RETHINKING PRIVACY TO DEFINE SURVEILLANCE

PROFESSOR ROSA MARIA GARCIA SANZ
COMMUNICATION LAW PROFESSOR
UNIVERSITY COMPLUTENSE OF MADRID
(Department Constitutional Law)

PRG MEMBER AT NYU Information Law Institute

Email: rosamga@pdi.ucm.es

Support for this paper came from a fellowship of Foundation Caja Madrid (Spain)

ABSTRACT.....4
I will observe and analyse recent surveillance activities and identify the "new elements" and the consequences for citizens' "private lives". I will address the issue of whether security and freedom are more or less protected by the new "technology surveillance" used by governments and the private sector.....4
1INTRODUCTION..... 4
2DIGITAL DEMOCRACY FAILURE.....4
2.1BLURRED LINES IN THE SEPARATION OF BRANCHES.....5
2.2GOVERNMENT TRESPASSING INTO CIVIL SOCIETY.....6
2.3LOSS OF SOVEREIGNTY AND LEGITIMACY 7
3BLURRED LINES BETWEEN THE PRIVATE/PUBLIC DIGITAL SPHERE.....8
3.1CRISIS OF FUNDAMENTAL RIGHTS AND LIBERTIES.....8
3.2PUBLIC/PRIVATE SURVEILLANCE OR ALL THE SAME.....8
4DO WE EXPECT PRIVACY ON THE INTERNET?.....9
4.1EVERYTHINS IS DATA ON THE INTERNET.....9
4.2PERSONAL DATA AND PRIVACY: NOT EVERYTHING IS PRIVATE.....10
4.3IDENTIFICATION AND IDENTITY.....11
5 CONCLUSION..... 11

ABSTRACT

I will observe and analyse recent surveillance activities and identify the "new elements" and the consequences for citizens' "private lives". I will address the issue of whether security and freedom are more or less protected by the new "technology surveillance" used by governments and the private sector.

Our lives online are data, information and expression. Surveillance on the Internet is easier than ever. Every "key stroke" provides a lot of meaningful data. Two fundamental rights are basic on the Internet: data protection and freedom of information and expression. These digital rights are the "trunk" from which other branches stem. The regulation and protection of these two rights are the initial protection for the others. A new understanding of "data protection" (privacy) is absolutely necessary in order to rethink "surveillance" in the public or private sector. The European law is too rigid and narrow, but the American perspective is too flexible and broad. We need to start again thinking about fundamental rights on the Internet in order to find a new way to provide security that maintains freedom.

This paper will focus on the public sector, i.e. government surveillance. Traditionally governance depends on surveillance in extreme circumstances to protect the rights and freedoms provided in democratic constitutions. We have a long tradition—and many reasons—to accept this kind of surveillance (to protect the country and citizens), but we cannot accept a government that acts as a "Big Brother" with expansive powers without limitation. A Big Brother enabled by "Big Data" can have the opposite result to the reason that traditionally legitimized the government surveillance. Strong fundamental digital rights with strong protection online are the way to control the unlawful surveillance.

1 INTRODUCTION

Although I will take into account the European impact of the disclosures of classified documents by Edward Snowden, I will focus and base my paper mostly on the American issues that have arisen after the unauthorized disclosure of these classified documents. The main facts[1] are well known around the world because of the regular stream of daily media coverage. On June 5, 2013, the British newspaper The Guardian published the first series of articles based on unauthorized disclosures of classified documents by Snowden, a contractor for the National Security Agency ("NSA"). The article described an NSA program to collect millions of telephone records, including records about purely domestic calls. Over the next days, additional articles were published regarding this program as well as another NSA program referred to as "PRISM." The NSA's telephone records program is operated under an order issued by the Foreign Intelligence Surveillance Act ("FISA") court pursuant to Section 215 of the Patriot Act, an order that is renewed approximately

[1] But Government surveillance goes beyond the National Security Agency activities. We have to think about surveillance cameras on the streets, facial recognition, drones, Google glasses, police search and seizures, etc. Before Jones case, the third party doctrine ensured that none of this activity was regulated by the Fourth Amendment. *United States v. Jones* 132 S. Ct. 945 (2012).

every ninety days. The program is intended to enable the government to identify communications among known and unknown terrorism suspects, particularly those located inside the USA. In the European context, the institutions are pointing out specifically to US NSA intelligence programs allowing for the mass surveillance of EU citizens through direct access to the central servers of leading US Internet companies (PRISM program).

Based on the distinction between metadata[2] and content, there is an inadequate protection for metadata and it leads to abuse in the US context. The Fourth Amendment to the US Constitution protects individuals from unreasonable searches and seizures. Initially, it would seem that this protection would apply just as clearly to the capture and analysis of metadata as to the interception or disclosure of the communication's contents. However, courts have frequently applied a judicially created exception to the Fourth Amendment, called the "third party doctrine." The doctrine holds that records of individual's phone calls, location, Internet use and more collected data or metadata by companies lack constitutional protection. Law enforcement and national security entities frequently demand metadata from third parties. The consequences of lesser metadata protection have been mass surveillance and frequent abuses that undermine the privacy and civil rights of Americans and all the citizens around the world.

Although the third party doctrine has been widely challenged in recent years, it looks like the Fourth Amendment to the US Constitution needs changes, taking into account the digital technology and Internet communications. The predominant interpretation of the Fourth Amendment provides a broad scope to the Government for surveillance. In addition the national security exceptions provided by the law[3] gives the US Government an almost unlimited spectrum for surveillance and citizens a very limited right of privacy.

We are living at a critical and exciting moment, because it looks like the right timing for a new legal framework for both the USA and UE[4].

