mediaLAWS
Law and Policy of the Media in a Comparative Perspective

Law and Media Working Paper Series

no. 8/2017

ANDREA SERENA

The Leviathan, the Chains, the Lock: Dynamics of Power in the Digital Surveillance State

SUMMARY: 1. Introduction – 2. The Leviathan – 3. The chains – 4. The lock – 5. Conclusion

1. *Introduction*

In 2013, Edward Snowden, a private contractor for the NSA, leaked to the press[1] how the US and its allies had been spying for years on individuals, companies and organisations in their own countries and abroad. On the one hand, these revelations acknowledged the undisputed role of digitalization and ICT in allowing the unparalleled depth and scope of this kind of mass surveillance, which ranges from interception of Internet traffic to remote control of devices. On the other hand, the implications of these new surveillance capabilities for the digital society of the future are still unclear. The ongoing debate will need to answer

[1] The Guardian published the story in a series of articles. For the first, see Greenwald, G. *NSA collecting phone records of millions of Verizon customers daily*. (2013) Available at: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (Accessed: 26th January 2016).

Law and Media Working Paper Series

Codice ISSN: 2531-484X

EDITORE: Oreste Pollicino - COORDINATORE EDITORIALE: Marco Bassini

SEDE: Via Roentgen, 1 – 20136 Milano e-mail: submissions@medialaws.eu

the legal, societal and economical concerns raised by this new phenomenon, such as the protection of civil rights in a surveillance state or the threats to cybersecurity of companies placed under surveillance.

The objective of this paper is to demonstrate how the digitally-connected society in which we live confers on network gatekeepers unprecedented capabilities of expanding or curtailing the executive power's scope of action, a role that has traditionally been held by the legislature, judiciary and civil activism only. Firstly, this essay describes the current legal framework surrounding surveillance in the US, highlighting the tendency of governments to exceed those limits. Secondly, it discusses the importance of the courts in overseeing such activities and in promoting legislative change. Thirdly, it assesses the effects of involving technology corporations in the dialectic between constitutional powers.

2. *The Leviathan*

The division of powers in Western democracies places the responsibility of assuring the safety of the nation on the executive, in accordance with the legal regime provided by the legislature. Most recently, mass surveillance has come to constitute the ultimate strategy developed by governments to fulfil that duty of public safety. Drawing on the American experience, the following shows how these new methods both create a new threat to the balance of constitutional powers, and how questionable is their effectiveness in assuring people's security.

A. The US

The National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) are the bodies respectively in charge of overseas and domestic surveillance. The following chapter

demonstrates how the limitations provided by law to such activities have been continuously surpassed by the U.S. Federal Government and its agents in the last decade.

The NSA is part of the military: it is in charge of protecting US government communications, and of collecting information and data for foreign intelligence purposes only. Following 9/11, the agency was secretly given the duty to engage in surveillance of domestic and overseas communications in order to help fight international terrorism.

Such activities would usually fall under the scope of the Fourth Amendment[2] and the relevant federal statutes,[3] which states that a citizen's private sphere can be violated only in the presence of a judicial warrant, provided that there is a probable cause and that the search is likely to be of use to the prosecution of a crime. However, as the NSA does not target U.S. citizens, a lower threshold applies, which has been framed in details by mainly the following three provisions:

- part 2.3 of the Executive Order 12333
- s.215 of the 2001 Patriot Act[4]
- s.702 of the 2008 FISA Amendments Act.

The background to all of them is the 1978 Foreign Surveillance Intelligence Act (FISA),[5] the Congress reaction to the executive excesses of the post-war era, such as COINTELPRO under Hoover's FBI. The Act was intended to control foreign intelligence activities through the establishment of a supervisory court, the Foreign Intelligence Surveillance Court (FISC), which issues warrants (FISA orders) applying a lower threshold than the Fourth Amendment, given the special nature of those investigations. The FISC, whose proceedings

[2] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[3] Broadly speaking, Rule 41 of the Federal Rules of Criminal Procedure and Omnibus Crime Control and Safe Streets Act of 1968 (42 U.S.C. § 3711). See also: *Katz v. United States*, 389 U.S. 347 (1967); *U.S. v. U.S. District Court* 407 U.S. 297 (1972).

