132

IPRIS Viewpoints

AUGUST 2013

Disclosed: EU Vulnerability. Taking US Mass Surveillance Seriously after the Snowden Affair

BRUNO OLIVEIRA MARTINS*
Aarhus University, Denmark
Affiliated Researcher, Portuguese Institute of International Relations and Security (IPRIS)

Over the last two months, a vast number of Mass Surveillance Systems (MSS) operated by the United States (US) have been revealed. What started as the disclosure of a comprehensive system that collected and stored data referring to phone calls of American citizens, developed later into the revelation of several MSS that encompassed all the main providers of digital communication systems, such as Google, Skype, Apple, Microsoft, Facebook and Yahoo, among others. People around the world became familiar with top-secret MSS and surveillance tools such as PRISM, XKeyscore, Tempora, or Boundless Informant, thereby learning that their digital communications and personal data are being collected in bulk, and indiscriminately monitored by state-of-the-art technology. These programs are operated mainly by the US, but other states' agencies are also trusted with access to the US technology, such as the British Government Communications Headquarters (GCHQ)[1] or the German Bundesnachrichtendienst (BND).[2]

The magnitude and comprehensiveness of these instruments, together with the fact that they target not only American citizens unsuspected of any crime, but similarly innocent citizens from many other countries, triggered fierce debate around the globe. Once again, this episode elevated counter-terrorism measures to the top of the agenda in international politics and confirmed that the post-9/11 world operates with different standards than the ones observed prior to 2001. 'Terrorism' became a magic key-concept that opens all the doors and enabled the *normalization* of measures that, until recently, were either non-existent or, at best, highly exceptional. In the name of the fight against terrorism, the US – and other liberal democracies including some European Union (EU) member states – used torture, targeted killings, indefinite detentions, warrantless wire-tapping, extraordinary renditions, and many other extra-judicial measures in a scale that would never be admitted by governments and constituencies in the pre-9/11 world. If it is obvious that surveillance, secrecy, intelligence and information gathering have existed for many decades, it is becoming increasingly clear that both the social and political acceptance of some counter-terrorism measures, as well as their scope and breadth, have changed the parameters of the debate surrounding the concepts of security, freedom, justice, and democracy.

This article focuses on the effects of what can be called the *Snowden affair*, i.e. the impact and the consequences of the

1 Nick Hopkins, Julian Borger and Luke Harding, "GCHQ: inside the top secret world of Britain's biggest spy agency" (*The Guardian*, 2 August 2013).

2 "'Key Partners': Secret Links Between Germany and the NSA" (*Der Spiegel*, 22 July 2013).

* The author would like to thank Sean Goforth, Åsne Kalland Aarstad and Romain Müller for useful comments and suggestions.

revelation of these secret programs by former National Security Agency (NSA) contractor Edward Snowden. More concretely, this article assesses this impact on the EU and on its relations with the US. It critically analyzes the context in which the EU operates in data-protection and counter-terrorism issues, an environment where national and supra-national levels of policy-making coincide and compete. It starts with an overview of the process through which those secret instruments have been revealed. It proceeds by analyzing the implications of their disclosure on international politics, with a focus on the EU and on its cooperation on counter-terrorism with the US. It places the important developments of the last two months against the backdrop of previous clashes between the EU and the US over data protection issues within the framework of US counter-terrorism measures. Finally, the article concludes by arguing that the EU should constitute an extra-layer of protection of fundamental rights and freedoms in Europe and should act preventively to provide cyber-security and respect of privacy in its territory. By failing in this task, the EU fails in a fundamental policy area and widens the gap between what its citizens expect and what it actually delivers.