2 DIGITAL DEMOCRACY FAILURE

I think it was a matter of time. The virtual world of the Internet is not like the "real" world, and digital technology is provoking and presenting "problems" in every area of law and policy. They look the same as old problems but they are quite different. When traditional cases are applied, like Smith v. Maryland[5], on a similar but new case on the

2! Data about data. Metadata means any data other than contents of a communication. See http://dictionary.reference.com/browse/metadata

3 The USA Patriot Act, 2001 ; The Foreign Intelligence Surveillance Act (FISA), 1978; FISA Amendments Act, 2008; and The Electronic Communication Privacy Act (ECPA), 1986. ECPA provides the framework for access to electronic information (metadata, law enforcement), and FISA establish its own demands for information, generally more permissive than ECPA in allowing access to information. Patriot Act amended FISA to give the NSA broad scope to compel the disclosure of "business records" in order to "obtain foreign intelligence information" or "protect against international terrorism or clandestine intelligence activities".

4! Ken Bamberger and Deirdre Mulligan, *Privacy on the Books and on the Grounds*, STANFORD LAW REV. Vol.63: 247 2011

5 Smith v. Maryland, 442 U.S. 735 (1979), in which the Court concluded that individuals have no constitutional right of privacy in the numbers that they dial from their telephones. That decision is now the lynchpin of the government's constitutional rationale underlying the NSA's telephone records program.

Internet, the result is totally unjust. Surveillance--and Government surveillance[6] in particular--is not new and, anyway, in a limited scope, it is necessary for security and, of course, for national security. In our traditional world, the executive branch had this important responsibility of national security surveillance, defined and limited by the law and controlled by the judicial branch (*ex ante* warrants and *post* verification). But the new world on the Internet and the new digital technologies has given governments some incredible tools for surveillance without precedent. In addition, these technologies are provoking new challenges because of the increasing capabilities of intelligence agencies in their surveillance activities. And they are creating new implications for the rule of law in a democratic society. Technologically advanced systems, designed by US and some UE Member States' intelligence services to collect, store and analyze communication and location data and metadata of all citizens around the world, are reaching an unprecedented scale and being conducted in an indiscriminate and non-suspicion-based manner.

When the NSA identifies communications that may be associated with terrorism, it issues intelligence reports to other federal agencies, such as the FBI, that work to prevent terrorist attacks. The U.S. Foreign Intelligence Surveillance Court (FISC[7]) order authorizes the NSA to collect nearly all call detail records generated by certain telephone companies in the United States, and specifies detailed rules for the use and retention of these records. Call detail records typically include much of the information that appears on a customer's telephone bill: the date and time of a call, its duration, and the participating telephone numbers. Such information is commonly referred to as a type of "metadata." The records collected by the NSA under telephone records program do not, however, include the content of any telephone conversation. After collecting these telephone records, the NSA stores them in a centralized database. Initially, NSA analysts are permitted to access the Section 215 calling records only through "queries" of the database. A query is a search for a specific number or other selection term within the database, under the terms of the law.

PRISM began in 2007 in the wake of the passage of the Protect American Act under the Bush Administration. The program is operated under the supervision of the FISA Court (or FISC) pursuant to the FISA. Its existence was leaked six years later by NSA contractor Edward Snowden, who warned that the extent of mass data collection was far greater than the public knew and included what he characterized as "dangerous" and "criminal" activities. *The Guardian* and *The Washington Post* published the disclosures on June 6, 2013. Subsequent documents have demonstrated a financial arrangement between the NSA's Special Source Operations division (SSO) and PRISM partners in the millions of dollars.

The documents Snowden released indicate that PRISM is the number one source of raw intelligence used for NSA analytic reports, and it accounts for 91% of the NSA's Internet traffic acquired under FISA section 702 authority. The leaked information came to light one day after the revelation that the FISA Court had been ordering a subsidiary of telecommunications company Verizon Communications to turn over to the NSA logs tracking all of its customers' telephone calls on an ongoing daily basis.
U.S. government officials have disputed some aspects of the *Guardian* and *Washington Post* stories and have defended the program by asserting it cannot be used on domestic targets without a warrant, that it has helped to prevent acts of terrorism, and that it receives

---

6 In United States v. Jones, the Supreme Court made statements that call into question the Court's "third party doctrine," the controversial notion that government officials need no justification under the Constitution to view or access any activities or information that can be viewed or accessed by third parties outside the home. United States v. Jones 132 S. Ct. 945 (2012).

7 Foreign Intelligence Surveillance Court or FISA Court.

independent oversight from the federal government's executive, judicial and legislative branches.

But it was not enough, because NSA had the capabilities of getting access to the servers and networks without any permission, according to *Washington Post* on July 10, 2013 and *New York Time*s, on September 5, 2013.

In Europe, concerns arose not just because of the use of the PRISM program, but also the analysis of content and metadata (Xkeyscore program), the circumvention of online encryption (BULLRUN), access to computer and telephone networks and access to location data, as well as to systems of the UK intelligence agency Government Communications Headquarters (GCHQ), such as its upstream surveillance activity (Tempora program) and decryption program (Edgehill). European authorities believe that the existence of a program of a similar nature, even if on a more limited scale, is likely in other EU countries such as France, Germany and Sweden.

Trust between countries and allies has been profoundly broken: trust between the two transatlantic partners, trust among EU Member States, trust between citizens and their governments, trust in the respect of the rule of law, and trust in the security of IT services.

2.1 BLURRED LINES IN THE SEPARATION OF BRANCHES

These mass surveillance programs can be necessary to combat terrorism, but I strongly believe that it can never in itself be a justification for untargeted, secret and sometimes even illegal mass surveillance programs. Principles regarding the legality, necessity and proportionality of these programs are calling in order to repair democracy. At this point, everybody agrees that international treaties and EU and US legislation, as well as national oversight mechanisms, have failed to provide for the necessary checks and balances and for democratic accountability. And these issues are not purely a matter of national security, but also a profound problem for Internet Governance and Digital Democracy. The PCLOBP[8] Report exposes the blurred lines in the separation of branches in relation to US Government surveillance activities.

