Seeing like Big Tech: security assemblages, technology, and the future of state bureaucracy

Félix Tréguer

8

SEEING LIKE BIG TECH

Security assemblages, technology, and the future of state bureaucracy

Félix Tréguer

In June 1831, a Frenchman, 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. The privately-owned telecommunications infrastructure he set out to build would not only serve the interests of French industry barons willing to track stock prices in the financial capital of the world; it could also be of use for the diplomatic communications of the French government. The whole plan was risky but, after all, there was no law sanctioning the monopoly of the French state over telegraph networks.

To be on the safe side, Ferrier thought it was best to ask the government for an explicit authorisation. But Casimir Périer, then head of the French government, was hesitant as to what his answer should be. 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 2009). Could the government seriously consider meet that demand while keeping its monopoly over the telegraph? Many thought not.

Alphonse Foy – 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, Foy wrote a letter that offered a more-than-tepid response to Ferrier's project. "Mr. Ferrier's request is entirely inadmissible," he wrote (Charbon 1991, 12). As a servant of the government, Foy was appalled by the notion that the French state could lose its monopoly over telecommunications infrastructures. As Foy argued, "the existence of this telegraph communication would necessarily harm the present privilege of the government to be the first instructed of all-important news." The government had to be the first one to see and learn about what was going on. But the fundamental belief expressed by Foy's blunt refusal was that a privatised telecommunications infrastructure was a challenge that the modern state simply could not handle. All the techniques of

power – like surveillance and censorship – institutionalised since the 16th century in partnership with private actors to control the subversive effect of the printing press and of postal networks while allowing them to serve the interests of both the state and early capitalism would come crumbling down.

So 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 that was not authorised by the government and not sent over public telegraph lines.

But in many respects, Foy and Gasparin fought a rear-guard battle. As it had already done with older communication technologies, the state would soon move to a lighter-handed approach. From the 1840s on, the development of the electrical telegraph accelerated national and transnational communications flows, as the industrial revolution spurred the demand for coordination and communications (Beniger 1986). By the end of the 19th century, private corporations did not only make extensive use of the telegraph and of the new communication technology of the time, the telephone; they also played a growing role in the construction and management of national and international infrastructures to serve the needs of states and globalising market actors (Barty-King 1980; Headrick 2012).

Fast-forward 150 years. Neoliberal policies launched in the 1980s have completed the dismantling of public and private monopolies over telecommunications networks, and digital technologies have profoundly intensified data flows. Once again, states have found ways to transpose their traditional techniques of power to digital communications (Galloway 2004; Goldsmith and Wu 2006). When they do – whether it is to engage in surveillance, censorship or propaganda – they almost always do so in interaction with companies who manage parts of the multi-layered architecture of the Internet.

In the process, actors who occupy key positions in the state's intelligence and now law enforcement agencies have to constantly negotiate alliances with these private actors. Today, that means not only dealing with large firms in the media and telecom sectors whose relations to the security field can be traced back from the 16th and 19th centuries, but also with tech firms that have come to dominate the digital economy – mostly US-based multinational online service providers, software producers and online platforms like Google, Apple, Facebook, Amazon and Microsoft.

In other words, "Big Tech" joins "Big Media" and "Big Telco" as yet another oligopoly commanding over the all-important communication industries, and more generally the global economy. Today, Apple, Amazon, Google/Alphabet, Microsoft, and Facebook have acquired the highest market valuations globally (Statista 2018). Tech is now the largest sector in global capitalisation, amounting to 3,582$bn, before financials (3,532$bn), consumer goods (2,660$bn), healthcare (2,300$bn), oil and gas (1,411$bn) or telecommunications (859$bn) (PwC 2017). Having championed new models based on the algorithmic regulation of online communications as well as regimes of surveillance relying on the

systematic collection and analysis of behavioral data (Fuchs and Trottier 2015), these resourceful companies hold an irresistible appeal for security professionals tasked with controlling communication flows.

This, in turn, is leading to a historic shift in the public-private assemblages regulating communication networks, which actually points to a much wider trend in modern state power. In *Seeing Like a State* (1998), James C. Scott has shown how modern statecraft was built by ensuring legibility through measures, metrics and other "state simplifications" aimed at representing and acting upon both the natural and social worlds. In the age of Big Data, the techniques mastered by Big Tech are now seen as crucial to make the digitised world legible and governable. Faced with swelling data stocks and flows, the state needs to see like Big Tech. This gives way to a negotiation process aimed at co-opting its infrastructures and its data-processing techniques. Big Data governmentality hence spreads throughout the security field and beyond, across state bureaucracies.

Shifting public-private assemblages in the security field

To make sense of these ongoing negotiations, it is useful to start with the concept of security assemblages. With the rise of security privatisation in the context of neoliberal economics, the public-private category has become a key theme in security studies, with research on topics ranging from private security guards to the role of private companies in the logistics of military forces or subcontractors in the intelligence field (Abrahamsen and Leander 2015; Williams 2010). But, against those insisting that the increasing role of private corporations in security is one more evidence of the weakening of traditional state sovereignty, critical security scholars like Abrahamsen and Williams (2010, 23) have instead argued that "privatisation is not a challenge to prevailing structures of authority, but is embedded in, and inseparable from, transformations in governance." Seeking to lay new theoretical foundations for understanding how private security is historically and socially constituted, the authors have introduced 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)*

Against those authors who ground the concept of assemblage in the philosophy of Gilles Deleuze (e.g. Haggerty and Ericson 2000), Abrahamsen and Williams instead anchor it in the Bourdieusian concept of "fields" to highlight the evolution of material, symbolic and cultural forms of capital within the security field. Their approach also builds on Saskia Sassen's notion of "disassembly" to highlight the fact that an assemblage is actually a process whereby some components of states are configured in new power structures, as formerly public functions are transferred

to the private sector. "Security assemblage," then, refer to the way security governance is increasingly achieved through fluctuating arrangements of networks of state, corporate and other voluntary actors, which together form "knots of statelike power" (Harcourt 2015).