The Process

Since 6 June 2013, the British newspaper *The Guardian* and its journalist Glenn Greenwald have been systematically publicizing classified information brought to them by Edward Snowden. Contrary to what succeeded with Bradley Manning, a US soldier charged with 22 crimes, including espionage,[3] for passing information to the website Wikileaks – which in turn uploaded it all without any critical filter – the procedure in the current Snowden affair has been more cautious. Following investigative journalistic standards, *The Guardian* consults with the US Government before publishing any story inviting comments or arguments about the need to suppress any information on the grounds of posing concrete threats to national security.[4] So far, the newspaper's editorial team has been reviewing these claims and rejected all of them because, arguably, the US Government has not presented any concrete evidence that the leaked information constitute a concrete security threat.[5]

The MSS revealed over the last two months show complex mechanisms of collection and storage of personal data, such as emails, phone and Skype conversations, and virtually the full web footprint of individuals around the globe. Most importantly, the data collection does not focus on specific suspect targets. Instead, the US preventively collect and store the private data of hundreds of millions of people in case any specific information is relevant in a possible future investigation. For this reason, among many others, the functioning of these systems is not based on any individual legal or judicial mandate and therefore their lawfulness is, at best, debatable. The complexity of this issue is enhanced by the secrecy in which these systems were created and implemented since 2007, and also by the fact that the NSA director James Clapper lied about them in front of the US Congress.[6] In a hearing before Senate Intelligence Committee on warrantless surveillance on 12 March 2013, when asked by Senator Ron Wyden if the NSA collected any type of data of millions of American, James Clapper said "no". In 4 August 2013, two months after the programs started to be undisclosed, it was revealed that members of the US Congress were also denied access to basic information about the NSA,[7] thus thickening the cloud of secrecy around this issue.

Implications

As expected, the revelations brought by Edward Snowden, and subsequent US Government statements, produced multiple consequences. Firstly, their impact has been felt in the US, where a robust public debate about the limits of secrecy, the extent of undercover counter-terrorism measures, the legality of data retention, and the inobservance of constitutional guarantees under the ever-legitimizing idea of countering the threat of terrorism unfolds, leading President Barack Obama to produce several statements. The Snowden affair bring new elements to question what Dana Priest and William Arkin call *Top Secret America*,[8] referring to the rise of a new America security state where the post-9/11 obsession with terrorism allowed the creation of an endless labyrinth made of government agencies, which include counter-terrorism teams and private contractors, and erode the usual mechanisms of supervision while spending billions of dollars.

Secondly, the impact was also felt outside the US. On one hand, the chase for Edward Snowden by US authorities led to frictions both with Russia, who eventually granted him temporary asylum, and with other countries that offered diplomatic protection after Snowden fled Hong Kong, where he was based at the time of the disclosures. On the other hand, many countries felt their national sovereignty was violated by US surveillance of their citizens. This includes EU member states. On 30 June the German magazine *Der Spiegel* revealed that the NSA was spying in the country to a higher degree than what was previously known,

3 Bradley Manning was charged with the majority of the crimes that he had been accused of, but not of "aiding the enemy".

4 Interview with Glenn Greenwald (*MSNBC*, 17 July 2013).

5 Idem.

6 After the Snowden revelations came public, Clapper apologized for the "clearly erroneous" answer. Kimberley Dozier, "James Clapper: Answer On NSA Surveillance To Congress Was 'Clearly Erroneous'" (*Huffington Post*, 2 July 2013).

7 Glenn Greenwald, "Members of Congress denied access to basic information about NSA" (*The Guardian*, 4 August 2013).

8 Dana Priest and William Arkin, *Top Secret America: The Rise of the New American Security State* (New York: Little, Brown and Company, 2011).

collecting 500 millions of German data connections,[9] in a scheme that targeted not only civilians not suspected of any crime, but also embassies, companies, and other institutions, leading Germany's Justice Minister, Sabine Leutheusser-Schnarrenberger, to say that these actions are "reminiscent of the actions of enemies during the cold war".[10] France and Luxembourg's Foreign Ministers, Laurent Fabius and Jean Asselborn, labeled the surveillance "unacceptable"[11] and "disgusting",[12] respectively.

The EU Conundrum

Perhaps more than the surveillance of the citizens of its member states, the revelation that US programs also directly spied on EU officials in Brussels and several EU embassies around the world, including the one in Washington, caused official EU outrage. Most importantly, in what regards the specific cases of EU facilities, it was not clear whether the surveillance was conducted by the NSA only, or also by the FBI and the CIA. As can be easily understood, there are neither counter-terrorism objectives nor concern with the protection of American citizens in these actions of espionage. Reacting to the news, European Parliament President, Martin Schulz, said he was "deeply worried and shocked about the allegations of US authorities spying on EU offices".[13] Many members of the European Parliament, European Commissioners, and other top-level practitioners expressed similar concerns.