[4] P.L. 107-56

[5] P.L. 95-511

are secret for reasons of national security, is in charge of authorising direct interceptions of an individual's communications or granting orders to compel third parties to collaborate with the ongoing investigations. For instance, such orders have been used to force ISPs and telecommunications providers to allow NSA's bulk data collection through their networks. Further, these warrants always contain a perpetual non-disclosure obligation (gag order), so that the subject of the surveillance will never be aware of it, inhibiting any kind of judicial recourse on the legality of these instruments.

The main requirement in order to obtain the court's approvals is that the surveillance is conducted with the *sole* purpose of gathering foreign intelligence. In the wake of the Twin Towers attacks, Congress passed the 2001 PATRIOT Act, which changed the word *sole* with *significant*, allowing the then Attorney-General J. Ashcroft to interpret the provision as if it now included in the FISA regime ordinary crimes investigations as well, which are not conducted by the NSA but by the FBI. As the FBI has both intelligence and crime prosecution tasks on behalf of the Federal Government, its officers apply both the FISA and Fourth Amendment thresholds, according to which kind of duty they are pursuing at the moment. Therefore, allowing the FBI prosecution branch to enjoy the exceptional FISA regime subverts the basic principles of the rule of law on which modern criminal law systems are rooted.[6]

For instance, National Security Letters (NSLs) practically allow the Bureau to engage in targeted and bulk surveillance under the same conditions as the NSA. Under s.505 of the Patriot Act, NSLs are warrantless administrative subpoena that order the third party to provide non-content data to the federal agent, and ban the former from disclosing the request to the subject targeted.

As a last example of how the U.S. government has misused the legal instruments provided by the legislature, in emergency situations the Attorney-General is granted the power to autonomously authorize governmental activities which normally fall under the

[6] On this matter, see *In re: Sealed Case No. 02-001*, 310 F.3d 717 (2002).

jurisdiction of the FISC. Following 9/11, the Attorney-General power has been frequently used despite its exceptional nature, subtracting from judicial oversight a number of intelligence programs whose intrusive character can threaten civil liberties and should have been made subject to the FISC at minimum. Donohue (2008)[7] reports that in 2002 Ashcroft only signed more than 170 of them.

The scenario laid out above needs to be put in context in order fully to understand the constitutional implications. Modern democracies have adopted the rule of law as a way of assuring that the government acts and enforces the law in accordance with civil rights, particularly in criminal matters. However, an extraordinary regime is usually put in place in the presence of special needs, such as intelligence activities for the protection of national security. In the US, governmental prosecution of crimes committed by US citizens is informed by Fourth Amendment case law, but NSA and FBI foreign intelligence operations are split out from it, allowing warrantless searches which only need to serve an investigation on international terrorism instead of satisfying the probable cause requirement.

The issue arising with mass surveillance programmes is that those searches, and the data obtained thereby, have been used to prosecute *common* criminals, from murderers to drug dealers, who should have been granted the protection of the Fourth Amendment. Furthermore, the sharing of data from the NSA and FBI *intelligence* branches to the FBI *criminal prosecution* branch contradicts settled case law, which requires a warrant even for domestic intelligence surveillance. Consequently, it is not that communications surveillance over suspects of a crime other than terrorism should be banned, but should be performed using a warrant, which defines the precise scope and modalities of the search, and is awarded by a court whose proceedings are public, allowing the defendant to resort to the same court to question the lawfulness of the issued warrant.

[7] Donohue, L. K. (2008) *The Cost of Counterterrorism. Power, Politics, and Liberty.* Cambridge: Cambridge University Press.

From the above, it can be concluded that the use of what should be exceptional tools, such as FISA orders and NSLs, in the prosecution of *common* crimes committed by US citizens, is a clear example of what we might term the 'natural' tendency of the executive to expand its powers beyond the limits of the law. In this case, such expansions have been successful because of the lack of the traditional safeguards, namely an independent judicial oversight, and a public debate which might prompt legislative change. As for independent oversight, either it is not required by law for NSLs, or it is fulfilled by the FISC, which only hears cases *ex parte* and has rejected only 11 out of 34,000 applications it has received since its formation in 1978 (Schneier: 2015). With regards to a public debate, the gag orders attached to these instruments prevent the press and the public from knowing the manner and scope of government surveillance, as violation of the ban is punishable with up to five years of imprisonment. In addition, targets are completely unaware of being put under surveillance, and are thus prevented from publicly challenging those practices before a competent court.