That the tech industry may play an important role in security assemblages may not be surprising. After all, from Charles Babbage's proposal of an Analytical Engine to Alan Turing's Enigma, the genealogy of computers clearly shows an immediate connection between the development of these technologies, and the needs of modern bureaucracies – whether public or private. Data processing tools associated with statistical work and calculation have historically played a key role in the modern state power (Agar 2003; Desrosières 2002). They have also long been a cornerstone of the military-industrial complex, as evidenced for instance by scholarship on the role of IBM in the Holocaust (Black 2012) or inquiries on the history of the Silicon Valley and its intimate relationship with the US military (Bellamy Foster and McChesney 2014; Edwards 1996; Harris 2014; Lécuyer 2007; Levine 2018; Nesbit 2017).

But what makes ongoing negotiations between Big Tech and the security field particularly interesting is that this oligopoly also originates from a corporate culture marked by a "counter-culture libertarianism" (Barbrook and Cameron 1995) – one that has deep historical roots (Turner 2006). As a consequence, from the point of view of many stakeholders, these organisations first appeared as relative outsiders to the security field. As the process of hybridisation between the state and the new masters of communication industries unfolds and has yet to stabilise, the security field intersects with other social fields that traverse these organisations and are influenced by this counter-cultural, oppositional ethos – like the field of computer security or that of digital rights. For this reason, the incorporation of Big Tech in the state's security apparatus is marked with intense power struggles that are often made visible, for instance through the media.

Post-Snowden: cooperation or resistance?

These struggles can provide key insights to understand data politics and modern state power. In recent research conducted on the surveillance of Internet communications by intelligence agencies, we approached these issues by looking at the debates around Internet surveillance in the aftermath of the 2013 Snowden disclosures in the United States and in France (Tréguer 2018). By following interactions between Big Tech and governments as they moved from surveillance to other issues of interest to the security field (such as the weakening of encryption or the fight against terrorist propaganda), we worked through an inductive approach to identify factors influencing how these profit-seeking entities and their managers would fall in the cooperation/resistance spectrum, depending on the changing context and constraints that they face across time and space.

Among the factors making up this constraint structure were a firm's internal corporate culture, past and ongoing dealings with the human rights field (e.g. past human rights scandals affecting them), the importance of user trust and the threat

of competition. The relative weight of these constraints in a given context made resistance to the demands of the security field more likely. In turn, the sensitivity of these firms to regulatory changes, the identification of their managers to what Mills called the "power elite" (Mills 1959), their dependence on public funding and procurements, and the existence of criminal sanctions for non-cooperation all made cooperation more likely.

Looking at post-Snowden debates in the United States and in France to see how this constraint structure played out, we noticed some differences between the two countries from 2013 to 2015. In the US (and although these actions had global repercussions), we first see overt and multi-pronged resistance strategies being staged by Big Tech, whether through "technical resistance" with the roll-out of encryption on their products, or legal and political resistance through litigation and political advocacy aimed at reigning in the power of intelligence agencies.

In part, these can be read as instances of "double dealings" in the field of human rights defenders and that of hackers and engineers who were mobilised to beef up privacy protections in response to the Snowden disclosures. In Bourdieu's research such double-dealings refer to situations "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, and Danaher 2002). By aligning themselves with the privacy claims of their own workers concerned about their incursion in the military-industrial complex, the demands of human rights organisations and those of the field of computer security, these firms were able to remobilise workers, mitigate reputational risk and restore the trust of their users and customers concerned by the revelations, thereby securing or even reinforcing their market positions.

Encryption is a case in point. Whereas media coverage often over-emphasised the tensions between Big Tech and governments on this issue – for instance in 2016 when Apple refused a request by the FBI to collaborate in order to bypass encryption on a iPhone used by the San Bernadino shooter – such legal resistance often simply came down to respecting the state of the art, as computer engineers across the world worked to draw the lessons of the Snowden disclosures and beef up computer security globally (Rogers and Eden 2017).

Big Tech did not go much further. When strong, end-to-end encryption was rolled-out, the companies often declined to make it a by-default option. It was the case with Facebook Messenger, Microsoft's Skype or Google's Allo. An FBI source reacted to the launch of Allo by saying that "having [strong encryption] as an opt-in feature is certainly useful to us" (as quoted in Nakashima and Tsukayama 2016). Even when they are used by default, the strong encryption features like those deployed by Facebook on WhatsApp only encrypt the content of communications, not the metadata (who communicates with whom, when, from where, etc.). In other words, these deployments still allowed companies to mine metadata so as to monitor their users' behaviour and serve them with targeted advertising. Of course, such metadata can be, and frequently is, handed over to law enforcement (e.g. Biddle 2016; Fox-Brewster 2017).

Looking at these developments, some scholars have argued that the spread of encryption on Big Tech's infrastructures – which, according to NSA officials, had a significant inhibiting effect on the surveillance capabilities of law enforcement and intelligence agencies (McLaughlin 2016) – can be seen as a way of ensuring that the surveillance of users' communication could only happen with the companies' knowledge and consent, thereby reinforcing their position in the security field (Rubinstein and Van Hoboken 2014).

These shortcomings may primarily be driven by business considerations, rather than result from direct negotiations between Big Tech and the security field. But in mid-2015, a White House memo on encryption contemplated the possibility of "voluntary assistance," possibly in a "private" way to avoid the chilling effects that publicity might have on such cooperation (US National Security Council 2015). Since then, US intelligence and its allies have indeed exerted more quiet pressure to boost cooperation (e.g. Sanger and Frenkel 2018). We also know from the Snowden archives that prior to 2013, the NSA spent $250 million a year to work with tech companies to make commercial software – and in particular encryption software – more exploitable (Ball, Borger, and Greenwald 2013).

Surveillance reform and the Snowden paradox

When it comes to legal and political resistance staged by Big Tech, 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 has led to what we have called the "Snowden paradox" (Tréguer 2017): 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 decreasing the level of secrecy to secure their legality and legitimacy.