Part of this reaction is explained by the surprise and disappointment regarding an attitude of an ally. Ever since the inception of the European integration project, the US has been EU's main ally and, for many decades, security in Europe has relied on the US military presence. But this surprise is also result of an EU intrinsic misconception about world politics that leads it to see international affairs through different lenses than many other countries, including some EU member states. Due to factors such as its *sui generis* political character, the characteristics of its foreign and security policies, and the maintenance of the majority of the European security portfolio within the realm of its member states, the EU tends to have an image of itself as an international actor at odds with what it actually projects to the outside world. EU's self-image is different from a self-image of a state that typically has security concerns that are wider and sharper than those of the EU. Seen from Brussels, the idea of an ally spying on the EU was unimaginable.

In the particular case of counter-terrorism cooperation with the US, which has been wide and multifaceted over the last 12 years, this misperception is notoriously problematic because it means that the EU has not learned from the past, when smaller but similar situations occurred. The next paragraphs will analyze the two major cases regarding privacy and data protection where the EU clashed with the US in recent years. This exercise is important because it enables a better understanding of what could be done differently by the EU in order to enhance the protection of fundamental rights of its own citizens.

The Passenger Name Record Agreement

The Passenger Name Record (PNR) is the record of a travel route of an individual or group stored in a computer reservation system. For each journey, the airline companies create these records about passengers so that airline professionals can manage the proceedings of a flight travel, including the connecting flights, special meal orders, and all the information that is provided when a flight reservation is operated. In the days following 9/11, the US increased the measures aimed at gathering data related with flights. The US Aviation and Transportation Security Act from November 2001 introduced a clause requiring that airlines conducting flights to, from or through the US provide access to PNR data upon request of US authorities. These data contained not only all the information related to the flight but also the personal data of the passengers, including address and credit card details.

By imposing this requirement, the US created problems for external countries. In the case of the EU, the main issue came from the incompatibility of that requirement with EU legislation on data protection, more specifically the European Parliament and Council Directive 95/46/EC from 24 October 1995 (Data Protection Directive). Specifically, the problem related to the fact that the US did not have sufficiently high standards of data protection. By this, it impended in the clause of article 25 n. 4 of the Data Protection Directive, which states that when the Commission finds that a third country does not ensure an adequate level of protection, member states shall take the measures necessary to prevent any transfer of data to the third country in question.

This created serious problems for the airline companies, which were caught between not providing the PNR to US authorities (therefore being subject to heavy fines) or violating the EU's Data Protection Directive. In an attempt to solve the quarrel and find a solution for the problem, the European Commission negotiated a transition period (during which the US norm did not apply) and drafted an agreement with the US. Another important fact is that the Commission faced severe opposition from the European Parliament, namely its Civil Liberties, Justice and Home Affairs Committee. In a letter of 23 March 2004, Member of the European Parliament (MEP) Johanna Boogerd-Quaak wrote that she was personally convinced that the

9 Laura Poitras, Marcel Rosenbach and Holger Stark, "Partner and Target: NSA Snoops on 500 Million German Data Connections" (*Der Spiegel Online International*, 30 June 2013).

10 Ian Traynor, "Berlin accuses Washington of cold war tactics over snooping" (*The Guardian*, 30 June 2013).

11 Josh Levs and Catherine E. Shoichet, "Europe furious, 'shocked' by report of U.S. spying" (*CNN*, 1 July 2013).

12 "EU concern over Der Spiegel claim of US spying" (*BBC*, 30 June 2013).

13 "EU officials furious over reports NSA bugged diplomatic offices on both sides of Atlantic" (*Associated Press*, 30 June 2013).

