whether that was the FBI not being able to get into the San Bernardino attacker's iPhone, you see a request by policy-makers coming from the law enforcement side for access to data. I think my biggest frustration is that it's very very rare for that debate to be looked at holistically and for encryption to be looked at [all around?].

[3:43'40] It is fortunate there is a debate and there'll be a Communication next week by the Commission, it's going to be as part of the terrorism package, which I think is totally unfortunate, and it's not part of the cyber security package although it was mentioned in the cyber security package but again it was put into one rather than the other. I think they

---

181. [https://ec.europa.eu/commission/commissioners/2014-2019/ansip\\_en](https://ec.europa.eu/commission/commissioners/2014-2019/ansip_en)

182. [https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018\\_eleventh\\_progress\\_report\\_towards\\_an\\_effective\\_and\\_genuine\\_security\\_union\\_en.pdf](https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_eleventh_progress_report_towards_an_effective_and_genuine_security_union_en.pdf)

will probably acknowledge that as part of the debate.

[3:44'03] And aside from the frustration for not looking at it holistically I think there is a frustration about not looking at this in a long-term way. I had the great pleasure of listening to one of your colleagues, Brian Lamacchia<sup>183</sup>, one of the great Microsoft cryptographers, talking about this and I also spent a lot of time with Matthew Green, who's a fantastic cryptographer in the States. And listening to them talking about how cryptography has developed, we are very much at the Wright brothers stage of developing technology. We are just about off the ground and we are doing this in a very precarious way and if anyone gets any doubts about that, the FBI helped by somebody else, managed to get into the iPhone. It wasn't that it was an entirely impossible thing of doing that.

[3:45'05 ] What Wright brothers technology means is that if we start tinkering with that now, if we do anything to reduce the effectiveness of encryption, we'll be basically setting ourselves back and we wouldn't do that with cures for cancer anything else so why are we doing it with cyber security? The Wright brothers technology analogy also works when it comes to the solutions that are presented to us. And, believe me, WhatsApp gets presented with a lot of solutions to the end-to-end encryption problem. The same problem that you have is that if you are trying to scale up some of these theoretical solutions. That's again like trying to build a jumbo jet using Wright brothers technology for their first flying machine. We really need to be understanding that when we look at what we're asking companies to do in terms of changing their technology. We really are stopping ourselves from getting the very best security and technology that we could possibly have and there are lots of different examples of when we've done that in the past, whether it's the MD5 hash or whether it's the controls that President Clinton put in place in terms of strong encryption that have had impacts on security as we know it now.

[3:46'27] The fact that there is end-to-end encryption doesn't mean that companies shouldn't be responsible and shouldn't be part of the discussion on what does being a responsible company if you provide end-to-end encryption mean. I think that again it comes back to the e-evidence debate: what data is that we should be providing, under what circumstances, so we're not saying to law enforcement "you can never have anything at any point in time". We are being very transparent about what can be provided, and what can be used for, and what circumstances they were ever breaking our end-to-end cryptography. And I can guarantee that WhatsApp would never be breaking end-to-end encryption, because it is so fundamental to the company, also we believe in the future of a safe Internet ecosystem.

[3:47'39 - Marc Mossé] A lot of things have been said so... first of all, we should keep in mind - it has been said, but... - when weakening the encryption we may undermine both privacy and public safety. We have to keep this in mind, especially in a time when cybersecurity is on the top of the agenda, so we really have to take care of a comprehensive approach of this question. I would add another point which is often when government, not only government but agencies and others, are talking about encryption to me it's not always clear what they are talking about...

[3:48'27 - Gail Kent] I do not think it's clear to them either, Marc...

[3:47'39 - Marc Mossé] Maybe it's your assumption here, but the fact is do they speak about stored data? Do they speak about data in real-time transit? It's not exactly the same and it will not be solved through the same rule or process or technical means. We are in a time, again we perfectly understand the need to fight against terrorism, there is no discussion about this, but the question is: What are the keys, what are the scenarios to address and what are the concrete proposals?

[3:49'04] Once we have this on the table, the discussion could take place. Until that, it's a theoretical discussion and a discussion where we cannot find any real answer because we are not necessarily talking about the same things and the same problem. So I'm not getting back from the question, I am just saying that at that time we absolutely need to take into account all the aspects of this question which is, again, public safety, privacy, lawful access, cybersecurity as well and we need to approach this question through a comprehensive approach, yet again, and try to design a framework which is the one that we need: an international framework.

[3:50'00 - Alex Macleod] Thank you very much. This is the end of this part of the roundtable. Finally we'll have a discussant, who is Joris von Hoboken.