In the US, the most important piece of legislation in this respect was the USA Freedom Act, passed in June 2015. Rather than allowing the NSA to collect and store domestic telephone records in bulk, the legislation effectively gives that authority to telecommunication providers (who will have to query their own databases with selectors provided by the NSA and hand over the matching data). In no way did this stop the growth of large-scale surveillance conducted by US intelligence. According to the reports published by the Office of the Director of National Intelligence in 2017 and 2018, the amount of data collected by the NSA has surged since 2013 (Gallagher 2017; Volz 2018), including the data collected from Big Tech (according to the Google Transparency Report, by virtue of the Foreign Intelligence Surveillance Act, it provided data on 14,000 user accounts in the first semester of 2013; in the first half of 2017, that number rose to more than 48,500 accounts – a 350% increase). Even legislative changes allowing companies to ask a judge to review gag orders attached to surveillance requests (preventing any public disclosure on the existence of such requests) have since been selectively used by companies like Google and Facebook, leading to criticisms from human rights organisations (Cardozo 2017).

In France, US tech companies' push for surveillance reform originally acted in a much more antagonist environment, partly resulting from existing public-private alliances with French telecom and defence firms and from repeated calls in favour of "digital sovereignty" by decreasing the dependency of the French security field on US companies. In fact, Big Tech's 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 more discreet forms of engagement when France expanded the surveillance powers of its intelligence agencies through this new legislation. As for the amount of data provided by Big Tech to the French police and judiciary in the past years, it has also sharply increased, in part due to a better compliance rate after a "group of contact" was established between technology companies and the Ministry of the Interior in 2015 (Cassini 2015). In the first half of 2013 (January–June), Google was served with 2,011 requests by French authorities (it complied with 49 % of them); Facebook was served with 1,547 requests (39 % compliance rate). In the first half of 2017, Google received 5,661 requests (it complied with 63 % of them); Facebook, 4,700 requests (74%). In four years, that makes for a 360% and 570% increase in the number of requests for which some data was produced, respectively.

Controlling data flows: A "fundamental shift" in "scale and nature"

After 2015 and save for a few exceptions, the influence of the human rights field on the global debate on surveillance reform withered along with media attention to state surveillance issues. Through securitisation discourses – where securitisation refers to speech acts calling for urgent and exceptional measures to deal with the terrorist threat (Buzan and Wæver 2003, 491) – the security agenda became dominated by the terrorist threat. This led to new calls on the part of the security field to limit encryption, boost surveillance capabilities, and fight against terrorist propaganda on online networks, often with the threat of new legislation and criminal sanctions if the companies failed to cooperate. In this context, similar trends towards greater cooperation materialised both in the US and Europe, suggesting strong transnational field effects across the Atlantic (Bigo 2016). Two topics are particularly illustrative.

One area of cooperation that will help increase the already impressive growth in data requests sent to Big Tech companies are ongoing reforms around extraterritorial access to data. In March 2017, US President Donald Trump signed into law the CLOUD Act. This piece of legislation – first presented by the Department of Justice in mid-2016 – was added at the last minute to a spending bill to revise the legal framework regulating US law enforcement access to online data stored overseas as well as access to data by foreign law enforcement authorities to data held in the US.

The goal is to provide a streamlined legal avenue to bypass the often long and tedious procedures of international judicial cooperation provided by Mutual Legal Assistance Treaties (MLATs) (Vergnolle 2017) while clarifying

the extra-territorial effects of US law. With the CLOUD Act, if a country is deemed by the US government to have an adequate legal framework for surveillance, a bilateral agreement will be concluded giving to that country the possibility to directly send surveillance requests to US companies, without having to go through the US judiciary, even when the data is stored in the US. Conversely, US law enforcement agencies will be able to request any user data from US companies, regardless of the nationality of targeted persons and regardless of where the data is stored.

Drafted and passed with wide-ranging support from the tech sector (Smith B, 2018; Walker 2017), the CLOUD Act further entrenches the privatisation of the justice system for regulating trans-border data flows. As a result of this legislation, tech companies who receive requests from a third country will be the only ones able to oppose these requests; with MLAT procedures, the whole process would have been supervised by foreign and US judges. It also gives new leverage to the US government – i.e. whether or not to conclude a bilateral agreement with foreign governments to give them direct access to the data troves of US companies – which may be abused 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 legislation reaped with ambiguities (Singh Guiliani and Shah 2018; Wong 2017). In Europe, the adoption of the CLOUD Act was immediately followed by a proposal for a "directive on electronic evidence" aimed at enacting similar rules. Both initiatives could quickly expand worldwide through an ongoing revision of the Convention on Cybercrime of the Council of Europe.

In both the US and Europe, another hot topic has been that of terrorist propaganda, and the intensifying pressure put on online service providers to police such speech. Since the Paris attacks of 2015 and a visit of the French Minister of the Interior to Silicon Valley, France has been the European leader in this push toward privatised censorship, which was quickly taken up at the level of the European Union. The European Commission and Europol have convened regular meetings to get online platforms to sign a code on hate speech in 2016. 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).
>
> *(Europol 2016, 4)*

The US government followed suit in February 2016, when US Cabinet members and intelligence officials also met with tech companies. At the time, the White

House press secretary 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" (as quoted in Jose and California 2016). A key aspect of the discussions laid in understanding how technology could be used to boost censorship of terrorist propaganda and so-called counter-discourse. 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 could not do considering the "First amendment" issues raised by such policies (Menn and Volz 2016).

Of course, online censorship represents 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; and on Facebook, every day, 510,000 comments are posted, 293,000 statuses are updated, and 136,000 photos are uploaded. So besides hiring thousands of content-moderators, often through subcontractors based in low-wage countries where basic social rights are discarded (Roberts 2016), these efforts have led to significant investment in tools based on "Machine Learning" systems aimed at censoring terrorist-related content.

As the British Prime Minister Theresa May, explained at UN General Assembly in New York in September 2017:

> 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.
>
> *(as quoted in Hope and McCann 2017)*

A year later, in September 2018, the European Commission was announcing a proposal for transcribing the extra-judicial and automated mechanisms experimented over the past years into EU law.