EU needed a focused approach that targeted terrorists and criminals and "not millions of normal citizens".[14] The European Parliament subsequently voted against the document on 31 March 2004. In this resolution the Parliament argued that the Commission had exceeded its powers and, most importantly, reserved the right to appeal to the Court of Justice of the European Union (CJEU) if the Commission adopted the draft decision.

In a ruling on 30 May 2006, the CJEU found that the first EU-US PNR Agreement entered in force incorrectly in the EU legal system. This was due to the fact that the agreement was wrongfully grounded on a legal disposition regarding transportation; although it indirectly related to transportation, its final aim was security-related and therefore should be treated under the intergovernmental proceedings prescribed for the third pillar.[15] After the CJEU ruling, EU-US negotiations resumed, this time conducted by the EU presidency, and a draft agreement was announced on 28 June 2007, leading to more opposition from the MEPs.[16] The opposition abated though, and the Council approved the agreement on 23 July 2007.[17]

After three years, the European Commission sketched out its global external PNR strategy. In *The global approach to transfers of Passenger Name Record (PNR) data to third countries,*[18] the Commission called for a renegotiation of the PNR agreements with the US, Australia, and Canada, while stating that the data transferred within the realm of these agreements should be used exclusively to fight terrorism.

These efforts notwithstanding, the Council adopted a decision on the conclusion of a new EU-US PNR agreement[19] that replaced the existing one and was eventually approved by the European Parliament on 19 April 2012. Its main innovations are a legally binding commitment from the US Department of Homeland Security to inform EU member states and authorities of any EU relevant intelligence breakthrough following analysis of PNR data; rights of access, rectification and erasure and the possibility to obtain administrative and judicial redress; and a limited usage of PNR data for a period of up to 10 years for transnational crime and 15 years for terrorism. After six months, personally identifiable information of PNR data would be masked and after five years PNR data would be moved to a dormant database with additional controls.[20] The new PNR entered into force on 1 June 2012.

The SWIFT Agreement

In order to better monitor terrorist financial transactions, the US created a secret program called Terrorist Financing Tracking Program (TFTP). Within this framework, US authorities would have the right to request financial data collected by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a Belgium-based company that serves as a global clearing house for financial transfers between banks. SWIFT secretly provided US authorities access to financial data. The scheme, commonly referred to as *the SWIFT affair*, became public with an investigative news report published by Eric Lichtblau and James Risen[21] in *The New York Times* in June 2006.

Given that a relevant part of the information accessed by the US related to EU citizens, the contents of the US TFTP raised serious criticism in the EU. The Article 29 Working Party, EU's data protection organization, investigated the agreement and found that SWIFT violated the EU Data Protection Directive. EU-US negotiations for a mutual SWIFT agreement commenced in July of 2009 and concluded in 30 November 2009, the day before the entry into force of the Treaty of Lisbon. Knowing that its consent would be necessary for the agreement, the European Parliament pressured SWIFT, the European Central Bank, and the Group of 10 Central Banks to ensure the personal data of EU citizens. The European Parliament had been adopting resolutions in 2006, 2007, and 2009 aimed at influencing the contents of the agreement that was being negotiated by the Council.

On top of this, the circumstance that the EU-US agreement had been signed on the day before the entry into force of the Treaty of Lisbon caused profound discontent in the European Parliament. Had it been concluded one day later, the proceeding would have been different and the Parliament's participation would have been mandatory.

The European Parliament voted the rejection of this agreement, known as SWIFT 1. This meant that a new agreement would have to be negotiated between the US and the EU, which occurred between March and 8 July 2010, date of the approval of SWIFT 2. A comparative analysis of the two SWIFT agreements reveals several changes, namely regarding the procedural structure, the legal technique, the guarantees and safeguard mechanisms, the rules on the transfer of data and issues of transparency and legal protection. The contentious negotiations and the inflexibility of the Parliament during the SWIFT agreement

14 Document available at statewatch [http://www.statewatch.org/news/2004/mar/JBQ-Brok.pdf].

15 Joined cases C-317/04 and 318/04, *Parliament vs Council of the European Union and Commission of the European Communities*.

16 "MEPs fear that new PNR agreement fails to protect citizens' data" (*European Parliament Press Release*, 12 July 2007).

