EUROPEAN PARLIAMENT

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C:

CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens' fundamental rights

NOTE

Abstract

In light of the recent PRISM-related revelations, this briefing note analyzes the impact of US surveillance programmes on European citizens' rights. The note explores the scope of surveillance that can be carried out under the US FISA Amendment Act 2008, and related practices of the US authorities which have very strong implications for EU data sovereignty and the protection of European citizens' rights.

AUTHOR(S)

Mr Caspar BOWDEN (Independent Privacy Researcher)

Introduction by Prof. Didier BIGO
(King's College London /
Director of the *Centre d'Etudes sur les Conflits, Liberté et Sécurité* – CCLS, Paris, France).

Copy-Editing: Dr. Amandine SCHERRER
(*Centre d'Etudes sur les Conflits, Liberté et Sécurité* – CCLS, Paris, France)

Bibliographical assistance : Wendy Grossman

RESPONSIBLE ADMINISTRATOR

Mr Alessandro DAVOLI
Policy Department Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
E-mail: poldep-citizens@europarl.europa.eu

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

To contact the Policy Department or to subscribe to its monthly newsletter please write to:
poldep-citizens@europarl.europa.eu

Manuscript completed in MMMMM 200X.

This document is available on the Internet at:
http://www.europarl.europa.eu/studies

DISCLAIMER

for ε

CONTENTS

LIST OF ABBREVIATIONS

ACLU	American Civil Liberties Union
AUMF	Authorization to Use Military Force
CIA	Central Intelligence Agency
CNIL	Comité National pour l'Informatique et les Libertés
DPAs	Data Protection Authorities
EDPS	European Data Protection Supervisor
ENISA	European Network and Information Security Agency
FAA	Foreign Intelligence Surveillance Amendment Act (2008)
FBI	Federal Bureau of Investigation
FIVE EYES	UK, US, Canada, Australia, New Zealand: sharing intelligence under UKUSA
FISA	Foreign Intelligence Surveillance Act (1978)
FISC	Foreign Intelligence Surveillance Court
FISCR	Foreign Intelligence Surveillance Court of Review
NSA	National Security Agency
PAA	Protect America Act (2007)
SHA	EU-US Safe Harbour Agreement (2000)
TIA	Total Information Awareness
WP29	Article 29 Data Protection Working Party

EXECUTIVE SUMMARY

This Briefing note provides the LIBE Committee with background and contextual information on PRISM/FISA/NSA activities and US surveillance programmes, and their specific impact on EU citizens' fundamental rights, including privacy and data protection.

Prior to the PRISM scandal, European media underestimated this aspect, apparently oblivious to the fact that the surveillance activity was primarily directed at the rest-of-the-world, and was not targeted at US citizens. The note argues that the scope of surveillance under the *Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008* (FAA) has very strong implications on EU data sovereignty and the protection of its citizens' rights.

The first section provides **a historical account of US surveillance programmes**, showing that the US authorities have continuously disregarded the human right to privacy of non-Americans. The analysis of various surveillance programmes (Echelon, PRISM) and US national security legislation (FISA, PATRIOT and FAA) clearly indicates that surveillance activities by the US authorities are conducted without taking into account the rights of non-US citizens and residents. In particular, the scope of FAA creates a power of mass-surveillance specifically targeted at the data of non-US persons located outside the US, including data processed by 'Cloud computing', which eludes EU Data Protection regulation.

The second section gives **an overview of the main legal gaps, loopholes and controversies of these programmes and their differing consequences for the rights of American and EU citizens**. The section unravels the legal provisions governing US surveillance programmes and further uncertainties in their application, such as:

- serious limitations to the Fourth Amendment for US citizens
- specific powers over communications and personal data of "non-US persons";
- absence of any cognizable privacy rights for "non-US persons" under FISA

The section also shows that the accelerating and already widespread use of Cloud computing further undermines data protection for EU citizens, and that a review of some of the existing and proposed mechanisms that have been put in place to protect EU citizens' rights after data export, actually function as loopholes.

Finally, **some strategic options for the European Parliament are developed**, and related recommendations are suggested in order to improve future EU regulation and to provide effective safeguards for protection for EU citizens' rights.

INTRODUCTION

Background

This Briefing note aims at providing the LIBE Committee with background and contextual information on PRISM/FISA/NSA activities and US surveillance programmes and their impact on EU citizens' fundamental rights, including privacy and data protection.