What is happening here, with these moves around extra-territorial access to data or the censorship of terrorist propaganda, is a major reconfiguration of security assemblages tasked with the management of data flows and stocks, as new actors, technologies and regulations become necessary for the state to handle the surge in public and private communications entailed by digital technologies and keep its traditional techniques of power afloat. But the more we look at these new security assemblages involving Big Tech, the more we start to understand that they are but a sign of a broader reconfiguration of bureaucracies in the digital age.

Bureaucracies in the age of data governance

In her work on neo-liberal bureaucratisation, Béatrice Hibou has shown how, from the 1970s on, the logic of management migrated from the private realm to state

institutions (Hibou 2015). Through imperatives of "efficiency", "cost-effectiveness", "flexibility" and through practices of "auditing", and "benchmarking", bureaucratic practices within public administrations grew increasingly hostile to the post-war social values embedded in the public sector. With the so-called "New Public Management," the abstract principles of neoliberalism were pushed so far as to cause a complete divorce between "efficiency" and the ends that state bureaucracies were supposed to pursue (Graeber 2015).

If, according Hibou, bureaucracy is seen "as a power concentrated in the hands of those who create the validated abstractions and put them at the core of government" (p. 86), it looks like Big Tech may fast be dominating the whole administrative field. Zuboff (2015) and others trace back the origin of this diffusion of power to Google's popularisation of "data governance", referring to bureaucratic models based on "data extraction and analysis", "new contractual forms due to better monitoring", "personalization and customization", and "continuous experiments" championed by Google's chief economist (Varian 2010, 2014). They were later relayed in the book *How Google Works?* (2015), authored by Eric Schmidt, Executive Chairman of Google/Alphabet from 2001 to 2017 and still a board member today, and Jonathan Rosenberg, a former Senior Vice President of Products at Google. In this book, the pair document business management lessons from Google, an experience that led them to "relearn everything" they knew through data-intensive models.

Data means knowledge means hard power

After having contributed to the shaping of US Internet diplomacy under the tenure of former Secretary of State Hillary Clinton (Assange 2014; Powers and Jablonski 2015; Schmidt and Cohen 2013), Eric Schmidt has been the most visible agent of a crowd of current and former "Googlers" helping spread these models at the heart of the US military-industrial complex. In March 2016, Schmidt was appointed by the Secretary of Defense as chairman of the Defense Innovation Board (DIB). A position as advisor to the Pentagon that he still holds at the time of writing despite him quitting his official positions at Alphabet/Google in January 2018. 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 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.
>
> *(DIB 2017)*

In one of its recommendations entitled "Forge New Approach to Data Collection, Sharing, and Analysis", the DIB insists on the importance of data to 21st 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 organises 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.
>
> *(DIB 2017)*

Companies like Google and their executives are selling solutions aimed at expanding the technological superiority and "efficiency" of security bureaucracies. According Scott Frohman, Google's Director of Defense and Intelligence Sales, Big Tech can bring these "radical innovations" at "ultra-low cost." "Through the use of Google's capabilities remade for the enterprise," he writes on his LinkedIn profile, "the government gets innovation fast and with significantly reduced cost" (Frohman 2018).

The "Startup Nation" as a new bureaucratic paradigm

These trends go beyond the security field and expand to virtually all public policies. The integration of Big Tech in the administrative and political fields has been going on for at least a decade. It vastly expanded under the Obama administration, with over 251 individuals changing position between Google or related firms and the federal government, national political campaigns and Congress ('Google's Revolving Door (US)' 2017).

Under Trump, it may look different on the surface. For one thing, the tech industry has voiced strong criticism of his immigration and climate policies (Streitfeld, Isaac and Benner 2017). Big Tech workers have also played an important role in denouncing Google's participation to drone warfare. At Microsoft they opposed a $19.4 million contract with US Immigration and Customs Enforcement (ICE), while Amazon was criticised for selling facial recognition technologies to US police forces. Trump has of course "trolled" Big Tech, for instance by accusing them of censoring conservative views online (Swisher 2018).

But in the back rooms, it looks like business as usual. In a memorandum signed in late-March 2017 creating the "American Technology Council," Donald Trump opened new channels for sustaining the reciprocal influence between the tech industry and the US government. The initiative is overseen by his son-in-law and Senior Advisor Jared Kushner and seeks to "modernize" the US public sector. Discussions have touched on how to make public procurement more flexible, cut

down on some 6,000 government-owned data centres by shifting those responsibilities to the private sector, or on the release government-held data on a range of issues, particularly on health care, for private-sector use (Romm 2017).

In France too, where a lot of revolving door activity is also happening ("Google's European Revolving Door" 2016; Léchenet 2017), the debate on the "reform of the state" has moved from the premises of the New Public Management to those of data governance. By coining terms like "Startup Nation" – an expression championed by French President Emmanuel Macron – or the "Platform State," today's reformers are re-modelling bureaucracies and decision-making processes around the need to produce massive amounts of data, make it available and usable, maintain its integrity and feed it to powerful data-processing tools that will be used to "optimise" bureaucratic outputs (e.g. Algan and Cazenave 2016; Bertholet and Létourneau 2017; Pezziardi and Verdier 2017). Even when these reformist discourses claim to be opposing the hegemony of US tech companies, they are in fact assuming the superiority of their models 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).

Despite calls of security insiders and state reformers to establish "digital sovereignty," the products and services of US tech firms continue to have an irresistible appeal. In 2017, a contract between Microsoft and the French Ministry of Defence was signed despite widespread criticism. A year earlier, the DGSI, France's domestic intelligence, contracted Palantir, a Big Data analytics firm very close to US intelligence, to mine the vast amount of data seized during house raids and digital seizures authorised under the state of emergency post-November 2015 (Tesquet 2017).

As this latter example suggests, new security assemblages do not only embark large tech firms used daily by billions of Internet users. Many small companies specialised in data analytics or vulnerabilities are also partnering with intelligence agencies to sell their products and services (Deibert 2013). Older tech and utility companies in the defence, transportation or energy sectors are also trying to catch up by investing in Big Data analytics – sometimes in partnership with their US competitors like IBM to secure access to key technologies – and are fast-developing solutions for Big Data policing, just as local elected officials hope to get votes by framing these new programs as advancing the project of a "Smart City."