The PCLOBP said the intelligence community had good intentions and although the NSA program, talking about the bulk phone record program, does not fit in the Statute, there is not Constitutional violation[9] after all (based on Smith v. Maryland and third part doctrine). And besides the Congress extended the program without amending the Statute with no

8[!!] Privacy and Civil Liberties Oversight Board. REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215,OF THE USA PATRIOT Act. And on the Operations of the Foreign Intelligence Surveillance Court. January 23, 2014. Available at http://www.pclob.gov/.

9 Chistopher Slobogin, *Making the Most of "United States v. Jones in a Surveillance Society: A Statutory Implementation of Mosaic theory"* , VANDERBILT UNIVERSITY LAW SCHOOL. Available at http://ssm.com/abstract id=2098002

"In short, both concurring opinions endorsed what the lower court in Jones called the "mosaic theory" of the Fourth Amendment—the idea that certain types of governmental investigation enable accumulation of so many individual bits about a person's life that the resulting personality picture is worthy of constitutional protection.[15] The opinions in Jonesthus open the door to a more expansive Fourth Amendment. But the Court still has much to work out. At present, the mosaic theory is little more than a name"

consequences. A special court (FISC) provided secret orders with broad interpretations of the law that led to unexpected consequences. Even more, warrants were not necessary at all because the NSA had a sophisticated and tempting technology, which could escape control. Anyway, it looks like nothing is like it used to be. Following the PCLOBP Report, in 2010, and again in 2011, Congress prevented Section 215 from expiring by extending its expiration date. Courts and the government have concluded that by twice extending the expiration date of Section 215, while the NSA's bulk telephone records program was ongoing, Congress implicitly adopted an interpretation of Section 215 that legitimizes the program. This conclusion rests on the principle that "Congress is presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statute without change. On multiple grounds, however, we believe that principle has no place here. Considers it very doubtful that data collection of such magnitude is only guided by the fight against terrorism, as it involves the collection of all possible data of all citizens; points therefore to the possible existence of other power motives such as political and economic espionage" the UE Report[10] statement says.

But Section 215 was designed to enable the FBI to acquire records that a business has in its possession, as part of an FBI investigation, when those records are relevant to the investigation. Yet the operation of the NSA's bulk telephone records program bears almost no resemblance to that description.

> *"While the Board believes that this program has been conducted in good faith to vigorously pursue the government's counterterrorism mission and appreciates the government's efforts to bring the program under the oversight of the FISA court, the Board concludes that Section 215 does not provide an adequate legal basis to support the program.*
>
> *There are four grounds upon which we find that the telephone records program fails to comply with Section 215. First, the telephone records acquired under the program have no connection to any specific FBI investigation at the time of their collection. Second, because the records are collected in bulk — potentially encompassing all telephone calling records across the nation — they cannot be regarded as "relevant" to any FBI investigation as required by the statute without redefining the word relevant in a manner that is circular, unlimited in scope, and out of step with the case law from analogous legal contexts involving the production of records. Third, the program operates by putting telephone companies under an obligation to furnish new calling records on a daily basis as they are generated (instead of turning over records already in their possession) — an approach lacking foundation in the statute and one that is inconsistent with FISA as a whole. Fourth, the statute permits only the FBI to obtain items for use in its investigations; it does not authorize the NSA to collect anything. In addition, we conclude that the program violates the Electronic Communications Privacy Act. That statute prohibits telephone companies from sharing customer records with the government except in response to specific enumerated circumstances, which do not include Section 215 orders. Finally, we do not agree that the program can be considered statutorily authorized because Congress twice delayed the expiration of Section 215 during the operation of the program without amending the statute. The "reenactment*

10 EUROPEAN PARLIAMENT 2009 - 2014 Committee on Civil Liberties, Justice and Home Affairs 2013/2188(INI) 23.12.2013. Draft Report on the US NSA surveillance program, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)) Committee on Civil Liberties, Justice and Home Affairs. Rapporteur: Claude

doctrine," under which Congress is presumed to have adopted settled administrative or judicial interpretations of a statute, does not trump the plain meaning of a law, and cannot save an administrative or judicial interpretation that contradicts the statute itself. Moreover, the circumstances presented here differ in pivotal ways from any in which the reenactment doctrine has ever been applied, and applying the doctrine would undermine the public's ability to know what the law is and hold their elected representatives accountable for their legislative choices."

In this way, the US Government is, by its own interpretation, making the law and avoiding the judicial and legislative branches. And Congress extending the program without changing the law is avoiding its responsibility and the judicial branch is becoming an "orders vending machine" at the service of the Government. But even more, the Government touched a point where it did not need any Court order or Congress collaboration, thanks to the collaboration of Internet companies and its own surveillance technology it was able to do incredible things, such as gaining direct access to all communications. These mass surveillance programs can be necessary to combat terrorism, but it can never in itself be a justification for untargeted, secret and sometimes even illegal mass surveillance programs. And we need to apply the principles of legality, necessity and proportionality to these programs in order to repair democracy. At this point, there is broad agreement that international treaties and EU and US legislation, as well as national oversight mechanisms, have failed to provide for the necessary checks and balances and for democratic accountability. And these issues are not purely a matter of national security but a profound problem as it concerns Digital Democracy and Internet Governance.