On June 5th the *Washington Post* and *The Guardian* published a secret order made under s.215 of the PATRIOT Act requiring the Verizon telephone company to give the NSA details of all US domestic and international phone calls, and "on an ongoing basis". On June 6th the two newspapers revealed the existence of an NSA programme codenamed PRISM that accessed data from leading brands of US Internet companies. By the end of the day a statement from Adm. Clapper (Director of NSA) officially acknowledged the PRISM programme and that it relied on powers under the FISA Amendment 2008 s.1881a/702 (FAA). On June 9th Edward Snowden voluntarily disclosed his identity and a film interview with him was released.

In the European Parliament resolution of 4 July 2013 on the US National Security Agency surveillance programme, MEPs expressed serious concern over PRISM and other surveillance programmes and strongly condemned spying on EU official representatives and called on the US authorities to provide them with full information on these allegations without further delay. Inquiries by the Commission[1], Art.29 Working Party[2], and a few MS Parliaments are also in progress.

The problem of transnational mass surveillance and democracy[3]

Snowden's revelations about PRISM show that Cyber mass surveillance at the transnational level induces systemic breaches of fundamental rights. These breaches lead us to question the scale of transnational mass surveillance and its implications for our democracies.

> *"Our government in its very nature, and our open society in all its instinct, under the Constitution and the Bill of Rights automatically outlaws intelligence organizations of the kind that have developed in police states"* (Allen Dulles, 1963)[4]

> "*There's been spying for years, there's been surveillance for years, and so forth, I'm not going to pass judgement on that, it's the nature of our society*"
>
> (Eric Schmidt, Executive chairman of Google, 2013).

These two quotations are distinct in time by 50 years. They differ in the answers but address the same central question: how far can democratic societies continue to exist in their very nature, if intelligence activities include massive surveillance of populations? For Eric Schmidt and according to most of the media reports in the world, the nature of society has changed. Technologies of telecommunication, including mobile phones, Internet, satellites and more generally all data which can be digitalised and integrated into platforms, have given the possibilities of gathering unprecedented amount of data, to keep them, to organise them, to search them. If the technologies exist, then they have to be used: "it is not possible to go against the flow". Therefore it is not a surprise to discover that

---

[1]. European Commissioner - Reding, Viviane (2013), Letter to the Attorney General, Ref. Ares (2013)1935546 - 10/06/2013, Brussels, 10 June 2013

[2]. Article 29 Working Party, Letter from the Chairman to Mrs Reding regarding the PRISM program 13th August 2013

[3]. Preface by Prof.Didier Bigo

[4]. Dulles, Allen Welsh (1963), The Craft of Intelligence, New York: Harper&Row, p.257.

programmes run by intelligence services use these techniques at their maximum possibilities and in secrecy. The assumption is that if everyone else with these technical capabilities uses them, then we should too. If not, it would be naivety or even worse: a defeat endangering the national security of a country by letting another country benefit from the possibilities opened by these technologies.

However, should we have to live with this extension of espionage to massive surveillance of populations and accept it as "a fact"? Fortunately, totalitarian regimes have more or less disappeared before the full development of theses capacities. Today, in democratic regimes, when these technologies are used, they are limited on purpose and are mainly centred on antiterrorism collaboration, in order to prevent attempts of attacks. According to Intelligence Services worldwide, these technologies are not endangering civil liberties; they are the best way to protect the citizen from global terrorism. Intelligence services screen suspicious behaviours and exchange of information occurs at the international level. Only "real suspects" are, in principle, under surveillance. From this perspective, far from being a "shame", the revelations of programmes like PRISM could be seen as a proof of a good level of collaboration, which has eventually to be enhanced in the future against numerous forms of violence.

In front of this "recital" given by the most important authorities of the different intelligence services and the antiterrorists agencies in the US, in the UK, in France, and at the EU level, it is critical to discuss the supposedly new nature of our societies. The impact of technological transformations in democratic societies, how to use these technologies as resources for both information exchange and competition over information (a key element of a globalised world), what are the rights of the different governments in processing them: these are the core questions.