The Government Machine and the rule of law

Such trends towards technical, managerial and technological responses to security challenges have been sweeping the modern security field for quite some time now (Abrahamsen and Williams 2010; Bonelli 2010). But as Big Tech becomes part of the state and now serves the "Government Machine" (Agar 2003), we might be reaching a tipping point in the history of governmentality.

That being said, political theory suggests that the blurring public-private distinction is a feature of state power, not a bug. According to Timothy Mitchell, we need to see the state not "as a free-standing entity, whether an agent, instrument,

organisation 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 (Mitchell 1991, 94). 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." Rather, "producing and maintaining the distinction between state and society is itself a mechanism that generates resources of power."

The "Big Tech vs. the Surveillance State" narrative emphasises that distinction. Post-2013, it served to counter that put forward by Snowden and journalists working on his disclosures of unabated and extra-legal cooperation. It helped reassure Internet users that these companies worked to protect their rights and resisted the state on their behalf. But soon enough, through more discreet moves, the state-private distinction was again crushed when, to effectively control communications and avoid investing resources in the justice system, security professionals co-opted Big Tech and their censorship and surveillance techniques for their own ends. Such double-dealings are still ongoing.

Towards hybrid rule

Through public-private hybridisation, it becomes easier for governments to escape the important safeguards that our legal systems have developed over time to protect political rights, but which are apparently ill-suited (or at least too costly) to accommodate the surge in communications entailed by digital technologies. In this way, "political elites (. . .) rely on the private sector to shield national security activities," thus "expanding state power while constraining democratic accountability" (Hurt and Lipschutz 2015, 2).

This was in part a deliberate strategy first envisioned in the mid-1990s, when security professionals – in particular at the Pentagon – feared the consequence of the compression of time and space induced by digital networks and sought for new ways of enacting state power. The result was the formulation of new doctrines and practices whereby "the military and law enforcement, the government and private industry, and domestic and foreign surveillance would necessarily mix in ways long seen as illicit if not illegal" (Jones 2017, 13). It followed that "constitutional interpretation, jurisdictional divisions, and the organisation of bureaucracies alike would need to undergo dramatic – and painful – change."

As we have seen, part of such change resides in automation and extra-judicialisation,which both lead to a profound shift in the history of the justice system. In his 1971–1972 lectures at the Collège de France, Foucault explained how, from the 14th century on, the old feudal institution of Parliaments was gradually co-opted by the Crown and entrusted with investigative powers (Foucault 2018). To assert its power without having to bear the costs of military occupation, the Prince relied on Parliaments to interrogate people, to make them say what they knew so as to produce knowledge on the basis of which he would adjudicate and eventually govern "his" territory and the population.

In today's computerised world, the legal restrictions of state power that were progressively coded into the justice system are radically overtaken by "data governance." Digital traces form the basis of a new statistical power-knowledge that is seen as the most effective and cost-efficient way of governing the natural and social worlds. In the process, the legal norms and principles which somewhat circumscribed the power of the Prince get lost in computer code. Once it has morphed into algorithms, power becomes even more diluted and harder to challenge (Rouvroy, 2012). Can we even reasonably hope to make these ever more complex algorithms auditable, and their designers accountable, when experts in "Deep Learning" and "Neural Networks" say that even they cannot understand how these increasingly unpredictable systems work (Knight 2017; Smith, A. 2018)?

Stopping the machine?

That begs the question of how best to challenge these new security assemblages.

For one thing, it is worth stressing that Big Data bureaucracies might not be that good at doing what they are supposed to. We can therefore oppose the arguments of those legitimising these new governance models on the grounds of accuracy and reliability. There are reasons – and growing evidence – to doubt that the new "regimes of truth" championed by "Big Data security assemblages" will in any meaningful way provide solutions to security issues (Aradau and Blanke 2015). Technological solutionism in the age of data governance, bolstered by marketing discourses, 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. After all, history tells us, bureaucracies tend to fail. By disregarding "all the subtleties of real social existence," "reducing everything to preconceived mechanical or statistical formulae," bureaucratic dispositifs like "forms, rules, statistics, or questionnaire" – even when fuelled by complex algorithms and troves of data –, remain abstract simplifications that might only reinforce the forms of structural violence they are said to alleviate or even solve (Graeber 2015, p. 75; see also Eubanks 2018, O'Neil 2016).

Bureaucracies often fail to meet their alleged goals but still, they strengthen the power of those who invest in them. They transform the social world and can go awfully wrong (Scott 1998). If, following Tim Mitchell and critical security scholars, we refuse to "see the state and private organizations as a single, totalized structure of power," another complementary way of resisting these assemblages is to build on the conflicts that inevitably occur "between different government agencies, between corporate organizations, and within each of them" (Mitchell 1991, 90). We can amplify the words of those who denounce the oppressive and manipulative use of modern computer technologies, applaud tech workers opposing the direct involvement of their company in the military-industrial complex, or support security professionals seeking to automate intelligence oversight so as to catch up with large-scale surveillance systems and mitigate abuse. We can, and we should.

But post-Snowden controversies also show that these forms of resistance create a risk that we will overlook the pervasiveness of the institutions and technologies, of the rationalities and practices that created the problem in the first place. The risk is that all we are able to come up with are legal, technological or bureaucratic fixes to try to contain the most disturbing aspects of data-driven bureaucracies, without affecting the longer-term trend of a technological arms race that only seems to intensify the issues it was allegedly meant to solve.

Some kind of deeper resistance might be warranted. In his writings on power, Foucault once asked: "How can the growth of capabilities" – and he explicitly mentioned "techniques of communication – "be disconnected from the intensification of power relations?" (Foucault 1984, 48). Computing technologies have since become immensely powerful and yet, we are still struggling to find a satisfactory answer to this crucial question. Despite the hopes of early hackers and Internet pioneers, the decoupling of technology and power is not happening. The key question then becomes whether technology itself or law or ethics can actually be effective instruments to achieve such decoupling.