[3:50'10 - Joris von Hoboken] Thank you for having me here, I'll give a few comments and I'll go to the Q&A with the audience. I am an Internet and fundamental rights scholar, I did some work on transnational surveillance, cloud surveillance issues, encryption, human rights and intermediate liability. I wanted to just mention, there was this issue around how was your Snowden day at the beginning, and I had a pretty funny one because I was at a privacy conference, the Privacy Law Scholars Conference which took place in Berkeley that year and basically after imagine "la creme de la creme" of privacy law people coming all together, including Jennifer Grannick and people like that but also government officials, quite senior people at the government and then this panic broke out and everybody was together in

---

183. <https://www.microsoft.com/en-us/research/people/bal/>

this hotel and then the newspapers were put in our rooms the next morning with the big headlines, people started to fly to DC and other places like... to do more important things than having conferences...I was actually there for a paper on FISA 702 and how this issue is raised also from a European perspective.

[3:51'31] I'm going to give a few comments and each of them will have something like a question and then I guess you'll do it like the other time when everybody can just pick and choose, you know... You can take the ones that you feel would add something to the discussion.

[3:51'47] I wanted to start with something which is like the grey zone. This is not my term, this is a term of Bob Litt, who's an NSA general counsel. Bob Litt had this comment in a panel celebrating the first year of Snowden revelations: there has been a long history of cooperative relationships between American business and American government in the interest of protecting the nation and its citizens. Companies have not been asked to do anything illegal, they have their own lawyers, they are pretty good at protecting their own interest but just as you talked about technological gaps that NSA looks to fill, there are legal gaps. There can be an area of space between what is specifically authorized by statutes and what's specifically prohibited by law. And then there is a grey area in-between, where we have been very successful over the years in securing voluntary cooperation. I think it has been an unquestionable loss for our ability to protect the nation if companies would stop this kind of voluntary cooperation".

[3:52'53] My question is: Do you recognize this observation? Is there something like that? Has there been a shift in the willingness of the companies you operate in? I think it definitely connects to the issue of encryption because you can basically think of a scale where you have end-to-end encrypted products, you can call it adversarial design (you design your products in a way that you already anticipate being in this relationship with unlawful access where actually law can't help you). You can also think of a very different stance in designing these types of services or products which you could call anticipatory design where we are going to have these types of services - governments are going to be very interested in that - and organize around that we know that we'll be able to provide the lawful access that will be requested from us. That's my first question.

[3:53'54] The second question is on the differences in legal systems that have been discussed quite a lot already. The difficulties of resolving these challenges have become quite significant because of the height of involvement of courts, specially in this area of intelligence surveillance. You are basically seeing levels of courts involvement that are quite unique. For law enforcement this is maybe not so unique but for intelligence issues I think it is. There is a very sharp difference in legal approach between the EU and the US as regard standing to sue, so basically the ability to bring cases on privacy issues that come from lawful access dynamics.

[3:54'50] On the EU side, there is a very broad ability to sue. Now we have the Charter of Fundamental Rights which basically makes everything that happens to your data a Fundamental Rights issue. What is also legally and politically very relevant is that we have a main court that interprets these provisions in light of the European integration project. That means that the Luxembourg Court is super interested in claiming that it is actually protecting European citizenship and you see this in the number of rulings. So it is also a political project that we are running into in Europe at the moment.

[3:55'37] On the US side, and I am just focusing on the US although we could look at other relations [?], there are very strict constitutional limits on your ability to sue in surveillance cases, and civil society has run into that a number of times, for instance in the Clapper case<sup>184</sup>. So these are, I think, very deep constitutional differences and divides that cannot be easily overcome. Now especially that the Court has become a key player that really articulates these differences very heavily and you see that in the Snowden cases. So my question is: do you believe the current level of scrutiny of lawful access by the courts system, in particular in the intelligence context, is temporary or do you think we will continue to have such courts scrutiny in the future?

[3:56'40 - Alex Macleod] Just want to mention one thing... [about Marc Mossé having to leave at 6:30 sharp]

[Some time during which Joris chooses his next question]

[3:57'09 - Joris von Hoboken] On the legal issues on surveillance law reform, I am wondering what the panel thinks about the need to broaden the conversation a little bit: what types of data are we talking about? We have the tradition of having a surveillance debate which is quite heavily focused on communications, I mean, traditionally those are telecommunication companies and of course we have seen a shift about which types of services are being offered by cloud companies and different types of architecture. I think it makes a lot of sense to keep focusing on communication surveillance but there are a lot of other types of datasets and other services that have quite enormous privacy implications, you can think for instance of the services that are offered in educational contexts.

---

184. Clapper vs. Amnesty International. <https://www.oyez.org/cases/2012/11-1025>

[3:58'05] I am wondering if we shouldn't broaden the conversation beyond that kind of strict focus on consumer-oriented communication services. Just as an example: the laws are typically over focused on those types of services, just if mention could be made of the Stored Communications Act in the US, we have a new Dutch intelligence law, there was the news today that this new intelligence bill will be the subject of a general advisory referendum, which is I think quite unique for such thing as an intelligence act and raises all sort of interesting political questions. That surveillance law has new rules for communication surveillance but it has also kind of hidden, in-between, draconian provisions on access to other types of data systems. For instance like BD access to complete datasets that are held in the private and the public sector and also the possibility to obtain direct access to such information systems holding this kind of data.