As stated by Allen Dulles above, justifications given by intelligence services work in favour of a police state and against the very nature of an open society living in democratic regimes. Proponents of an open society insist that, against the previous trend, technologies ought not to drive human actions; they have to be used in reasonable ways and under the Rule of Law. The mass scaling has to be contained. Constitutional provisions have to be applied, and the presumption of innocence is applicable for all human beings (not only citizens). If suspicions exist, they have to be related to certain forms of crime, and not marginal behaviours or life styles. Hence, what is at stake here is not the mechanisms by which antiterrorism laws and activities have to be regulated at the transatlantic level, even if it is a subset of the question. It is even not the question of espionage activities between different governments. **It is the question of the nature, the scale, and the depth of surveillance that can be tolerated in and between democracies.**

The Snowden's revelations highlight numerous breaches of fundamental rights. This affects in priority all the persons whose data have been extracted via surveillance of communications, digital cables or cloud computing technologies, as soon as they are under a category of suspicion, or of some interest for foreign intelligence purposes. However, all these persons are not protected in the same way, especially if they are not US citizens. **The EU citizen is therefore particularly fragile in this configuration connecting US intelligence services, private companies that provide services at the global level and the ownership they can exercise over their data**. It is clear that if EU citizens do not have the same level of protections as the US citizens, because of the practices of the US intelligence services and the lack of effective protections, they will become the first victims of these systems. Freedom of thought, opinion, expression and of the press are cardinal values that have to be preserved. Any citizen of the EU has the right to have a private life, i.e, a life which is not fully under the surveillance of any state apparatus. The investigative eyes of any government have to be strongly reminded of distinctions between private and public activities, between what is a crime and what is simply a different life-

style. By gathering massive data on life-styles in order to elaborate patterns and profiles concerning political attitudes and economic choices, PRISM seems to have allowed an unprecedented scale and depth in intelligence gathering, which goes beyond counterterrorism and beyond espionage activities carried out by liberal regimes in the past. This may lead towards an illegal form of Total Information Awareness where data of millions of people are subject to collection and manipulation by the NSA.

This note wants to assess this question of the craft of intelligence and its necessary limits in democracy and between them. As we will see, through the documents delivered by Snowden, the scale of the PRISM programme is global; its depth reaches the digital data of large groups of populations and breaches the fundamental rights of large groups of populations, especially EU citizens. The EU institutions have therefore the right and duty to examine this emergence of cyber mass-surveillance and how it affects the fundamental rights of the EU citizen abroad and at home.

Privacy governance: EU/US competing models

A careful analysis of US privacy laws compared to the EU Data Protection framework shows that the former allows few practical options for the individual to live their lives with self-determination over their personal data. However a core effect of Data Protection law is that if data is copied from one computer to another, then providing the right legal conditions for transfer exist, the individual cannot object on the grounds that their privacy risk increases through every such proliferation of "their" data[5]. This holds true if the data is copied onto a thousand machines in one organization, or spread onward to a thousand organisations, or to a different legal regime in a Third Country. The individual cannot stop this once they lose possession of their data, whereas for example if the data was "intellectual property", then a license to reproduce the data would be necessary by permission. We are all the authors of our lives, and it seems increasingly anomalous that Internet companies lay claim to property rights in the patterns of data minutely recording our thoughts and behaviour, yet ask the people who produce this data to sacrifice their autonomy and take privacy on trust.

The EU Data Protection framework in theory is categorically better than the US for privacy, but in practice it is hard to find any real-world Internet services that implement DP principles by design, conveniently and securely.

Privacy governance around the world has evolved around two competing models. Europe made some rights of individuals inalienable and assigned responsibilities to Data Controller organizations, whereas in the United States companies inserted waivers of rights into Terms and Conditions[6] contracts allowing exploitation of data in exhaustive ways (known as the 'Notice-and-Choice" principle).

The PRISM crisis arose directly from the emerging dominance over the last decade of "free" services operated from remote warehouses full of computer servers, by companies predominantly based in US jurisdiction, that has become known as Cloud computing. To explain this relationship we must explore details of the US framework of national security law.

Scope and structure

It is striking that since the first reports of "warrantless wiretapping" in the last decade, and until quite recently in the PRISM-related revelations, European media have covered US surveillance controversies as if these were purely parochial arguments about US civil

[5]. Hondius, Frits W (1975), Emerging data protection in Europe. North-Holland Pub. Co.
[6]. cf. the documentary "Terms and Conditions May Apply" (2013, USA) dir. Cullen Holback.

liberties, apparently oblivious that the surveillance activity was **directed at the rest-of-the-world**.