2.2 GOVERNMENT TRESPASSING INTO CIVIL SOCIETY

It looks very doubtful that the fight against terrorism is the only reason for data collection of such magnitude since it involves the collection of all possible data of all citizens. Instead it points to the possible existence of other power motives, such as political and economic espionage. The surveillance programs are yet another step towards a fully-fledged preventive state, changing the established paradigm of criminal law in democratic societies. They are promoting instead a mix of law enforcement and intelligence activities with blurred legal safeguards, often not in line with democratic checks and balances and fundamental rights, especially the presumption of innocence. It recalls the prohibition of the use of preventive dragnets unless there is proof of a concrete danger to other high-ranking legally protected rights, whereby a general threat situation or international tensions do not suffice to justify such measure. The UE Report points out:

"Is adamant that secret laws, treaties and courts violate the rule of law; points out that any judgment of a court or tribunal and any decision of an administrative authority of a non-EU state authorizing, directly or indirectly, surveillance activities such as those examined by this inquiry may not be automatically recognized or enforced, but must be submitted individually to the appropriate national procedures on mutual recognition and legal assistance, including rules imposed by bilateral agreements. Points out that the abovementioned concerns are exacerbated by rapid technological and societal developments; considers that, since Internet and mobile devices are everywhere in modern daily life ('ubiquitous computing') and the business model of most internet companies is based on the processing of personal data of all kinds that puts at risk the integrity of the person, the scale of this problem is unprecedented."

The US Government (or any government) is not allowed to act on the Internet like it were another private corporation: taking data from users and exploiting their data without consent

and legal control in a kind of "virtual wild west." Acting in collaboration with companies or even against the companies but taking "illegally" all data from citizens all around the world is bringing governments to a point where there is a lack of sovereignty and legitimacy. Because governments cannot behave like a private citizen but with all the powers of a State given by their respective constitutions, a lot of modifications are needed in order to address this problem.

We have begun to see the reactions from the US courts to this problem[11]. For instance, the District Court for the District of Columbia, in its Decision of 16 December 2013, ruled that the bulk collection of metadata by the NSA is in breach of the Fourth Amendment to the US Constitution. However, in contrast, a Decision of the District Court for the Eastern District of Michigan ruled that the Fourth Amendment requires reasonableness in all searches, prior warrants for any reasonable search, warrants based upon prior-existing probable cause, as well as particularity as to persons, places and things and the interposition of a neutral magistrate between Executive branch enforcement officers and citizens.

The President's Review Group on Intelligence and Communication Technology of 12 December 2013 proposes 45 recommendations to the President of the US. The recommendations stress the need simultaneously to protect national security and personal privacy and civil liberties. The recommendation of the report invites the following:

- US Government to end bulk collection of phone records of US persons under Section 215 of the Patriot Act as soon as practicable
- To undertake a thorough review of the NSA and the US intelligence legal framework in order to ensure respect for the right to privacy
- To end efforts to subvert or make vulnerable commercial software (backdoors and malware)
- To increase the use of encryption, particularly in the case of data in transit
- Not to undermine efforts to create encryption standards
- To create a Public Interest Advocate to represent privacy and civil liberties before the Foreign Intelligence Surveillance Court
- To confer on the Privacy and Civil Liberties Oversight Board the power to oversee Intelligence Community activities for foreign intelligence purposes, and not only for counterterrorism purposes
- To receive whistleblowers' complaints
- To use Mutual Legal Assistance Treaties to obtain electronic communications
- Not to use surveillance to steal industry or trade secrets.

In respect to intelligence activities about non-US persons under Section 702 of FISA, the Recommendations to the President of the USA recognize the fundamental issue of respect for privacy and human dignity enshrined in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights. They do not recommend granting non-US persons the same rights and protections as US persons. However, the President Obama "Presidential Policy Directive/PPD- (Subject Signals Intelligence Activities)[12] January 17, 2014, is intended for everybody in the world

11! ACLU v. Clapper, No. 13-3994 (S.D.N.Y. Dec. 27, 2013); Klayman v. Obama, No. 13-0851 (D.D.C. Dec. 16, 2013); Amended Memorandum Opinion, In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, No. BR 13-109 (FISA Ct. Aug. 29, 2013).

12! THE WHITE HOUSE Office of the Press Secretary January 17,2014 PRESIDENTIAL POLICY DIRECTIVE/PPD-28 SUBJECT: Signals Intelligence Activities

not just Americans.

Fundamental rights, notably freedom of expression, of the press, of thought, of conscience, of religion and of association, private life, data protection, as well as the right to an effective remedy, the presumption of innocence and the right to a fair trial and non-discrimination, are in danger. This kind of surveillance is not protecting citizens, fundamental rights nor the Constitution. This Governmental surveillance is attacking the Constitutional rights of the citizens of the world under the pretext of terrorism.

2.3 LOSS OF SOVEREIGNTY AND LEGITIMACY

This global, bulk and indiscriminate data and communication surveillance, which we became aware of after the Snowden's revelations, means less sovereignty for the US and for the rest of countries that were under this illegal surveillance. The US has suffered the exposure of its encryption technology and technologies dependent upon that encryption, and a loss of legitimacy in relation to citizens. In addition, the other countries had no data sovereignty at all, and then ultimately no sovereignty at all. Just the sheer magnitude of the data collection makes the argument that it was just for fighting terrorism seems implausible. It is more plausible that this level of data collection points to the existence of other power motives such as political and economic espionage, as the UE Report statement indicates. And the Government using data for political purposes, i.e. political elections, compromises the basis of democratic systems because political interests can target voters as consumers with targeted advertising.

If the rules of the "game" are not observed, we are calling for a new game and new rules or provoking "chaos." Because this is not the legitimate government surveillance that we accepted in a democratic system, cyber security can be attacked by hackers, society groups with powerful knowledge of software and encryption, citizens using open-source tools, whistleblowers, companies, etc. And at the end of the day we will not find any national security at all.