At this stage of technological development, if we feel like they cannot – at least not in the near foreseeable future – that means it is probably time to refocus on tackling the imaginaries and institutions that underlie the "growth of capabilities" itself: the blind faith in technological progress; the oft-repeated mantra that technology is neutral, that its negative potential will somehow be contained; places like the universities, R&D labs, ministries, start-ups, shops and factories where complex and powerful technologies are designed, produced and traded. As philosopher Jacques Ellul observed, "we set huge machines in motion in order to arrive nowhere" (Ellul 1989, 51). If it is not Thomas More's eu-topia ("no place") that we are fast approaching but rather a "dystopian void" (The Luddbrarian 2018), what we need is not just a technological fix, a bureaucratic patch, a principled law or even a good ethics; what we need first and foremost is to get off and stop the machine.

References

Abrahamsen, Rita, and Anna Leander. 2015. *Routledge Handbook of Private Security Studies*. Routledge.

Abrahamsen, Rita, and Michael C. Williams. 2010. *Security Beyond the State: Private Security in International Politics*. Cambridge University Press.

Agar, Jon. 2003. *The Government Machine: A Revolutionary History of the Computer*. MIT Press.

Algan, Yann, and Thomas Cazenave. 2016. *L'Etat en mode start-up*. Eyrolles.

Aradau, Claudia, and Tobias Blanke. 2015. 'The (Big) Data-Security Assemblage: Knowledge and Critique'. *Big Data & Society* 2 (2). 1–12.

Assange, Julian. 2014. *When Google Met Wikileaks*. OR Books. https://www.orbooks.com/catalog/when-google-met-wikileaks/.

Ball, James, Julian Borger, and Glenn Greenwald. 2013. 'Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security'. *The Guardian*, 6 September 2013, sec. World news. http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

Barbrook, Richard, and Andy Cameron. 1995. 'The Californian Ideology'. *Mute* 1 (1): 44–72.

Barty-King, Hugh. 1980. *Girdle Round the Earth: History of Cable and Wireless*. Heinemann.

Bellamy Foster, John, and Robert W. McChesney. 2014. 'Surveillance Capitalism: Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age'. *Monthly Review* 66 (3). http://monthlyreview.org/2014/07/01/surveillance-capitalism.

Beniger, James R. 1986. *The Control Revolution: Technological and Economic Origins of the Information Society*. Harvard University Press.

Bertholet, Clément, and Laura Létourneau. 2017. *Ubérisons l'État! Avant que d'autres ne s'en chargent*. Armand Colin.

Biddle, Sam. 2016. 'Apple Logs Your IMessage Contacts—and May Share Them with Police'. *The Intercept*. 28 September 2016. https://theintercept.com/2016/09/28/apple-logs-your-imessage-contacts-and-may-share-them-with-police/.

Bigo, Didier. 2016. 'Sociology of Transnational Guilds'. *International Political Sociology* 10 (4): 398–416.

Black, Edwin. 2012. *IBM and the Holocaust: The Strategic Alliance Between Nazi Germany and America's Most Powerful Corporation*. Expanded edition. Washington, DC: Dialog Press.

Bonelli, Laurent. 2010. 'Les modernisations contradictoires de la police nationale'. In *L'État démantelé*, 102–17. La Découverte.

Buzan, Barry, and Ole Wæver. 2003. *Regions and Powers: The Structure of International Security*. Cambridge University Press.

Cardozo, Nate. 2017. 'Requiring Judicial Review for Every Gag Order Is a Simple Way to Have Our Backs: Apple Does but Google and Facebook Fall Short'. *Electronic Frontier Foundation*. 10 July 2017. www.eff.org/deeplinks/2017/07/requiring-judicial-review-every-gag-order-simple-way-have-our-backs-apple-does.

Cassini, Sandrine. 2015. 'Terrorisme: Accord Entre La France et Les Géants Du Net'. *Les Échos*. 23 April 2015. www.lesechos.fr/journal20150423/lec2_high_tech_et_medias/02124922454-terrorisme-accord-entre-la-france-et-les-geants-du-net-1113723.php.

Charbon, Paul. 1991. 'Genèse du vote de la loi de 1837, origine du monopole des télécommunications'. In *L'État et les télécommunications en France et à l'étranger*, 18371987, edited by Catherine Bertho-Lavenir, 11–22. Actes du colloque organisé à Paris les 3 et 4 novembre 1987 par l'Ecole pratique des hautes études et l'Université René Descartes. Librairie Droz.

Deibert, Ronald J. 2013. *Black Code: Inside the Battle for Cyberspace*. Random House.

Desrosières, Alain. 2002. *The Politics of Large Numbers: A History of Statistical Reasoning*. Translated by Camille Naish. Harvard University Press.

DIB. 2017. 'Recommendations'. *Defense Innovation Board*. 2017. https://innovation.defense.gov/Recommendations/.

Edwards, Paul N. 1996. *The Closed World: Computers and the Politics of Discourse in Cold War America*. MIT Press.

Ellul, Jacques. 1989. The Presence of the Kingdom. 2nd edition. Helmers & Howard Publishing.

Eubanks, Virginia. 2018. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press.

Europol. 2016. 'EU Internet Referral Unit – YEAR ONE REPORT'. *Europol*. www.europol.europa.eu/content/eu-internet-referral-unit-year-one-report-highlights.

Flichy, Patrice. 2009. *Dynamics of Modern Communication: The Shaping and Impact Of New Communication Technologies*. SAGE.

Foucault, Michel. 1984. 'What Is Enlightenment?' In *The Foucault Reader*, edited by Paul Rabinow. Pantheon Books.

———. 2018. *Penal Theories and Institutions: Lectures at the Collège de France*, 1971–1972. Translated by Graham Burchell. 1st edition. 2018 edition. Palgrave Macmillan.

Fox-Brewster, Thomas. 2017. 'Forget About Backdoors, This Is the Data WhatsApp Actually Hands to Cops'. *Forbes*. 22 January 2017. www.forbes.com/sites/thomasbrewster/2017/01/22/whatsapp-facebook-backdoor-government-data-request/.

Frohman, Scott. 2018. 'Scott Frohman LinkedIn Profile'. *LinkedIn*. 2018. https://www.linkedin.com/in/scottatsas/.