[3:59'22] My question is: do you agree that the debate is focusing too much on communications content and related data and not addressing the privacy implications of other services enough and what could we do to bring those other types of privacy issues into focus in the debate so that we move forward on how to design of the laws. Thank you.

[3:59'45 - Alex Macleod] So, would somebody like to start, there? Gail?

[3:59'49 - Gail Kent] I can probably answer two of them very briefly. Firstly I think there is a debate on the difference between them in reverse order. I think there is a debate already on the different types of data particularly under the Budapest Convention of the Council of Europe. Because that comes from the cybercrime perspective, that's not just about communications data, that's also about if you are trying to investigate the cybercrime investigation [??]. I think that has already started but I'd agree it probably needs to go further because all the different companies that are here have different types of data because they provide different services.

[4:00'26] In terms of resolving the difference between different types of law, and the role the courts are playing, I think that's where, it feels to me that there is quite an easy almost cut and paste between what European judgements on surveillance legislation have been and what good standards may be. So somehow the ruling on Safe Harbor and the Privacy Shield actually helped a lot because I think it outlined eight different standards for what good legislation might look like and what the Fundamental Rights Agency look like and it looked at what different European surveillance legislations looked like and one of those was the ability you highlighted to have standards and to go and plead your case. And that's obviously one of the things that came out as part of the Privacy Shield discussions that Maud talked about earlier, the ability to go to some body in the States and claim that something is happening that shouldn't be.

[4:01'35] And then probably the most important one for me is your first question about should we be anticipating law enforcement's requirements in terms of how a service might be used. I think one of the first things I said is that it's part of my job and I have thought long and hard and really intellectually about this and I don't believe that we should. And the reason I don't believe that we should is that law enforcement, like companies, like technology, is constantly evolving or perhaps it should be evolving. We shouldn't be at the point where we just always expect we should be doing things because it makes law enforcement's life easier because that's a pretty weird state for us all to be living in if we're doing it so that we allow or we're enabling better surveillance. So I think that from that perspective it's you know it's a strange angle to come from.

[4:02'29] I think the other thing is that what one of the things that I'm thinking about WhatsApp is that... You know, Jan and Brian, when they founded WhatsApp and when security was a really big part of it, they did it for, Brian for security reasons and Jan, because he came from Ukraine and absolutely understood what it meant to have a government looking at your your communication. But even us wouldn't have thought that end-to-end encryption was the most important thing when users were using it. Maybe it was the sort of delightness and the ease that WhatsApp can be used was the reason that it is so popular.

[4:03'16] But actually going out and talking to people and doing research and doing questionnaires onto what actually matters to people is no, that end-to-end encryption really does matter to people. It matters to people that for the first time they can have private, secure communications that used to only be available to governments. That level of security matters for those that are communicating with doctors. It matters for people that are using it for business purposes, and there are a lot of people that do use it for business purposes including politicians, that matters to you know husbands and wives having conversations.

[4:03'55] And even if I think about using it myself I like that level of assurance that it's not available to anyone, that nobody can get that data. And I think if we start exactly the same sort of like putting a freeze on what you can do in encryption, if we start limiting what companies can do for technology reasons then we really really, we're shooting ourselves in the foot and we're stopping great innovation and technology that will probably improve all of our lives.

[4:04'27 - Alex Macleod] Thank you. Is there anybody else on the panel? I that case I would throw it open to the floor. Is there somebody that would like to make a comment or ask a question to all members of the [panel]? Yes, please.

[4:04'50 - unnamed participant] My question is about e-evidence. I am wondering whether disagreements or tensions

might arise member states and the Commission and Internet companies because when I listen to you I understand that you all want to have a framework. So where are the disagreements?

[4:05'10 - Acadia Senese] I'll let my European colleagues take that one...

[4:05'18 - Marc Mossé] To know the disagreements we should know what the proposal is. So we do not know what the proposal is yet but the point is... I am not trying to escape the question [laugh from several people]... My point is more simple here. What is the efficient way to get access to evidence in terms of public safety that protects privacy? To do so there is a mechanism of mutual recognition that we know pretty well in Europe as a mechanism of cooperation between the member states, which means that, if a request from a member state is fully compliant with the law of this member state, it should be welcome in the member state that will execute this order. It's a mechanism which is pretty simple when you describe it, but it's a little more complicated to put in place. This mechanism of mutual recognition is one of the angles. The other aspect is, as we discussed earlier in the panel, when it's possible the government should go first to the customer, rather than to the company, just in order to avoid to put us in a difficult situation most of the time.