The effectiveness of the mass surveillance programs undertaken by the NSA and the FBI in fighting international terrorism, on the other hand, has proved to be, at the very least, questionable. Schneier (2015) argues that bulk data collection did not prevent events such as the 2013 Boston bombings, and that the only success derived from the retention of telephone metadata has been the conviction of a taxi driver sending $8,500 to a Somali organisation. This is because online surveillance has proved to be effective only when it is *targeted*, that is collecting information with a specific criterion. Acquiring a large dataset, in order to find out about meaningful terrorist activity, has not given any result.

Conversely, however, placing large amounts of data on its citizens in the hands of government threatens more common citizens than it does terrorists or criminals. Firstly, echoing Bentham's Panopticon, the fear of being constantly watched can chill freedom of expression and political dissent, as it can the spread of so-called "citizen reporting programs" (e.g. the DoJ's *Terrorism Information and Prevention System*). Secondly, datasets can be misused to discriminate between individuals or they can be targeted by hackers. Thirdly,

the practice of law enforcement agencies of mining raw data, until some criminal pattern emerges to their mind, brings back the shadows of inquisitorial judicial systems more typical of totalitarian countries than healthy democracies.[8] Moreover, in order to perform surveillance, the government creates or harnesses cybersecurity flaws in the networks of the third parties involved, leaving those gateways into their systems at the mercy of cybercriminals, with great damage for American businesses.

In conclusion, the development of mass communications surveillance happened straight after 9/11, in a political climate in which a quick and tough response was the only concern. The content of the Patriot Act and of the other laws speaks of the influence of this. However noble and honest the intentions of the legislator at that time, pieces of legislation such as the Patriot Act have opened a season of government interference in the 'right to be let alone' of individuals and businesses, which exemplifies how an unchecked executive almost inevitably bends the rule of law, in order to pursue objectives other than the one it was entrusted with by the people.

3. *The chains*

Here we analyse how unlawful governmental surveillance over its citizens is opposed by judges. Looking at the EU, the following paragraph shows how this element has proved to be decisive in answering Juvenal's question: "Sed quis custodiet ipsos custodes?".[9]

A. The courts

[8] "*Show me six lines written by the most honest man in the world, and I will find enough therein to hang him*" Cardinal de Richelieu, in Schneier B. (2015) *Data and the Goliath*. New York: W. W. Norton & Company.
[9] Juvenal, *Satires*, VI, O31-O32.

The experience of the Court of Justice of the European Union (CJEU) in relation to the regulation of digital surveillance is highly relevant for the purposes of this essay, as it neatly underlines the power of the judiciary in keeping the executive within its constitutional borders. Drawing on a landmark decision of the Court, this part will analyse how courts are able to protect civil rights against government interferences and promote legislative change with their decisions.

The case is *Digital Rights Ireland*,[10] which addressed the validity of the 2002 Data Retention Directive,[11] in the face of the fundamental values of the right to a private life and data protection, recognised by the Charter of Fundamental Rights of the European Union art. 7[12] and 8[13] respectively, which is part of the EU primary body of law.

The Directive placed an obligation on Internet Service Providers (ISPs) to retain users' metadata for the purpose of investigating international terrorism, hence interfering with the above mentioned rights. Following art. 52(1)[14] of the Charter, interferences in the Charter's rights are allowed *only* if they are proportionate and necessary, are provided by law, and respect the *essence* of the rights. Although satisfying the other requirements, the Court invalidated the Directive because it did not meet the 'necessity' requirement, arguing that the 'retention regime' was too broad to assure that interference in fundamental rights would

[10] Joined Cases C-293/12 And 594/12 Digital Rights Ireland And Seitlinger And Others.
[11] Directive 2002/58/EC.
[12] "*Respect for private and family life*. Everyone has the right to respect for his or her private and family life, home and communications."
[13] "*Protection of personal data*. 1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority."
[14] "*Scope of guaranteed rights* 1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."

happen only when necessary. Specifically, the Directive failed to specify any criteria for determining the kind of users to be targeted, the retention time period, and which authorities would supervise the process of acquisition and subsequent use of the metadata.

Following the decision, the different data retention regimes implemented by the Member States have been subject to review, in order to comply with the interpretation laid down by the Court of art. 7 and 8 of the Charter. For instance, the Belgian Constitutional Court annulled the national law implementing the invalidated Data Retention Directive. Subsequently the Belgian legislature drafted a new law, on the basis of the findings in the Digital Rights Ireland judgment. On top of that, on 27 April, 2016, the EU institutions adopted a new Directive[15] on the processing of personal data by the competent national authorities for the purposes of criminal investigation, establishing a legal framework surrounding those activities, which respects the right to data protection as interpreted by the CJEU.