EU Member States therefore ask that appropriate measures be taken to ensure its internal and external security. The mere fact that a decision concerns state security does not necessarily mean that European Union law is inapplicable. It further demands that the protection of the privacy of all EU citizens is at stake, as are the security and reliability of all EU communication networks. Further, discussion and action at EU level is not only legitimate, but also a matter of EU autonomy and sovereignty, the EU Report[13] cited.

3 BLURRED LINES BETWEEN THE PRIVATE/PUBLIC DIGITAL SPHERE

The architecture of the Internet does not provide a clear separation of private and public spheres like we can understand in the "real world." Moreover, the digital tools, software, apps and algorithms, provoke a lot of doubts about to what extent something is public or private. A large set of data can reveal sensitive information that cannot be inferred from any specific element in that set. This means that privacy protections need to apply not only to data directly collected from an individual but also to any inferences or derivative information generated through the analysis of the data. It requires carefully evaluating the circumstances where law enforcement can get data about individuals without any sort of

[13] See the European Report, supra note 10.

legal process. It requires knowing where privacy starts and where the public sphere ends. And we have a lot of examples in relation to rights and liberties affected by this issue. The national security right is just another one, not the only one with problems generated by this blurred line without clear definition. Also copyrights are suffering problems about what is private copy, especially when a lot people are able to share (i.e., P2P); or, what is public communication, etc. Data protection on the Internet does not have a clear definition of personal data, because every keystroke can be considered, after relations and correlations, private data[14]. "Big data" can be the result of neutral and insignificant data and metadata, but all become private and personal content after analysis. Many consider that freedom of information and free speech are the realm of the Internet, because it is not easy to prove what is private and intimate and not for public exhibition.

These are only a few examples showing that this blurred line generates a lot of problems for understanding the fundamental rights on the Internet. Security (peace) is absolutely necessary in order to enjoy and exercise our other rights and liberties, but surveillance for the sake of security is confused because it is trespassing the "red line" of privacy beyond what is necessary to achieve that security. The problem is that it is not clear where the "red line" is on the Internet. Is everything private? Is almost everything public? I think it is calling for a criteria or standards in order to sort out the inherent problems.

3.1 CRISIS OF FUNDAMENTAL RIGHTS AND LIBERTIES

Most citizens of democratic countries condemn in the strongest possible terms the vast, systemic, blanket collection of the personal data of innocent people, often comprising intimate personal information. Citizens emphasize that the system of mass, indiscriminate surveillance by intelligence services constitute a serious interference with their fundamental rights. Many have stressed that privacy is not a luxury right, but that it is the foundation stone of a free and democratic society. They point out, furthermore, that mass surveillance has potentially severe effects on the freedom of the press, thought and speech, as well as a significant potential for abuse of the information gathered against political adversaries. European perspectives have emphasized that these mass surveillance activities appear also to entail illegal actions by intelligence services and raise questions regarding the extra-territoriality of national laws. They note that fundamental rights, notably freedom of expression, of the press, of thought, of conscience, of religion and of association, private life, data protection, as well as the right to an effective remedy, the presumption of innocence and the right to a fair trial and non-discrimination, as enshrined in the Charter on Fundamental Rights of the European Union and in the European Convention on Human Rights, are cornerstones of democracy.

Focus on the American scenario--only taking into account the phone records program and analyzing it in the light of the laws--the US Government used the technology ignoring the laws and collected data in an unprecedented way. But it was not the only way, and apart

14 And we have to consider the legal protection of: "Expression Metadata. Numerous state and federal laws also protect the privacy of metadata that is related to expressive activity. These laws recognize that such metadata may both reveal sensitive information about an individual and implicate the freedoms guaranteed by the First Amendment". "Associational Metadata Finally, the First Amendment also protects the privacy of associational information. In a seminal case, NAACP v. Alabama, the Supreme Court held that constitutional protection for freedom of expression and freedom of association include a right to privacy with regard to associational information" And "legal Protection for Location Information". See: METADATA. Piecing to together a privacy solution. A REPORT BY THE ACLU OF CALIFORNIA. FEBRUARY 2014. See online at: ACLUNC.ORG/TECH/META

from the PRISM program and regardless the law, it was able to get direct access to the fiber optic cable networks and servers and collect information on its own at extraordinary levels. Newly revealed documents show that the NSA has circumvented or cracked much of the encryption that automatically secures emails, Web searches, Internet chats and phone calls of Americans and others around the world. The project, referred to internally by the codename Bullrun, also includes efforts to weaken the encryption standards adopted by software developers.

As we learned from the PCLOP Report, American Government violated several laws. And states that:

> *"Every FISA court order renewing the bulk telephone records program puts telephone companies under a continuing obligation, over a period of ninety days, to provide the NSA with their newly generated calling records on a daily basis. In other words, when telephone companies receive an order from the FISA court, they are not directed to turn over whatever calling records they have in their possession at the time. Instead, every day for the next ninety days after receiving the order, they must furnish the NSA with the new calling records generated that day by their customers. No language in Section 215 purports to authorize the FISA court to issue orders requiring the ongoing daily production of records not yet in existence. The government discerns support for its position in decisions holding that a provision in the Stored Communications Act ("SCA") permits orders for the prospective disclosure of records. These decisions involve the prospective disclosure of a particular type of telephone metadata — cell site location information. But the courts that have approved prospective orders for cell site location information have done so through a so called "hybrid theory" that invokes "the combined authority of the Pen Register Statute and the Stored Communications Act." Under this hybrid theory, the Pen Register, apart from the lack of express or implied authority in Section 215 for orders that require the disclosure of newly created records prospectively, the text of the statute suggests that such orders are not within its scope. Even if Section 215 were compatible with orders for the prospective disclosure of items that do not yet exist, orders requiring the daily disclosure of new telephone calling records are inconsistent with the structure of FISA as a whole. A different portion of that statute directly authorizes the prospective collection of telephony metadata through pen registers or trap and trace devices. Construing Section 215 to permit ongoing acquisition of the very same data renders FISA's pen register provision superfluous. It also allows the government to evade the limitations in that provision that govern such prospective monitoring. Under FISA's pen register provision, the government may apply for an order authorizing the installation and use of a pen register or trap and trace device in a counterterrorism investigation. Such devices capture the same dialing, routing, and addressing information that is included in the calling records obtained by the NSA.*
>
> *As the FISA court acknowledged, the very statute that created Section 215, the Patriot Act, also amended ECPA "in ways that seemingly re-affirmed that communications service providers could divulge records to the government only in Specified circumstances" — without including FISA court orders issued under Section 215. The fact that the same statute both created Section 215 and amended ECPA, but without adding an exception to ECPA for Section 215 orders, undermines the notion that ECPA and Section 215 are in conflict, and provides an additional basis for strictly adhering to ECPA's prohibitions by not inferring unwritten exceptions to those prohibitions. It also demonstrates that another fundamental canon of statutory construction applies here — that the inclusion of some implies the exclusion of others not mentioned. "Where there is an express*

exception, it comprises the only limitation on the operation of the statute and no other exceptions will be implied." In addition to concluding that the NSA's bulk telephone records program is unauthorized by Section 215, we also believe that it violates the Electronic Communications Privacy Act ("ECPA"). ECPA limits the circumstances under which a telephone company or other electronic communication service provider may divulge records about its customers. Apart from certain enumerated exceptions, a provider "shall not knowingly divulge a record or other information pertaining. In late 2008, the government submitted an application to the FISA court seeking Congress did not add an exception to ECPA for Section 215 orders, even though it amended ECPA in other ways at the same time that it created Section 215. That omission should be respected. In addition to concluding that the NSA's bulk telephone records program is unauthorized by Section 215, we also believe that it violates the Electronic Communications Privacy Act ("ECPA")."

All those violations mean that, as a consequence of that massive and indiscriminate surveillance, a lot of constitutional rights were broken as above mentioned. As we know in a democratic and rule-of-law state, fundamental rights have to be balanced and sometimes it is necessary to sacrifice one in order to protect another. But what US Government and other countries did has nothing to do with balance: for the purpose of national security they violated a lot of humans rights. The cost and benefits of this surveillance to prevent terrorism has to be weighed and it looks like we paid a high price for the supposed benefits.

3.2 PUBLIC/PRIVATE SURVEILLANCE OR ALL THE SAME

The US Government isn't allowed to wiretap American citizens without a warrant from a judge. But there are plenty of legal ways for law enforcement to do it, and to snoop on the digital trails (metadata) we create every day. Authorities can often obtain your emails and texts by going to telecommunication and Internet companies, with a simple subpoena that doesn't require showing probable cause of a crime. More revelations about classified NSA surveillance programs show that the government is regularly sweeping up data on Americans' telephone calls and has the capability to access emails, files, online chats and other data — all under secret oversight by a special federal court. PRISM is only one part of the NSA's system for electronic eavesdropping. The "Upstream" program collects from the fiber-optic cable networks that carry much of the world's Internet and phone data. It has mapped the undersea cables that connect North America to the rest of the world.

The collaboration of the private Internet companies, the law enforcement blurred with surveillance activities, the government capability to access emails, files, etc., without legal support or judicial control, brings into question whether there is a difference between the public sector surveillance and the private sector version. Or whether there is just general surveillance in which there is a collection millions of data points everyday and transferred to databases where it is exchanged and available for everybody's business. The Government it is not another company or citizen. The law should define the role of Government on the Internet. We cannot expect good practices from private companies and citizens when governments are the leading culprits of these bad practices.

The Global Network Initiative (GNI[15]) Report says that the GNI Principles and implementation guides companies to narrowly interpret government requests and to ensure that applicable legal procedures are followed. They had limitations on their independent assessment regarding secret national security requests. The companies cannot disclose whether or not they have been subject to national security surveillance under FISA. In order to assess how companies respond to such requests, assessors required access to information that companies are legally prohibited from disclosing. Taking into account this fact, the Report shows us that they review a total number of cases of 59 and out of them:

Cases involving specific government request: 47
Specific cases concerning privacy: 30
Specific cases concerning freedom of expression: 17
Cases related to the broader context of companies operations: 21

The demands for information about individuals from the US Government are large. But because enough information is not available and based on public information, we don't know the extent of collaboration and/or implication of the US Government and the private companies. Everybody is asking for transparency from the US Government and private companies in relation to our personal data.

4 DO WE EXPECT PRIVACY ON THE INTERNET?

Private surveillance, public surveillance and emerging technologies, increasing ubiquity of mobile devices, street cameras, powerful analytic software used by social networking companies and others corporations, all existing technological threats to individual privacy by states and corporations, push us to ask: do we expect privacy on the Internet? Is everything public? It looks like the only way to maintain privacy is to give up and not to use technology if we want to preserve our privacy. But this means to give up the contemporary world we live in now. Are individuals responsible for safeguarding their own privacy? It is almost impossible to decline voluntarily the sharing of information because of the way electronic communications function. Powerful algorithms, software and apps take our fingerprints beyond what we would wish. Big databases with big data render our personal data and metadata ready for analytics and profiles of any kind and any purpose.