This note aims to document this under-appreciated aspect. It will show that the scope of surveillance conducted under a change in the FISA law in 2008 extended its scope beyond interception of communications to include any data in public cloud computing as well. This has very strong implications for the EU's continued sovereignty over data and the protection of its citizens' rights. The aim is here to provide a guide to how surveillance of Internet communications by the US government developed, and how this affects the human right to privacy, integrating historical, technical, and policy analysis from the perspective of the individual EU citizen[7]. The Note will therefore cover the following:

- (I) An account of US foreign surveillance history and current known state
- (II) An overview of the main legal controversies both in US terms, and the effects and consequences for EU citizens' rights
- (III) Strategic options for the European Parliament and recommendations

1. HISTORICAL BACKGROUND OF US SURVEILLANCE

KEY FINDINGS

- A historical account of US various surveillance programmes (precursors to Echelon, PRISM, etc.) and US legislation in the field of surveillance (FISA and FAA) shows that the **US has continuously disregarded the fundamental rights of non-US citizens**.
- In Particular, the scope of FAA coupled with expressly 'political' definitions of what constitutes '*foreign intelligence information*' creates **a power of mass-surveillance specifically targeted at the data of non-US persons** located outside the US, which eludes effective control by current and proposed EU Data Protection regulation.

A historical account of US surveillance programmes provides the context for their interpretation as the latest phase of a system of US exceptionalism, with origins in World War II. These programmes constitute the greatest contemporary challenge to data protection, because they incorporated arbitrary discriminatory standards of treatment strictly according to nationality and geopolitical alliances, which are secret and incompatible with the rule of law under EU structures.

1.1. World War II and the origins of the UKUSA treaties

In the 1970s there were the first disclosures of the extent of Allied success in WWII cryptanalysis. The world discovered the secret history of Bletchley Park (aka Station X), Churchill's signals intelligence headquarters. The story of post-war secret intelligence

[7]. New stories based on Snowden's material were breaking throughout the drafting of this Note and whilst every effort has been made to ensure accuracy, it is possible that further revelations could change the interpretations given.

partnerships at the international level is intertwined with the personal trajectory of Alan Turing, a great mathematician and co-founder of computer science, who was critical to the effort to design automated machines which could feasibly solve ciphers generated by machine, such as Enigma (used for many Nazi Germany communications).

Alan Turing travelled to the US in 1942 to supervise US Navy mass-production of the decryption machines (called 'bombes') for the Atlantic war, and to review work on a new scrambler telephone at Bell Laboratories to be used for communications between Heads of Government. Unfortunately Turing was not equipped with any letters of authority, so he was detained by US immigration as suspicious until rescued by UK officials in New York. What was initially supposed to be a two-week trip turned into months, as no precedent existed to grant even a foreign ally security clearance to the laboratories he was supposed to visit. There followed several months of fraught UK diplomacy and turf wars between the US Navy and Army, since the latter had no "need-to-know" about Ultra (the name given to intelligence produced from decryption at Bletchley). The UK wanted as few people as possible in on the secret, and the disharmony thus experienced inside the US military security hierarchies became known as "the Turing Affair".

These were the origins of the post-war secret intelligence partnership between the US and UK as "first" parties, Canada/Australia/New Zealand as second parties, and other nations with lesser access as third parties. The treaty is named UKUSA, and we know the details above about its genesis because in 2010 the US National Security Agency declassified the unredacted text of UKUSA treaties[8] up until the 1950s with related correspondence (the current text is secret). GCHQ[9] did not declassify much in comparison, although the occasion was billed as joint exercise.

The purpose of the UKUSA treaties was to **establish defined areas of technical co-operation and avoid conflicts. However, no general "no spy" clause appears in the versions published up until the 1950s, but expressions of amity comparable to public treaties**. It is not known whether any comprehensive secret "no spy" agreement exists today between the UK and US, and neither has ever given legislative or executive comment on the matter.