Similarly to the Patriot Act, the Data Retention Directive was conceived in the aftermath of terrorist attacks, namely those in Madrid in 2004 and in London in 2005, and under the British presidency of the European Council. As a matter of fact, the UK intelligence agency GCHQ has been working closely with the NSA to develop communications surveillance programs, and the broadness of the Directive can be interpreted in the direction of granting intelligence forces with as much leeway as possible. Therefore, the CJEU's intervention proves how fundamental the action of the courts can be in controlling the expansion of government activity, and in triggering its other constitutional check, the legislature.

4. *The lock*

[15] Directive (EU) 2016/680.

In the digitally-networked society we live in, the shift towards a surveillance state is not only redesigning the dynamics between constitutional powers, but also adding another element to the equation, i.e. the private agents who control the network infrastructure.

A. Gatekeepers

The rise of network gatekeepers has been made possible by a fundamental shift in ICT technologies, namely from an open and decentralized environment to an ecosystem of appliances tethered to the owner of the platform on which they rely to function (the most important example of this being cloud computing, and the switch from product to service-based businesses).[16]

Empowered by the Internet, those networks of devices are completely at the disposal of the entity that controls the network and its ways of access, i.e. the gatekeeper – the Googles and Apples.

The unmatched scale of mass surveillance has been possible because technology has significantly lowered the cost and structural complexity of surveillance, which has always been one of the structural limits to it.

In fact, the reasons whereby state surveillance have assumed such an unregulated dimension can be analysed through the lenses of Lessig's four modalities of regulation, namely law, social norms, market and architecture[17]. Before digitalisation, the cost of surveillance used to rise proportionally with the number of subjects targeted because of the less ubiquitos nature of telecommunication systems, which meant that these activities were naturally limited by market and architectural constraints. Nowadays, this twofold barrier has fallen thanks to the rise in the digital industry of the so-called 'surveillance capitalism', that is a business model centered on the collection and processing of as much as possible user's data from devices tethered to a proprietary network or platform. Moreover, social

[16] Zittrain, J. (2008). *The future of the Internet and how to stop it*. New Haven: Yale University Press.
[17] Lessig, L. (2006) *Code: Version 2.0*. 2nd ed. New York: Basic Books.

norms that valued the respect of the private sphere of Americans against government intrusions have been put aside in the aftermath of 9/11, relaxing the public oversight on such actions. Laws such as FISA were ineffective as well, as they needed the contribution of the other modalities in order to function properly.

In the digital infosphere every user is a node of the network, however there are some nodes which have more *regulatory gravity* (Murray, 2011),[18] i.e. regulatory actions over them affect the other nodes linked to them as well. In such environment, the market and technical constraints of addressing every node disappear, while it is sufficient to operate over these gatekeepers to influence all the appliances and users tethered to them. Precisely, phenomena as mass surveillance have demonstrated this new quality of regulatory switches attached to these private actors.

On the other hand, the debate sparked by the introduction in consumer products of 'full-disk' and 'end to end' encryption allows us to observe the figure of the gatekeeper from the perspective of the inhibitor rather than of the facilitator. The law enforcement community[19] has warned about the risks of the technology, which will prevent those products from being searched even in the presence of a court warrant. Pursuant to the Fifth Amendment 's right against self-incrimination, the defendant cannot be compelled to provide the court with the device passcode, blocking the only way to decrypt the data. The most common proposal advanced by the supporters of this thesis is to regulate encryption technology in smartphones at the federal level, for instance through the creation of a 'backdoor' dedicated to law enforcement agents. The solution would fall under the scope of the Commerce Clause, and it already has a precedent in 1994 CALEA.