Fuchs, Christian, and Daniel Trottier. 2015. 'Towards a Theoretical Model of Social Media Surveillance in Contemporary Society'. *Communications-European Journal of Communication Research* 40 (1): 113–35.

Gallagher, Sean. 2017. 'US Intelligence "Transparency Report" Reveals Breadth of Surveillance by NSA, Others'. *Ars Technica*. 3 May 2017. https://arstechnica.com/tech-policy/2017/05/us-intelligence-transparency-report-reveals-breadth-of-surveillance-by-nsa-others/.

Galloway, Alexander R. 2004. *Protocol: How Control Exists after Decentralization*. MIT Press.

Girard, René. 2002. 'What Is Happening Today Is Mimetic Rivalry on a Global Scale'. *South Central Review* 19 (2/3): 22–27.

'Global Top 100 Companies by Market Capitalisation (31 March 2017 Update)'. 2017. https://www.pwc.com/gx/en/audit-services/assets/pdf/global-top-100-companies-2017-final.pdf.

Goldsmith, Jack, and Tim Wu. 2006. *Who Controls the Internet?: Illusions of a Borderless World*. Oxford University Press.

'Google's European Revolving Door'. 2016. *Google Transparency Project*. 2016. https://googletransparencyproject.org/articles/googles-european-revolving-door.

'Google's Revolving Door (US)'. 2017. *Google Transparency Project*. 2017. https://googletransparencyproject.org/articles/googles-revolving-door-us.

Graeber, David. 2015. *The Utopia of Rules: On Technology, Stupidity, and the Secret Joys of Bureaucracy*. Melville House.

Haggerty, Kevin D., and Richard V. Ericson. 2000. 'The Surveillant Assemblage'. *British Journal of Sociology* 51 (4): 605–22.

Harcourt, Bernard E. 2015. *Exposed - Desire and Disobedience in the Digital Age*. Harvard University Press.

Harris, Shane. 2014. *@War: The Rise of the Military-Internet Complex*. Eamon Dolan/Houghton Mifflin Harcourt.

Headrick, Daniel R. 2012. *The Invisible Weapon: Telecommunications and International Politics, 1851–1945*. Reprint. Oxford University Press, USA.

Hibou, Béatrice. 2015. *The Bureaucratization of the World in the Neoliberal Era*. Palgrave MacMillan.

Hope, Christopher, and Kate McCann. 2017. 'Google, Facebook and Twitter Told to Take down Terror Content within Two Hours or Face Fines'. *The Telegraph*, 19 September 2017. https://www.telegraph.co.uk/news/2017/09/19/google-facebook-twitter-told-take-terror-content-within-two/.

Hurt, Shelley, and Ronnie Lipschutz, eds. 2015. *Hybrid Rule and State Formation: Public-Private Power in the 21st Century*. 1st edition. Routledge.

Jones, Matthew L. 2017. 'The Spy Who Pwned Me'. *Limn*, no. 8 (June). http://limn.it/the-spy-who-pwned-me/.

Jose, Danny Yadron Julia Carrie Wong in San, and California. 2016. 'Silicon Valley Appears Open to Helping US Spy Agencies after Terrorism Summit'. *The Guardian*, 8 January 2016, sec. Technology. http://www.theguardian.com/technology/2016/jan/08/technology-executives-white-house-isis-terrorism-meeting-silicon-valley-facebook-apple-twitter-microsoft.

Knight, Will. 2017. 'There's a Big Problem with AI: Even Its Creators Can't Explain How It Works'. *MIT Technology Review*. 11 April 2017. https://github.com/alphoenix/donnees/tree/master/lobbies-gafamut.

Léchenet, Alexandre. 2017. 'L'influence Tentaculaire Des Géants Américains'. https://github.com/alphoenix/donnees.

Lécuyer, Christophe. 2007. *Making Silicon Valley: Innovation and the Growth of High Tech, 1930–1970*. MIT Press.

Levine, Yasha. 2018. *Surveillance Valley: The Secret Military History of the Internet*. PublicAffairs.

Luddbrarian, The. 2018. 'Challenging the Tech Companies from Within'. LibrarianShipwreck, 28 June 2018. https://librarianshipwreck.wordpress.com/2018/06/28/challenging-the-tech-companies-from-within/.

McLaughlin, Jenna. 2016. 'Spy Chief Complains That Edward Snowden Sped Up Spread of Encryption by 7 Years'. *The Intercept*. 25 April 2016. https://theintercept.com/2016/04/25/spy-chief-complains-that-edward-snowden-sped-up-spread-of-encryption-by-7-years/.

Menn, Joseph, and Dustin Volz. 2016. 'Exclusive: Google, Facebook Quietly Move toward Automatic Blocking of Extremist Videos'. *Reuters*, 25 June 2016. www.reuters.com/article/us-internet-extremism-video-exclusive-idUSKCN0ZB00M.

Mills, C. Wright. 1959. *The Power Elite*. Oxford University Press.

Mitchell, Timothy. 1991. 'The Limits of the State: Beyond Statist Approaches and Their Critics'. *The American Political Science Review* 85 (1): 77.

Morozov, Evgeny. 2013. *To Save Everything, Click Here: The Folly of Technological Solutionism*. PublicAffairs,U.S.

Nakashima, Ellen, and Hayley Tsukayama. 2016. 'Why People like Edward Snowden Say They Will Boycott Google's Newest Messaging App'. *Washington Post*. 21 May 2016. www.washingtonpost.com/news/the-switch/wp/2016/05/21/why-people-like-edward-snowden-say-they-will-boycott-googles-newest-messaging-app/.

Nesbit, Jeff. 2017. 'Google's True Origin Partly Lies in CIA and NSA Research Grants for Mass Surveillance'. *Quartz*. 8 December 2017. https://qz.com/1145669/googles-true-origin-partly-lies-in-cia-and-nsa-research-grants-for-mass-surveillance/.

O'Neil, Cathy. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown.

Pezziardi, Pierre, and Henri Verdier. 2017. *Des startups d'État à l'État plateforme*. CreateSpace Independent Publishing Platform.