[4:06'46] It would be easier to get the data from the customer if there is a need to do so. If not, again, it should be done in a way that both legal systems of the states, which are the state asking for the data and the state where the data is stored, are agreed on the legal requirements. This is where the mutual recognition mechanism is maybe, I would say, the most effective one. Again, we have seen some lines drawn in the non-paper that has been issued in December 2nd, 2016, if I'm right. We'll need to see further details to be sure that it works well, but again what we should absolutely avoid is a mechanism where service providers are confronted to a sort of contradictory injunctions. We should be in the position that if we agreed on the request, we respect both legal systems.

[4:08'02 - Maud Sacquet] Perhaps just one point. You would be surprised how much, even though 28 member states can agree on a framework, they can then disagree on the way to think. That's often why it takes so much time to actually get any kind of legislative acts in Brussels. It's fascinating to see on which issues you have some coalitions between some countries and in another issue the coalition changes completely. On this point, we haven't seen the proposal so it's a bit difficult to say but you have to think for example that in some countries law enforcement can get content data while in some others they can't. There is very important difference into what kind of data and mechanism that works in every system and so I'm guessing that where the blocks will come in the definition is especially around this issue that what can get in every country and should you as, I don't know, an Irish police officer be able to hand more data to your French colleague about an Irish citizen than you would be able to do under Irish law. Very practically, this is the kind of issues that I'm guessing will be discussed.

[4:09'22 - Marc Mossé] We have seen already something working with the EIO, which is the Executive [in fact European] Investigation Order. This is a directive from 2014 or so, that should be now in force in 2017. So it can work, this is mutual recognition mechanism as well. Just think about mutual recognition as a way to ensure that both systems are respectful of the principles of each member state. You have to be sure that when I'm acting under this legal system I am sure that this request will be totally compliant with the legal system of the other member states. This is where there is still room for negotiation. 28 -still 28- member states can work.

[4:10'27] There is still another option, which is the enhanced cooperation, if that fails with 28 or 27 member states. This is one option, it exists in the treaty, nothing very extraordinary, and we know some possibility: Schengen is an enhanced cooperation, the EIO I think is an enhanced cooperation as well, so there are different options that could be decided in the coming months because again, following the report of December 2016, the proposal could come in 2018 or beginning of 2019 if I am right.

[4:11'08 - Didier Bigo] It was just a remark about what may be the case if you remember in 2005 how people were so pleased to succeed to have this agreement between the EU and the US about the legal agreements [probably "assistance" or "cooperation"]. But what happened was that the NSA bypassed completely all law enforcement agencies. So we have discussed, and that's crucial, about law enforcement agencies and their practices but we still have - we'll invite you again - on foreign intelligence and how the protection given by the Fourth Amendment to their own citizens in the US is not applying for others, the foreigners (for them, they are the citizens of other countries). And we know that, as long as we have this kind of elements it will be very complicated. I think that at the EU level it's almost the same kind of understanding.

[4:12'35] So I was surprised that the question of the distinction for you, in your practice, you have spoken a lot about the requests which come on crime, or on evidence of terrorism, but not so much about the large data where you have no warrant, regarding suspicion, on different case, the way it has worked through different possibilities and the UN... I was surprised that this has not come. So it's an invitation, because we will have three conferences. Today was the first one, we will have a second one with more discussion about what is going on at the UN level and we had a lot of expectations, two or three years ago, regarding that, but that has disappeared. Or what is going on with, now, the CJEU and EU-Canada PNR and what are the facts now with EU-Canada PNR that the definition of privacy is now changing,

at the same moment there is the e-directive. And we will have another one in almost a year, in September. I hope that most of you can come back, we'll have a couple or three days regarding that, where we will discuss also other people, but I thought it was really crucial to have all this discussion in details, for the law enforcement and the way you have framed that. It was important to say that before Marc leaves for you to have organized [to come here] and to have spent so much time. It was more a compliment than a question as such but also an invitation to come back, for most of you.

[4:14'58 - Gail Kent] Can I just say that? I think that you were suggesting that companies were providing bulk access for data and that's not true. So there...

[4:15'05 - Didier Bigo] I was not. I was referring to the case which was in 2013. The way it has been organized. So with PRISM and with the different activities, you have, willingly or unwillingly, distribution of the information by the private companies. So we can continue about that, no or yes, it will be one of the elements and that's why that's very important to come back to that because in 2005 the agreement was that the US could have passed through all the legislations that it had at the time. So it's not a blame but it's the way it has been done at that time and we may come back to that because you have different views about what happened at that time and what is Snowden is a question of foreign intelligence and not using bulk because you know that bulk signifies something different. So we need to come back to what happened and how a form of oversight, and not a national oversight, could create the conditions for this - I don't like the term balancing - but this demands constraint to have a high level of privacy and nevertheless to have safety and security. The terminology of balance is a very US way of thinking, or UK way, you know that the European Court of Justice for example asked for a very different thing from balance. We can continue on this later.