4.1 EVERYTHINS IS DATA ON THE INTERNET

It is not a huge revelation to say that everything on the Internet is data and information[16]: content of communication. It depends on the context in order to distinguish different categories calling for more or less protection. Is every piece of content private? Or is it just freedom of speech and information? It is not easy to be anonymous, because our Internet data trails show our daily life and if connected and related with all our data and movements on the Internet[17], it is not difficult for anyone with the right capabilities to get our

15[!] Global Network Iniciative (GNI). January, 2014. PUBLIC REPORT ON THE INDEPENDENT ASSESSMENT PROCESS FOR GOOGLE, MICROSOFT AND YAHOO. www.globalnetworkinitiative.org

16 The distinction between "metadata" and content of communications is just fiction in the digital environment.

17 "Mosaic theory" of privacy presented by D.C. Court of Appeals in United States v. Maynard, 615 F. 3d 544, 561-63 (D.C. Cir. 2010).

identification and identity. Of course, included in this is the personal information that we reveal voluntarily. There are "magical tools" to do relations and correlations and to create profiles for each of us and identify us as we pursue different goals. At this point, every piece of data is personal data. Metadata deserves the same protection as content of communication in general, and some of the data privacy protection. The EU Date Protection Law[18] has a definition of "personal data" which is not useful anymore, because digital developments overran that definition. We are at the point where just using cell phones, or just keeping them open, provides a lot of personal data. Or just every keystroke is passing on personal data.

4.2 PERSONAL DATA AND PRIVACY: NOT EVERYTHING IS PRIVATE

We cannot expect the same kind of privacy on the Internet and new digital technologies as we enjoy in the "real world." We cannot expect the same "privacy in public" on the Internet. (And again it is calling for a more clear idea about the Internet private/public sphere). It is simple: the "real world" ideas of what is private and what is public does not apply on the Internet. And we have a lot of evidence so far to prove it. It is much more difficult and in many cases impossible to decline voluntarily the sharing of information about electronic communications. A letter can be sent without a return address and dropped off in mailbox, greatly reducing the possibilities of connecting the sender to the recipient[19]. Individuals cannot make or receive a cell phone call without having that information tracked by their carrier. Internet communications require the use of IP addresses that can be logged. "Thus, there is little "voluntary" surrender of privacy in an electronic communication analogous to the readily-available choices available to a letter writer" [20] But we have to find a broader perspective: there are more rights to apply other than privacy, i.e. the right to identity and publicity, freedom of speech and information or just the right to be anonymous[21]. The Internet is global, information is global too, but privacy is not global at all. And we have to find more legal tools to protect our personal information beyond data protection law. There are different traditions, cultures, laws and people. USA prefers "privacy by design" [22] but EU prefers a clear frame of laws to follow[23]. Everything is OK but it does not work. Not on the Internet.

18! Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available at http://www.eur-lex.europa.eu/LexUriServ/

19! See THE REPORT BY THE ACLU OF CALIFORNIA. February 2014. P. 10

20! See the same above Report. P.10

21 The Supreme Court has held that "protection for anonymous speech are vital to democratic discourse. Allowing dissenters to shield their identities frees them to express critical minority views" McIntyre v. Ohio Elections Commission, 514US. 334 (1995). Regardless this concept, in this paper I am thinking for a broader and specific right of anonymity on Internet: the right of not to associate our data or metadata and all our communications in order to preserve our identity and personal lives. Maybe Twitter case challenging law enforcement efforts to unmask anonymous online speakers is close to my approach: See, e.g., Elinor Mills, *Twiter Challeges Court Order to Hand over User Data, CNET, May 8, 2012, http://news.cnet.com/8301-1009_3-57430273-83/twitter-challeges-court-orderto-hand-over-user-data*

22! http://www.privacybydesign.ca/content/

23! http://europa.eu/rapid/press-release_MEMO-14-186_en.htm

Well, let us go to start again: every piece of data is personal data but not every piece of personal data has to be private. For instance, thinking of other law areas, maybe it has to be like copyrights law[24] on the Internet: because the Internet needs technical copies in order to work those copies are not covered by copyright law and permission is not required. We cannot ask for consent on every piece of data. And the Internet systems and digital devices need data to work and to offer all the wonderful services we have. So, to what extent is data technically necessary for the Internet to work? We take for granted these types of data don't need express consent. However, these pieces of data can be protected later when collected and stored by a right of anonymity. Of course, there is a lot of data that will need an express consent and other controls from the data holder. And here is where the

24! Pamela Samuelson, *Privacy as Intellectual Property*, 52 STAN. L. REV. 1125 (2000).

rights of EU Directive of Data Protection [25]should be applied, not because every single data is private but because they are all together our personal information and we should have the control and rights.

The problem comes when someone takes them and uses them for a different purpose than what we consented to or just because they are public. Here is where "contextual integrity" [26] can be useful. So, at this point data sets are in databases or servers. A breach of our given consent for that unique purpose or used in a different context must be punishable by law[27]. Law must establish the master legal lines and basic rights for all information processes, and when the data is in the database, it should be possible to allow "privacy by design" in which mechanisms are used to create the desired privacy[28]. Algorithms and software should be capable to get the identification of a person but also the opposite, unless that person consents. A right to be anonymous pops up in the state of technology,[29] with legal limitations. Online we cannot expect anonymity[30] but yes later in the servers and databases, using tools for disassociation and to make it anonymous. Online we expect safe networks and communications without breaking our freedom of speech and information, and, for personal messages (emails, private transactions, etc.) privacy too. It depends on the different categories of information sensitivity.

Of course, we need a lot of watchdogs to preserve databases, and resistant encryption[31] to protect our computers and online communications first of all.

Database protection brings issues about storage time, technical safeguards and human safeguards. The data should be stored the shortest and most limited amount time in the databases and technically well protected. Journalists and media, civil society organizations and representatives of companies should have databases and servers "watchdogs," having access and knowledge about every movement, operation or request.