1.2. ECHELON: the UKUSA communications surveillance nexus

From the founding of the US National Security Agency (NSA) in 1952 throughout the Cold War, both the UK and US vastly expanded their signal intelligence capacities, collecting from undersea cables at landing points[10], satellites intercepting terrestrial microwave relays, and arrays of antennae usually sited in military bases and embassies. The evolution and nature of these capabilities were documented from open source research in two reports[11] to the European institutions culminating in the Parliament's inquiry into ECHELON in 2000. ECHELON was in fact a codeword for one particular surveillance system, but became in common usage a synecdoche for the entire UKUSA communications surveillance nexus. The last meeting the EP inquiry committee was on September 10, 2001. The

[8]. UKUSA Agreement Release 1940-1956 Early Papers Concerning US-UK Agreement – 1940–1944, NSA/CSS

[9]. Government Communications Head-Quarters, the UK national cryptologic and information national security surveillance organisation, the descendent organisation from Bletchley Park.

[10]. This practice started with the earliest cables for telegraphy in the 19th century and was a crucial aspect of Zimmerman Telegram affair which was influential in persuading America to join WW1. See: Desai, Anuj C. (2007), Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy, Stanford Law Review, 60 STAN L. REV. 553 (2007).

[11]. STOA interception Capabilities 2000) and EuroParl ECHELON (2001) - reports by Duncan Campbell.

Committee recommended to the European Parliament that **citizens of EU member states use cryptography in their communications to protect their privacy**, because economic espionage with ECHELON had obviously been conducted by the US intelligence agencies.

1.3. 1975-1978: Watergate and the Church Committee

After the US was convulsed by the Watergate scandal culminating in the resignation of Richard Nixon, Senator Frank Church led a Congressional committee of inquiry into abuses of power by law-enforcement and intelligence agencies which had conducted illegal domestic wire-tapping of political and civic leaders under presidential authority, and contrary to the Fourth Amendment of the US constitution which protects privacy against unreasonable searches without a particular warrant, issued on "probable cause" (meaning evidence of a 50% likelihood of criminality).

The Church inquiry reported on the question of whether the Fourth Amendment restricts the mass-trawling and collection of international communications, which they discovered had been secretly conducted since the 1940s on telegrams[12]. The inquiry canvassed that **inadvertent collection of Americans' data transmitted internationally was tolerable**, if procedures were made for "minimization" of erroneous unwarranted access (and mistakes not used prejudicially against Americans).

This idea was codified into the first **Foreign Intelligence Surveillance Act of 1978 (FISA)**, which regulated the interception of international (and domestic) "foreign intelligence information" from telecommunications carriers. Collection of data by any nation from outside its territory is literally lawless and not restricted by any explicit international agreements.

1.4. The post-9/11 context: extension of intelligence powers

After the terrorist attacks of September 9/11, privacy and data protection has been deeply challenged by exceptional measures taken in the name of security and the fight against terrorism.

The USA PATRIOT Act of 2001 was voted by the US Congress on October 26, 2001, and its primary effect was to greatly extend law enforcement agencies' powers for gathering domestic intelligence inside the US. The revised **Foreign Intelligence Surveillance Amendment Act of 2008 (FAA)[13]** created a power of mass-surveillance specifically targeted at the data of non-US persons located outside the US. These aspects and their implications for EU citizens will be analysed in the following section (Section 2).

Numerous new surveillance programmes and modalities were further suggested to President Bush by NSA Director Gen. Hayden, without explicit authorization under statute, and approval was nevertheless given. Those programmes were retroactively deemed lawful in secret memoranda prepared by a relatively junior legal[14] official, under the *Authorisation*

---

[12]. No formal authority for the SHAMROCK collection (or sister MINARET trawling) programme existed but at the government's request a tape of all cables was delivered by courier every day to the NSA. See Snider, Britt L. (1999): Unlucky SHAMROCK - Recollections from the Church Committee's Investigation of NSA.

[13]. US Congress (2008), Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, 122 Stat. 2436, Public Law 110-261, July 10, 2008.

[14]. John Yoo, who similarly gave a secret opinion that water-boarding was not torture and thus permissible.

to Use Military Force (AUMF) for the war in Afghanistan and associated War on Terror operations.