[4:17'10 - Marc Mossé] I am sorry because I have my train... You have re-opened a very interesting debate that could take a little bit more time... just two things: on the "balance", I use often this word because it's maybe a bad translation of my constitutional background which is in the jurisprudence of the Conseil Constitutionnel we talk about conciliation, which is a way of balancing both principles but at the end of the day I come back to one very important principle, which is: there is no hierarchy between the Fundamental Rights: you always have to balance those in a way that you respect the constitutional heritage. This is how works the jurisprudence of, I would say, most of the courts across the world.

[4:18'02] I have a third book for you, which is called "les entretiens de Provence", written by 4-5 judges from different supreme courts. In fact, it was Robert Badinter, Chief justice in France, Stephen Breyer and Antonio Cassese, another judge, that spent one week all together talking about how supreme courts take a decision, not only how they take the decision itself, but how they go to the decision, what's the process, how they interact intellectually to get the decision. What you can see when you read this book, which is very interesting, really, with this dialogue between judges from supreme courts from all over the world is really how you can, how you have to balance between those fundamental rights.

[4:19'09] But, again, it is a very interesting debate and I would love to continue on this and, I have seen Gail react, we do not give any bulk of data as a principle, this is why this New York warrant case is so important, because beyond the grey zone we want to get clarity. We had a singer in France - you do not know him he is Eric Charden, maybe just a few here know him - who had a song which was "the world is grey, the world is blue", so maybe we went from a grey world and going to a blue one and I am going to [get] my train, thank you.

[4:19'54 - Alex Macleod] Immediately I want to thank our panel, which have given us their time and their energy, so thank and have a safe comeback.

[4:20'11 - Félix Tréguer] Thank you very much for this wonderful discussion, now we'll be moving to the concluding remarks, so we'll give the floor to Ron Deibert from the Citizen Lab at the University of Toronto, for ten minutes, and then we'll hear Mr. Thierry Delville, who is the ministerial delegate for security industries and cyberthreats at the Ministry of Interior, in France, the so-called "cyberprefect".

[4:20'35 - Ron Deibert] OK, hello everybody. I have the unenviable task of going at the end of a long day with very interesting discussion - not as enviable as the actual last speaker although. People were asking and talking about their Snowden moments so I might as well say mine... I published a book called "Black Code", which is about very much the subject matter about surveillance, in 2013 in fact the very day that Snowden fled to Hong Kong. And you know that could have been a disaster. But ultimately I think it worked in my favor and I didn't get too much wrong.

[4:21'14] I would just like to say a couple of things. Maybe what was overlooked mostly. And to that end I'd like to begin with what I think was an obvious thing that wasn't said right from the outset and that is what is it that we're talking about here in terms of the services that these companies provide and why we're in this situation to begin with. While the panels were going on I googled the mission statements of each of the companies that are up on the table. So, Facebook as I think it still "bring the world closer together"?

[4:21'48 - Gail Kent] We just changed that: "bring communities closer together".

[4:22'01 - Ron Deibert] Google: still "organizing the world's information, making it universally accessible". Microsoft (I couldn't believe it): "be what's next". Is that actually? That's why he [Marc] left because it can't be real. But you know, I think these mission statements I understand why their mission statement may actually obscure what it is really that these companies do. And I think it's important for us to define it from the outset that we live in a personal data economy. And these companies provide the infrastructure for commercial surveillance and behavioral engineering. That's what it is about. In spite of the mission statements.

[4:22'38] And then I think it's useful when you reflect on that for a minute and what that means, especially for private sector-government relations, to ask yourself what is the mission statement of states. There are many definitions we could go to you could think of Max Weber. But since we're in France and I'm here with Didier Bigo, I think I'd go to Foucault and say "the state is the organized practices through which subjects are governed". Is that right, Didier, would you agree? More or less? So when you compare those too, the infrastructure for commercial surveillance and behavioral engineering to push advertisements and profit ultimately make money and then to the organized practices through which subjects are governed, you can see there's a convergence of interests at a very fundamental level here.

[4:23'27] This is where big data meets Big Brother and that's the crux of the issue of why there is such an important connection here for governments, for states, for law enforcement, for intelligence. What these companies do is an irresistible proxy, an attraction for social control for everything that they're interested in doing: that's part of their mandate and that's why we have all of these issues about what is the relationship between the two.

[4:24'00] And I thought it was interesting that Mark said that the rule of law is our North Star and I was glad to hear Gail say "Well, that's true but there are some some complicated issues around following the rule of law, especially when the context is different". Of course, the rule of law varies country to country, and if you think China, for example, to state the elephant in the room, they have a new cybersecurity law (I think it went into effect in June of this year) that requires companies to host data locally to effectively police all of their users.