4.3 IDENTIFICATION AND IDENTITY

Technology is able to figure out our identification, but at the same time it is able to preserve our identity. In this way, our data can be used as big data for studies and research,

---

25 Paul M. Schwartz and Daniel J. Solove, *Reconciling Personal Information in the United States and European Union,* 102 CALIFORNIA LAW REVIEW (2014)

26 Helen Nissenbaum, PRIVACY IN CONTEXT, Stanford University Press, Stanford, California, 2010. P. 186

27 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

28 EU and USA perspective can be compatible and together more effective.

29 Software Companies are working on it: Microsoft is working on an algorithm called "differential privacy" that it is no able to protect "privacy" but instead to create the way to be anonymous in databases.

30 Because always there are data for our identification and data required for Internet functions.

31 Open source software maybe can provide safest algorithms and encryption than commercial products.

but without our identity. Moreover, companies could use our data (identification)[32] for commercial or whatever legal purposes, but without our identity. A breach of identity must be a serious crime that has to be punished by law.

Categories such as privacy/identity/identification and anonymity require more thought and studies in order to define their exact meaning and role on the Internet and data protection. "Our model places information on a continuum that begins with no risk of identification at one end, and ends with identified individuals at the other. We divide this spectrum into three categories, each with its own regulatory regime. Under the PII 2.0 model, information can be about an (1) identified, (2) identifiable, or (3) no identifiable person. These three categories divide up this spectrum and provide different regimes of regulation for each. Because these categories do not have hard boundaries, we define them in terms of standards, that is, as open-ended benchmarks rather than as hard-edged rules" [33].

5 CONCLUSION

Governments must not continue expanding their surveillance powers for national security based on old laws written for an "analog world," which result in their application to the digital environment that goes against the rule of law and democracy. A new privacy regime is needed for the Internet and digital environment, which provides criteria for a public and private sphere and as a consequence requires rethinking privacy for data protection. Government surveillance should be limited into a clear criterium of public/private information. The existing law is based on the content/metadata paradigm that is already outdated and behind the modern technology. A right to keep identity and/or anonymity can solve some problems online, where all content of communication cannot be protected by privacy. However, freedom of speech and information can be protected using powerful network encryption. A right of anonymity looks like it can protect privacy on databases and allows analytics for big data, without identity being compromised although identification being possible.

Governments should be subject to a general data protection law and for there to be a national security exception for it to act according to specific and strict legislation taking into account the general principles of data protection as much as possible. Law enforcement agencies should be confined to the limits of the new regime, and law enforcement must not be used as an excuse for surveillance.

Government surveillance needs to be under judicial control *ex ante* (warrants with strict requirements) and *ex post* (with strict verification). It can have access to the stored data in databases (anonymous data) under the vigilance of the watchdogs with strict directions and protocols. Time of data storage should be limited as much as possible. When surveillance agencies need access to networks, servers and databases to get personal information of identified persons, the law must establish determined circumstances, determined persons and given relevant facts for an investigation in order to protect national security.

---

32 Consent can be required.

33 Paul M. Schwartz and Daniel J. Solove, *Reconciling Personal Information in the United States and European Union.* 102 CALIFORNIA LAW REVIEW - (2014)

REFERENCES

Ken Bamberger and Deirdre Mulligan, *Privacy on the Books and on the Grounds*, STANFORD LAW REV. Vol.63: 247 2011

http://dictionary.reference.com/browse/metadata

Paul M. Schwartz and Daniel J. Solove, *Reconciling Personal Information in the United States and European Union.* 102 CALIFORNIA LAW REVIEW - (2014)

Helen Nissenbaum, PRIVACY IN CONTEXT, Stanford University Press, Stanford, California, 2010.

Elinor Mills, *Twitter Challenges Court Order to Hand over User Data, CNET, May 8, 2012, http://news.cnet.com/8301-1009_3-57430273-83/twitter-challeges-court-orderto-hand-over-user-data*

http://www.privacybydesign.ca/content/

http://europa.eu/rapid/press-release_MEMO-14-186_en.htm

Pamela Samuelson, *Privacy as Intellectual Property*, 52 STAN. L. REV. 1125 (2000).

http://www.eur-lex.europa.eu/LexUriServ/

Global Network Iniciative (GNI). January, 2014. PUBLIC REPORT ON THE INDEPENDENT ASSESSMENT PROCESS FOR GOOGLE, MICROSOFT AND YAHOO. www.globalnetworkinitiative.org

A REPORT BY THE ACLU OF CALIFORNIA. FEBRUARY 2014. See online at: www.ACLUNC.ORG/TECH/META

THE WHITE HOUSE Office of the Press Secretary January 17,2014 PRESIDENTIAL POLICY DIRECTIVE/PPD-28 SUBJECT: Signals Intelligence Activities

EUROPEAN PARLIAMENT 2009 - 2014 Committee on Civil Liberties, Justice and Home Affairs 2013/2188(INI) 23.12.2013. Draft Report on the US NSA surveillance program, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)) Committee on Civil Liberties, Justice and Home Affairs. Rapporteur: Claude

http://dictionary.reference.com/browse/metadata
Privacy and Civil Liberties Oversight Board. REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215,OF THE USA PATRIOT Act. And on the Operations of the Foreign Intelligence Surveillance Court. January 23, 2014. Available at http://www.pclob.gov/.

Chistopher Slobogin, *Making the Most of "United States v. Jones in a Surveillance Society: A Statutory Implementation of Mosaic theory"*, VANDERBILT UNIVERSITY LAW SCHOOL. Available at http://ssm.com/abstract id=2098002