[18] Murray, A.D. (2011) Nodes and Gravity in Virtual Space. 5 *Legisprudence* 195.
[19] Vance, Cyrus Jr. (2015) *Report Of The Manhattan District Attorney's Office On Smartphone Encryption And Public Safety*. Available at: https://cyber.harvard.edu/pubrelease/dont-panic/DA_Report_Smartphone_Encryption_Public_Safety_11182015.pdf (Accessed: 26th January 2016)

The rebuttal[20] to those arguments is usually that, although encryption can prevent access to certain types of data, the ability of law enforcement to prosecute crimes is not at all trumped, for several reasons. Firstly, digital companies will never implement extended data encryption, as they themselves rely heavily on users' data to run their services and to earn from them, in accordance with the 'surveillance capitalism model. Secondly, although encryption is mathematically hard to break, the software in which the encrypted data is placed is still subject to cybervulnerabilities, providing law enforcement with alternatives to acquire the information. Thirdly, the Internet of Things will open up new ways of obtaining the data needed to prosecute a crime. Fourthly, encrypted devices are mainly immune to mass surveillance only, whilst they are still vulnerable to targeted intrusion techniques, which harness flaws in the encryption software rather than trying to directly decrypt the intercepted data. The higher cost of targeted surveillance forces the attacker (i.e. law enforcement) to focus its efforts exclusively on real threats, bringing back some of the architectural and market constraints of the past. Another recurring argument in this debate, alive since the Cryptowars of the 90s is the danger of 'back doors' to the security and economic competitiveness of American firms in the ICT industry. As Yochai Benkler puts it:[21]

«*Apple's design of an operating system impervious even to its own efforts to crack it was a response to a global loss of trust in the institutions of surveillance oversight. It embodied an ethic that said: "You don't have to trust us; you don't have to trust the democratic oversight processes of our government. You simply have to have confidence in our math.*»

The problem with the FBI's approach is that it betrays exactly the mentality that got us into the mess we are in. Without commitment by the federal government to be transparent and accountable under institutions that function effectively, users will escape to technology.

[20] Zittrain, J. et al. (2016) *Don't Panic. Making progress of the "going dark" debate.* Available at: https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf (Accessed: 26th January 2016).

[21] Benkler, Y. (2016) *We cannot trust our government, so we must trust the technology*. Available at: https://www.theguardian.com/us-news/2016/feb/22/snowden-government-trust-encryption-apple-fbi (Accessed: 26 January 2017).

If Apple is forced to cave, users will go elsewhere. American firms do not have a monopoly on math.'

Civil rights should not be at the mercy of the changing outcomes of the fight between the government and tech corporations. There is a need for a democratic response which will have to take into account the features of this new regulating environment. The legislative process should be the venue where the conflicting interests of citizens, government and gatekeepers find a common direction, in order to elaborate a much-needed law which will be able to effectively regulate the digital society of the future.

5. *Conclusion*

This paper set itself the ambition of recognising ongoing trends in the dynamics of power in the digital surveillance state, which could eventually lead to a new theory of regulation as the digitally-networked society fully develops. Firstly, the US case has demonstrated how the executive harnesses legal tools and the political climate to expand beyond its constitutional limits in order to pursue its objectives. Secondly, the CJEU activism has evidenced how crucial the role of courts still is in informing legislation in respect of fundamental rights. Thirdly, the tragic facts of San Bernardino have highlighted how the digital society has shifted the balance of power from the traditional constitutional actors to the gatekeepers. The Internet has gone from a stateless dimension[22] to becoming the most effective instrument of power in the hands of government, and rising trends as the IoT promise to change again the 'network of the networks' as we know it. The hope is that the ongoing debate should be able to find the appropriate answers to the most pressing

[22] Barlow, J.P. (1999) *A Declaration of the Independence of Cyberspace*. Available at: https://www.eff.org/cyberspace-independence (Accessed: 26th January 2016). Johnson, D. R. and Post, D. G. (1996) Law And Borders: The Rise of Law in Cyberspace. 48 *Stanford Law Review* 1367.

challenges to the individual and his or her rights posed by this new articulation of powers, keeping in mind the lesson of Judge Learned Hand:[23]

«*I often wonder whether we do not rest our hopes too much upon constitutions, upon laws, and upon courts. These are false hopes; believe me, these are false hopes. Liberty lies in the hearts of men and women; when it dies there, no constitution, no law, no court can save it; no constitution, no law, no court can even do much to help it. While it lies there, it needs no constitution, no law, no court to save it. And what is this liberty which must lie in the hearts of men and women? It is not the ruthless, the unbridled will; it is not freedom to do as one likes. That is the denial of liberty, and leads straight to its overthrow. A society in which men recognize no check upon their freedom soon becomes a society where freedom is the possession of only a savage few – as we have learned to our sorrow.*»

[23] "*The Spirit of Liberty*" - speech at "I Am an American Day" ceremony, Central Park, New York City (21 May 1944).