[4:24'36] At Citizen Lab, we've been doing extensive research on China-based mobile applications where we reverse engineer them or do experiments to understand what type of filtering or surveillance they had baked into their applications or that are done on the server side by the companies. And what we find is of course quite astonishing that there there is deeply baked-in censorship and surveillance because they're following local laws in China. This is not so much an issue yet for Google or Facebook of course, although I did watch with interest the news about Facebook in discussions with China, eager to enter the market even going so far as to develop some kind of algorithm that would satisfy these requirements.

[4:25'24] So it's important to keep that in mind that there is this variation happening. And then also the trend lines: most of the discussion was about compliance with US, UK, European law. But there is a major demographic shift happening worldwide right now. The vast majority of Internet users, and hence the customers of these companies, are coming from the global south, now and certainly into the future. The sad reality is that most of these countries are not democratic countries. Most of them are authoritarian or hybrid regimes, sliding back into autocracy where the rule of law means something completely different.

[4:26'06] At Citizen Lab, we've just done several (I think five) consecutive reports where we've unearthed commercial spy were sold to the Mexican government, used to spy on journalists, activists, human rights defenders and so on. No law was broken there at all. NSO group, the Israeli spyware company that supplied this technology to the Mexican authorities, rightly claims that they follow Israeli and local law. So the issues that we're talking about here I would have liked to have seen been discussed more with the horizon in mind about what it means down the road.

[4:26'43] The other thing I'll bring up is around fake news and disinformation. I am surprised that topic didn't come up at all considering that both of these companies, I think today Google came out with the news of both the advertisements and Facebook did before that. Again here there's a convergence in a really odd way, I think a troubling way, which is where the company's revenue model, which rests on pushing advertisements and surveilling users in a very fine grained way. And I recall the Facebook experimentation that was done a few years back on manipulating people's emotions. This is actually fertile ground for political manipulation and disinformation and psychological operations.

[4:27'35] And I think we're going to be seeing soon a real problem around, that not only for the users but for the companies in terms of how they deal with that issue. And I saw Facebook today just released a post about how they will not have their platform used for the manipulation of elections which is commendable, but it makes me think maybe it's like a Band-Aid over you know flesh eating disease that maybe these companies, given the nature of their their platforms and how they operate at a core level, are really amplifying a kind of tribalism. And that really can't be escaped because of the nature of the way in which advertisements are pushed to siloed communities and increasingly will be manipulated in the future.

[4:28'27] The last thing I want to bring up was around targeted digital attacks. Another subject that didn't come up today when I think about security issues in this area, it's the one that I feel is most pressing, most urgent. At Citizen Lab we've been tracking what we call a silent epidemic of targeted espionage against civil society groups, human rights defenders worldwide. A lot of this campaigning takes place through the platforms of these companies through the misuse of their applications. To their credit, all of them, I think the ones that are represented here on the table want to do something about it and have taken some steps to do something about it. But I do believe that more could be done. One simple thing is requiring two-factor authentication by default.

[4:29'17] Now it's interesting to think about why that hasn't been done yet. Banks do it and I think it has to do with a principle: when companies are left holding the bag because their infrastructure is misused, in a certain way then they're incentivized to do something about it. But when users are left holding the bag the companies are incentivized to do something and I think that's the case here, unfortunately. So I hope steps will be taken to rectify that in the future. I would end it there, I really enjoyed the discussion and thank you Didier for the invitation.

[4:30'43 - Thierry Delville] Good evening everybody. I am Thierry Delville, the French delegate for the Ministry of Interior in charge of industrial security and cyber threats. Thank you for the invitation, I suppose I am the last to speak, so I will be short. I am very happy and honoured to be invited to speak in this chamber with so many researchers and experts. I recognise Mr Mossé, we were working together on different subjects. As a representative of the French Ministry of Interior I am aware of the sensitivity of such a subject, which refers to the very foundation of democracy whose strength is to know how to manage permanently the difficult balance between preservation of our individual freedoms and defence of the safety of the same individuals.

[4:31'46] Studying the techniques of interception and analysis of communication, the use that the services and agencies make of them, and the political and legal controversies they provoke seems to be at the heart of the reflection you are addressing. As well the analysis of the reconfiguration of the contemporary logics of surveillance wants to redefine the limits of democracy and questions to the sovereignty of states. (That's a good subject that you are studying). Obviously my remarks will not address the substance of all the issues that have already been or will be discussed at the next session, but allow me to give you some general thoughts on the evolution of security and the place of the states, I mean France in particular, but it will remain valid for most European democracies and countries as well.