Amongst these programmes was one codenamed *Stellar Wind* which involved placing fibre-optic cable "splitters" in major Internet switching centres, and triaging the enormous volumes of traffic in real-time with a small high-performance scanning computer (known as a deep-packet inspection box), which would send data filtered by this means back to the NSA. An AT&T technical supervisor in the San Francisco office was asked to assist in constructing such a facility ("Room 641A") and was concerned that this activity manifestly broke US Constitutional protections, because the cable carried domestic as well as international traffic. He took his story with documentation to the *New York Times*, which did not publish[15] the story for a year, until 2005 after the re-election of President Bush.

Other whistle-blowers from the NSA, CIA and FBI emerged with tales of illegal mass-surveillance via mobile phones, the Internet and satellites, and even revealed that phone calls of Barack Obama[16] (he was then Senator) and Supreme Court judges had been tapped. The controversy was exacerbated because two years before, a former National Security Adviser[17] had proposed a research programme for *Total Information Awareness* - T.I.A., a massive system of surveillance of all digital data, processed with advanced artificial intelligence algorithms to detect terrorist plots. Immediate adverse media commentary prompted the US Congress to de-fund research into T.I.A., but rumours persisted that it had been absorbed into an intelligence "black budget".

When the "warrantless wiretapping" allegations surfaced in a series of press reports from *The New York Times*, *The Los Angeles Times*, and *The Wall Street Journal*, the resonance with the supposedly cancelled T.I.A project intensified the level of public unease.

1.5. Edward Snowden's revelations and PRISM

On June 5th *The Washington Post* and *The Guardian* published a secret order made under s.215 of the PATRIOT Act requiring the Verizon telephone company to give the NSA details of all US domestic and international phone calls, and "on an ongoing basis". On June 6th the two newspapers revealed the existence of an NSA programme codenamed PRISM, which accessed data from leading brands of US Internet companies. By the end of the day a statement from Adm.Clapper (Director of NSA) officially acknowledged the PRISM programme and that it relied on powers under the FISA Amendment 2008 s.1881a/702. On June 9th Edward Snowden voluntarily disclosed his identity and a film interview with him was released.

The primary publication was in three newspapers: *The Guardian*, *The Washington Post*, and *Der Spiegel*. Four journalists have played a central role in obtaining, analysing and interpreting this material for the public: Barton Gellman, Laura Poitras, Jacob Appelbaum and Glenn Greenwald. They were joined by *The Guardian* (US edition), the *New York Times* in conjunction with *ProPublica* after the UK government insisted on destruction of *The Guardian*'s copy of the Snowden material in their London offices, under the supervision of GCHQ[18].

---

[15]. *New York Times*, Bush Lets U.S. Spy on Callers Without Courts, Risen J, Lichtblau E, December 16, 2005.
[16]. *Huffington Post*, Russ Tice, Bush-Era Whistleblower, Claims NSA Ordered Wiretap Of Barack Obama In 2004, 20th June 2013.
[17]. Admiral John Poindexter, convicted in the Iran/Contra affair of the 1980s and pardoned by President Reagan.
[18]. It is outside the scope of this report to give a full analysis of what has been revealed, but in what follows it is assumed that the slides and documents are authentic, and no serious suggestions have been made to the contrary.

What can be referred to as the 'PRISM scandal' revealed a number of surveillance programmes, including:

1.5.1 "Upstream"

The slides published from the Snowden material feature references to "Upstream" collection programmes by the NSA adumbrated by various codewords. Data is copied from both public and private networks to the NSA from international fibre-optic cables at landing points, and from central exchanges which switch Internet traffic between the major carriers, through agreements negotiated with (or legal orders served on) the operating companies (and probably also by intercepting cables on the seabed[19] when necessary).

1.5.2 XKeyscore

The XKeyscore system was described in slides[20] (dated 2008[21]) published by *The Guardian* on the 31st of July. It is an "exploitation system/analytic framework", which enables searching a "3 day rolling buffer" of "full take" data stored at 150 global sites on 700 database servers. The system integrates data collected[22] from US embassy sites, foreign satellite and microwave transmissions (i.e. the system formerly known as ECHELON), and the "upstream" sources above.

The system indexes e-mail addresses, file names, IP addresses and port numbers, cookies, webmail and chat usernames and buddylists, phone numbers, and metadata from web browsing sessions (including words typed into search engines and locations visited on Google Maps). The distinctive advantage of the system is that it enables an analyst to discover "strong selectors" (search parameters which identify or can be used to extract data precisely about a target), and to look for "anomalous events" such as someone "using encryption" or "searching for suspicious stuff".