17 "Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement)", *Official Journal* L 204/18, 4.8.2007.

18 "Communication from the Commission: On the global approach to transfers of Passenger Name Record (PNR) data to third countries" (European Commission, COM (2010) 492 final, 21 September 2010).

19 "Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security" (Council Decision 17434/11, Ref. JAI 862/USA 85/RELEX 1234/DATAPROTECT 139, Brussels, 13 December 2011).

20 "Frequently Asked Questions: Passenger Name Record" (Ref. Memo /12/258, Brussels, 19 April 2012).

21 Eric Lichtblau and James Risen, "Bank Data Is Sifted by U.S. in Secret to Block Terror" (*The New York Times*, 23 June 2006).

made it clear that an EU institution, vested with reinforced powers attributed by the Treaty of Lisbon can increase the democratic legitimacy of EU security action and the protection of fundamental rights of EU citizens.

Conclusion: Lessons Learned, Lessons not Learned

The EU has a history of clashing with the US over data protection measures that are allegedly used to fight terrorism. Some of the programs were being implemented by the US without the knowledge of the EU, who learned about their existence from the press, exactly as observed now during the Snowden affair. Although the US MSS revealed by Edward Snowden are wider than previous cases, they nevertheless exhibit similar patterns to disclosures during the SWIFT affair. These previous experiences with secret US data protection measures should have made the EU more proactive in fighting the continuous violation of fundamental rights of their citizens operated by the US.

Bearing in mind the complexity of these situations, there are some actions that may help prevent future intrusions. Firstly, the EU needs to advance its regulation on cyber-security and to define a better strategy for dealing with the challenges posed the current massive usage of web-based services. As in many other policy areas, the EU incapacity to develop a policy on cyber-security makes it vulnerable to other actors that anticipate the scenarios and turn the EU into a standard *follower* rather than a standard *setter*. Acting preventively in grey zones and emerging policy areas enables the EU to shape the course of events more efficiently that by reacting *a posteriori*.

Secondly, the EU needs to continue to develop itself as a security actor that operates within the law, not least within its own borders. During the recent weeks it was revealed that some member states, including the UK, France and Germany, used surveillance systems over their own citizens. A failure of the EU to deal with these cases will bring criticism equivalent to that launched against US privacy violations. The fact that EU member states act as *Big Brothers* in their territory should be investigated by the European Parliament and the CJEU to assess the conformity of these programs with the EU's Data Protection Directive and other legislation; after all, it is EU territory as well. This is the only way of ensuring that the EU can actually provide an extra layer of protection of fundamental rights in Europe.

Finally, in order to maximize opposition to "unacceptable" measures, the EU needs to make better use of all political resources available. Therefore, instead of releasing mere declarations or statements, the EU should focus on political measures in areas where its leverage is more visible. The launch of new EU-US free trade negotiations, agreed in February 2013 and scheduled for a few days after the US espionage on the EU was disclosed, provided an exceptional opportunity for the EU to raise the stakes of its protest and to have a serious impact on the US. Yet, despite threats of cancellation and some pressure for postponement made by Paris, negotiations for the most comprehensive Free Trade Agreement in the history of the transatlantic relationship started on the date scheduled, as if the trust between the parties had not been fundamentally shaken.

Faced by a complex international environment, conflicting interests, and a never-ending financial crisis, the EU's capacity to deal with difficult scenarios has been tested to a new extent by the Snowden revelations. Yet, effectively ensuring the protection of the fundamental rights of its citizens should be considered top-priority, and this requires more resources and more political will. The EU's peculiar political and legal nature requires it to provide additional protection of fundamental rights. Failing this challenge is to fail a vital objective of the European integration project.

EDITOR | Paulo Gorjão
ASSISTANT EDITORS | Kai Thaler • Sean Goforth
DESIGN | Atelier Teresa Cardoso Bastos

Portuguese Institute of International Relations and Security (IPRIS)
Rua da Junqueira, 188 - 1349-001 Lisboa
PORTUGAL

http://www.ipris.org
email: ipris@ipris.org

IPRIS Viewpoints is a publication of IPRIS.