[4:32'42] Digital transformation is at the heart of the society's major challenges: big data, clouds, smart TVs... we are speaking about smart and safe cities. All those developments lead or have led to the development of new economic actors (some of them are here, I suppose), who have developed and are able to work themselves on research and development, without external help. This is a big difference with the whole industry: unlike the pre-existing model, in the military shield for example, a large digital industry exists and developed without necessarily resorting to state budget, and that's a big difference in terms of relations with them. Interception tools and law - I will briefly make a shorts review of the context in France - the techniques of investigation in the digital age are seen as interferences in private life but they are necessary to characterize offenses, to protect the economic interests of a country and therefore they legislate or frame them very precisely.

[4:34'03] The use of interception of correspondence [through] the electronic communication or phone tapping is a procedure frequently used in criminal offence proceedings. The cases and the conditions under which such communications may be intercepted are provided for in different articles. Maybe I won't list the code of criminal procedure but you know the law, I suppose, the 1991 important law following the condemnation of France by the European Court of Human Rights.

[4:33'38 ] In practice, the interception of correspondence is carried out by requisitioning by any qualified official, service or organisation under the authority or supervision of the Minister of interior in charge of telecommunications, or any qualified agents of a network operator or access provider. The requisition of electronic communication operator put in place technical elements to intercept communication and collect data on their customers. Government, on the other hand, must have the technical tools to receive and decode this data. Nowadays [it requires] digital and human resources to exploit them.

[4:35'21] The legislator has intervened in many many occasions to shape the regime applicable to the judicial interception. There is a law with important modifications and evolutions in 2004. And the French legislator has adapted the means of the interception in the digital age with procedures very framed legally. It may also be geolocalization form of digital surveillance, infiltration, data capture with the aim of recovering numerical indices, enabling the compilation of indices, with which we subsequently characterize criminal offences for example.

[4:36'10] In the administrative or intelligence field, the legal framework is different and it is necessary to underline the recent evolution introduced by the law in 2015 on intelligence, which creates a the CNCTR. I suppose you know this organization, an independent administration who advise on their requests formulated by an internal ministry, like defence, justice, economy or finance, for customs or for border control. It's made mandatory prior to the prime minister

decision [?]. That's the context in our legislation.

[4:36'56] In a second time, I would like to speak about the interception tools and the digital revolution. Digital transformation is apparently a bargain for foreign intelligence or law enforcement agencies as a multiplication of sensor and the storage of the information in the servers or in the cloud and different things that are likely to be able to answer the needs of an investigation.

[4:37'23] In fact, several factors make today's task of the state services less easy than it seems. In reference to what happened a few years ago: a few years ago, in a number of cases, we are witnessing the development of a genuine capacity asymmetric between the means available to offenders and those used by the representatives of the rule of law. So development of end-to-end encryption is just as much a security factor for the confidentiality of information, it is increasingly exploited as a tool of concealment by large criminal organizations.

[4:38'03] The issue of the location of data and the legal status of the data is a considerable issue. Extraterritorial issues are very much [occupying?] the debates and legislative development and make it increasingly necessary to establish bilateral or multilateral agreements to facilitate information communication under the control of judges. So time is short for terrorist investigation or organized crime cannot be satisfied with the long communication time which can sometimes lead to a response after three hundred have died, to have an answer to our request.

[4:39'03] Legal interpretation specific to the major players on the Internet with whom we work at national level in particular I run actually quarterly like this [?]. We created a group two years ago, after the first attack in 2015, and we are sharing information with GAF A and telecom operators and their correspondents in France. We have also the same information-sharing at the European level and we see clearly that on the communication of data certain interpretation, linked for example to the difference of interpretation of hate speech, exist really between us and the operators, and sometimes between operators themselves.

[4:40'00] [It's our position?] that the technological development of communication tools that respond to strong economic imperatives should not take place within a framework that cannot be regulated or simply apprehended by the state services. The nation, as in the case of a terrorist threat or a flagrant crime, especially when the life of a person is at stake, it is essential that all means of interception can be activated within the framework of the law and regulation in force.

[4:40'35] In order to achieve lasting results, it is important that all economic actors, starting with industry, telecommunication regulation bodies, the agency responsible for their control and certification of tools should be committed to these requirements just as strongly as in the success of the new product line. This dialogue, if it exists, is nevertheless a major challenge to be [?] for the next years.

[4:41'08] I would conclude my remarks on the issue of cyber security interception. We have different concepts like data capture, the development of private offering of tools that are real tools for spying and capturing information remotely, is today a particularly important challenge. This issue of cyber defence is discussed at the same time as actors manipulated by states seeking to destabilize targets by this means. It is also about cybercrime, with actors who can sometimes be the same and who use the same tools to attack targets for the more directly lucrative purposes.

[4:41'51] The new reality that I can see is supplanting the old and the disappearance announce in a more or less short period of time of the classic currencies to the profit of the digital transfer or even the crypto money must encourage the states to wrestle in their way of fighting on equal terms against these new forms of delinquency. The challenge is, on the one hand to encourage companies and individuals to protect themselves. This is the meaning of the Military Programme Act of 2013 (I suppose you know this law) for operators of vital importance.