Powers, Shawn M., and Michael Jablonski. 2015. *The Real Cyber War: The Political Economy of Internet Freedom*. 1st edition. University of Illinois Press.

Roberts, Sarah T. 2016. 'Commercial Content Moderation: Digital Laborers' Dirty Work'. In *The Intersectional Internet: Race, Sex, Class, and Culture Online*, edited by Brendesha M. Tynes and Safiya Umoja Noble, 147–60. Peter Lang Publishing.

Rogers, Michael, and Grace Eden. 2017. 'The Snowden Disclosures, Technical Standards, and the Making of Surveillance Infrastructures'. *International Journal of Communication* 11 (0): 22.

Romm, Tony. 2017. 'Behind the Scenes at President Trump's Private Talks with the Tech Industry'. *Recode*. 20 June 2017. www.recode.net/2017/6/20/15838646/trump-apple-amazon-google-microsoft-tech-week.

Rouvroy, Antoinette. 2012. 'The End(s) of Critique: Data-Behaviourism vs. Due-Process'. In *Privacy, Due Process and the Computational Turn*. Routledge. http://works.bepress.com/antoinette_rouvroy/44.

Rubinstein, Ira, and Joris Van Hoboken. 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.

Sanger, David E., and Sheera Frenkel. 2018. '"Five Eyes" Nations Quietly Demand Government Access to Encrypted Data'. *The New York Times*. 5 September 2018. www.nytimes.com/2018/09/04/us/politics/government-access-encrypted-data.html.

Scott, James C. 1998. *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*. Yale University Press.

Schmidt, Eric, and Jared Cohen. 2013. *The New Digital Age: Transforming Nations, Businesses, and Our Lives*. Knopf Doubleday Publishing Group.

Schmidt, Eric, and Jonathan Rosenberg. 2015. *How Google Works*. London: John Murray.

Singh Guiliani, Neema, and Naureen Shah. 2018. 'The CLOUD Act Doesn't Help Privacy and Human Rights: It Hurts Them'. *Lawfare*. 16 March 2018. https://lawfareblog.com/cloud-act-doesnt-help-privacy-and-human-rights-it-hurts-them.

Smith, Andrew. 2018. 'Franken-Algorithms: The Deadly Consequences of Unpredictable Code', *The Guardian*, 30 August 2018. www.theguardian.com/technology/2018/aug/29/coding-algorithms-frankenalgos-program-danger.

Smith, Brad. 2018. 'The CLOUD Act Is an Important Step Forward, but Now More Steps Need to Follow'. *Microsoft on the Issues* (blog). 3 April 2018. 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/.

Statista. 2018. 'Most Valuable Companies in the World 2018'. May 2018. www.statista.com/statistics/263264/top-companies-in-the-world-by-market-value/.

Streitfeld, David, Mike Isaac, and Katie Benner. 2017. 'Silicon Valley's Ambivalence Toward Trump Turns to Anger'. *The New York Times*, 29 January 2017. https://www.nytimes.com/2017/01/29/technology/silicon-valleys-ambivalence-toward-trump-turns-to-anger.html.

Swisher, Kara. 2018. 'Trump's Ludicrous Attack on Big Tech'. *The New York Times*. 30 August 2018. www.nytimes.com/2018/08/29/opinion/trump-bias-google-twitter.html.

Tesquet, Olivier. 2017. 'Palantir, l'encombrant Ami Américain Du Renseignement Français'. 27 January 2017. www.telerama.fr/medias/palantir-big-data-renseignement,153229.php.

Tréguer, Félix. 2017. 'Intelligence Reform and the Snowden Paradox: The Case of France'. *Media and Communication* 5 (1): 17–28.

Tréguer, Félix. 2018. 'US Technology Companies and State Surveillance in the Post-Snowden Context: Between Cooperation and Resistance'. *UTIC Deliverable* 5. Paris: CERI. https://halshs.archives-ouvertes.fr/halshs-01865140.

Turner, Fred. 2006. *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. University of Chicago Press.

US National Security Council. 2015. 'Draft Options Paper on Strategic Approaches to Encryption'. Washington DC. http://apps.washingtonpost.com/g/documents/national/read-the-nsc-draft-options-paper-on-strategic-approaches-to-encryption/1742/.

Varian, Hal R. 2010. 'Computer Mediated Transactions'. *American Economic Review* 100 (2): 1–10.

Varian, Hal R . 2014. 'Beyond Big Data'. *Business Economics* 49 (1): 27–31.

Vergnolle, Suzanne. 2017. 'Understanding the French Criminal Justice System as a Tool for Reforming International Legal Cooperation and Cross-Border Data Requests'. *Georgia Tech Scheller College of Business Research Paper*. Data Protection, Privacy and European Regulation in the Digital Age. https://papers.ssrn.com/abstract=2921364.

Volz, Dustin. 2018. 'Spy Agency NSA Triples Collection of U.S. Phone Records: Official . . .'. Reuters, 8 May 2018. www.reuters.com/article/us-usa-cyber-surveillance/spy-agency-nsa-collected-500-million-u-s-call-records-in-2017-a-sharp-rise-official-report-idUSKBN1I52FR.

Walker, Kent. 2017. 'Digital Security and Due Process: A New Legal Framework for the Cloud Era'. *Google*. 22 June 2017. www.blog.google:443/topics/public-policy/digital-security-and-due-process-new-legal-framework-cloud-era/.

Webb, Jen, Tony Schirato, and Geoff Danaher. 2002. *Understanding Bourdieu*. SAGE.

Williams, Michael C. 2010. 'The Public, the Private and the Evolution of Security Studies'. *Security Dialogue* 41 (6): 623–30.

Wong, Cynthia M. 2017. 'US Cross-Border Data Deal Could Open Surveillance Floodgates'. *Human Rights Watch*. 18 September 2017. www.hrw.org/news/2017/09/18/us-cross-border-data-deal-could-open-surveillance-floodgates.

Zuboff, Shoshana. 2015. 'Big Other: Surveillance Capitalism and The Prospects of an Information Civilization'. *Journal of Information Technology* 30 (1): 75–89.