The analyst can use the result of these index searches to "simply pull content from the site as required". This system of unified search allows retrospective trawling through 3 days (as of 2008) of a much greater volume of data than is feasible to copy back to the NSA.

The system can also do "Persona Session Collection" which means that an "anomalous event" potentially characteristic of a particular target can be used to trigger automatic collection of associated data, without knowledge of a "strong selector". It is also possible to find "all the exploitable machines in country X" by matching the fingerprints of configurations which show up in the data streams captured, with NSA's database of known software vulnerabilities. The slides also say it is possible to find all Excel spreadsheets "with MAC addresses coming out of Iraq"[23].

Slide 17 is remarkable because it contained the first intimations of systemic compromise of encryption systems[24] (see BULLRUN below).

---

[19]. The existence US submarines specially equipped for intercepting undersea cables was outlined in the 2000 EP ECHELON report cf. "Ivy Bells"

[20]. http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-programme-full-presentation

[21]. A job advertisement was posted by a defence contractor in July 2013 indicating the programme is still active.

[22]. http://theweek.com/article/index/247684/whats-xkeyscore

[23]. This seems anomalous because ostensibly Microsoft stopped incorporating the MAC address in the GUID (Global Unique Identifier – a way of generating a unique document index number) with Office 2000, and MAC addresses are not correlated to a particular country (unless somehow the NSA has obtained a comprehensive database or built one somehow specially for Iraq or is able to monitor and collect WiFi signals at long range and/or systematically).

[24]. "Show me all the VPN startups in country X, and give me the data so I can decrypt and discover the users" - a VPN (Virtual Private Network) is an "encrypted tunnel" between the user's computer and a VPN provider, so

1.5.3 BULLRUN

BULLRUN[25] is the codename for a NSA programme for the last decade for an "aggressive multi-pronged effort to break into widely used encryption technologies", revealed in a joint *Guardian*[26]/*New York Times* story on September 1st. This programme has caused the greatest shock amongst the Internet technical security community of all the Snowden material so far, and frantic efforts are underway worldwide to assess which systems might be vulnerable, and to upgrade or change keys, ciphers and systems, not least because adversaries in hostile countries will now be trying to discover any backdoor mechanisms previously only known by the NSA.

The programme budget is $250m per annum, and may use some of the following methods: collaboration with vendors of IT security products and software, mathematical cryptanalysis and "side-channel" attacks, forging of public-key certificates, infiltrating and influencing technical bodies towards adopting insecure standards, and likely use of coercive legal orders to compel introduction of "backdoors". It is important to stress that no evidence has emerged (yet) that the fundamental cipher algorithms in common use have been broken mathematically, however over the past few years doubts have grown about vulnerabilities in the complex "protocols" used to set-up and ensure compatibility amongst the software in common use.

FISA 702 may require a service provider to *"immediately provide the government with all information, facilities, or assistance necessary to accomplish the acquisition"* of foreign intelligence information, and thus on its face could compel disclosure of cryptographic keys, including the SSL keys used to secure data-in-transit by major search engines, social networks, webmail portals, and Cloud services in general. It is not yet known whether the power has been used in this way.

Internet traffic notionally appears to originate from the VPN provider rather than the user, for privacy and security reasons.

[25]. The corresponding codename of the similar GCHQ cryptographic penetration programme is EDGEHILL, curiously both names of battles from each country's civil war, and is outside the scope of this Note.

[26]. http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

2. NSA PROGRAMMES AND RELATED LEGISLATION: CONTROVERSIES, GAPS AND LOOPHOLES AND IMPLICATIONS FOR EU CITIZENS

KEY FINDINGS

- The complexity of inter-related US legislation pertaining to 'foreign intelligence information', and its interpretations by secret courts and executive legal memoranda, has led to unlawful practices **affecting both US citizens and non-US citizens**.
- The consequences of this legal uncertainty, and lack of Fourth Amendment protection for non-US citizens, means that **no privacy rights for non-Americans are recognized** by the US authorities under FISA
- The accelerating and already widespread use of **Cloud Computing further undermines data protection for EU citizens**.
- A review of the mechanisms that have been put in place in the EU for data export to protect EU citizens' rights shows that they actually **function as loopholes**.