[4:42'35] This is also the meaning of the NIS directive which will operate next May. This is this also the meaning of the GDPR EU directive [not a directive in fact] that will allow as May 2018 to strongly condemn any economic actor who will not protect this personal data. On the other hand it is important that states organize themselves from what constitutes a new field of [maneuver?] of defence and security are formed more than in the physical world in the logic constitute a continuum and the technical expertise and ability to stay in the race are more challenging everyday. Thank you for your attention and I wish you on this exciting topic an excellent work.

[4:43'45 - Didier Bigo] Do you want to add some final comments? Or have we exhausted the topic? It was just a chance maybe to have answers to some of these elements that we have given.

[4:44'00 - Gail Kent] One very final sentence. We have seen in Facebook that we are 1% done. I don't think that any of us think we have all the solutions there, this is why this sort of conversations are really important.

[4:44'22 - Acadia Senese] As a follow-up on my very first answer, I think of this day, which was, I think, hours ago

now, but I was asked about the Snowden disclosures and I said my colleagues were quite surprised at the disclosure and frustrated with the government's failure to correct the inaccuracies. My fear is that those inaccuracies have persisted. And you know I think it's important that I say that you know Google doesn't do bulk, doesn't respond to bulk request for data. For its part during the Snowden disclosures Google's involvement was responding to compel legal process. So with that I think will be a segway to the future conversations that we have here. But I did want to end on that.

[4:45'07 - Didier Bigo] I have seen that it was also the next just for the people who had the courage to stay, I mean all these elements, we'll have two other conferences. One quite soon, which will continue on what are the forms of activism which have existed, what are the possibilities on encryption-decryption logic, what has been called for example countersurveillance. Why does that mean? Does it mean something?

[4:45'53] For certain people it's a strong belief that it means something. For others it's almost "we don't see the difference between surveillance and counter surveillance. Maybe it's just a loop". And that's one of the questions. We will have also, and maybe it's interesting to have all your voices before to have that. A lot of discussion about the different legal actions. We'll have a couple of lawyers coming from Privacy International. We will have all the people coming from the US and [?] and so on.

[4:46'41] I think it's always very important to have this first panel, because we have found your position, despite the diversity, was very strong in terms of saying the same form of narrative about what a private [company] have done, what they were obliged to do, what they have never done, and you insisted. Some people are saying "yes they have done" so we'll have a final conference on September 2018. So we are trying also to investigate more about that, with two or three days.

[4:47'23] Regarding panel with private actors, I hope that you will come back. We'll also have persons coming from activism and also persons who are in charge, at the of policy level, to intervene, also at the EU, at UN level. So we will have national, I hope, we are eager that you will come back also, we will have these two days, three days if we are lucky, but two days where we'll have this simultaneous discussion. The idea is really to try to, as I say, to deconstruct the stereotypes, to put more elements about what are the evidence people have.

[4:48'21] Could we have evidence based on this logic? Because we have seen that very quickly [we] can come back to belief. So what are the elements that can be put on the table? We know that we will not have one story, it's also constructed depending on the positions that people are occupying. Stories are complex but nevertheless I think it's very important.

[4:48'53] The second idea is nevertheless true. I think it's something most of the actors agree - not all. What are the conditions under which it is possible to have a better oversight? And the way to construct a bridge where this idea of trust will not be claimed because, it will be obvious in practice. Because the more you speak about trust, and that's really one of the law of sociology, it's because you are obliged to speak about trust, because nobody is trusting. It's about distrust, the practice is distrust, so you speak about trust. You never speak about trust as alone. If you have never divorced you don't understand what I am saying.

[4:49'44] The discussion about trust is always a question which will be put in practice, between the reluctance of people we'll see [many doubts in this sentence]. That distrust is the practice and we have seen a lot of discourse about trust. The discourse is not the proof that it works better or it will work better, it's because you have a problem and we need to come back to the roots of that.

[4:50'18] When we have MLAT, for example they are used. They are not bypassed. And that's also one of the key elements that we have to discuss certainly more to build at least some legal framework where the idea is that the legal framework is there to avoid to go in depth into practices, but that it could be operational and limit some of the elements about the form of intrusive surveillance which are not into this legal framework.

[4:51'02] So that's the general idea. I have tried to put it in a nutshell and I hope everyone will be sufficiently interested to come to the other conference. So we'll have the conference in December, we will send you more elements about this one soon. So it will be on the 18th of December. We will have the other other in September 2018.

[4:51'40] In the meantime we have also a running seminar with researchers and PHD students where, if you are interested, you can also register. You can come in. Thank you very much. Thank you also for the organizer because I've spoken a lot but all the work has been done by Félix Tréguer, who has really organized everything.