When analysing known US surveillance programmes and related legislation from a Fundamental Rights perspective, the legal 'grey areas' fall into two categories, which constantly interact[27]:

- a lack of legal certainty resulting in privacy invasions and other potential abuses and malpractices inside the US, through ostensibly unintended effects on American citizens and legal residents;
- the intent of the US FISA (and PATRIOT) laws to acquire "foreign intelligence information', concerning people who are not American citizens or legal residents.

2.1. Legal gaps and uncertainties of US privacy law: implications for US citizens and residents

2.1.1 The Third Party Doctrine and limitations to the Fourth Amendment

In two US cases in 1976 and 1979 the legal doctrine was established that for personal data entrusted to, or necessary to use a service provided by, a "third party" such as a bank or telephone company, there was no reasonable expectation of privacy, and therefore no warrant was required by the Fourth Amendment, which protects privacy against unreasonable searches without a particular warrant, issued on "probable cause" (meaning

evidence of a 50% likelihood of criminality). Consequently such business records as credit-card transactions, bank statements, and itemized phone bills can be obtained by law enforcement authorities through administrative procedures authorized by the law enforcement agency rather than an independent judge, and no "probable cause" has to be evidenced.

This doctrine has been subject to continuous criticism throughout the development of mobile communications which track individuals' location, Internet services which record of website browsing and search-engine activity, and social networks in which merely the structure of and dynamics social interaction reveal intimate[28] details of private life[29]. Obviously these conditions could not have been foreseen by courts in the 1970s, yet every challenge so far to overturn the doctrine has been unsuccessful.

Such privacy concerns were increased by s.215 of the PATRIOT Act 2001, that attracted considerable controversy. It allows security authorities to obtain "tangible" business records from companies under a secret judicial order. Although secret *non*-judicial orders to obtain "non-content" data (i.e. "metadata") were already available under a procedure called a 'National Security Letter', s.215 is applicable to any kind of "tangible" data held by a great variety of private-sector businesses.

After the first revelations about the PRISM programme, Gen. Alexander (Director of the NSA) confirmed over two public hearings of Congressional intelligence review committees that the NSA collects (both domestic and international) telephone call metadata from all major carriers and maintains a database of all such calls for five years[30]. By the NSA's own account it uses this data for the sole purpose of deciding whether there is a "reasonable articulable suspicion" of a connection to a terrorist investigation. The database is searched for whether a candidate target telephone number is within "three hops" (i.e. when there exists a "chain" of calls sometime over a 5 year period) to a nexus of numbers previously associated with terrorism.

2.1.2 CDRs and the 'Relevance Test'

So far, the greatest legislative controversy in the US about Snowden's revelations is not in fact about PRISM, but about the indiscriminate blanket collection of all telephone metadata (CDRs - call-detail-records), which appears to exceed the terms of the PATRIOT statute. Data can only be acquired under s.215 in the first place if it meets the standard that it must be "relevant" to an authorised investigation. The PATRIOT Act was amended in 2006 to include the relevance standard, with the intention of limiting the collection of data[31], but it appears to have been interpreted as a justification for massive data collection.

---

[27]. Forgang, Jonathan D., (2009), "The Right of the People": The NSA, the FISA Amendments Act of 2008, and Foreign Intelligence Surveillance of Americans Overseas, Fordham Law Review, Volume 78, Issue 1, Article 6, 2009.

[28]. Agarwal, A., Rambow, O. & Bhardwaj, N. (2009) Predicting Interests of People on Online Social Networks, CSE 2009: International Conference on Computational Science and Engineering.

[29]. Mislove, A., Viswanath, B., Gummadi, K.P. & Druschel, P. You are who you know: inferring user profiles in online social networks, Proceedings of the Third ACM International Conference on Web Search and Data Mining ACM, 2010, pp. 251-260.

[30]. The New York Times revealed on 1st September, from a different source than Snowden that the company AT&T has retained records of all long-distance and international calls since 1987, and provides these records to US Drug Enforcement Agency investigations under a secret programme codenamed HEMISPHERE. Retention of such records in the EU, beyond the 2-year maximum specified in the Data Retention Directive 2006, would be illegal under the e-Privacy 2002 Directive (and earlier 1998 "ISDN" Directive) requirement for such data to erased or made anonymous when any legitimate business purpose has expired.

[31]. According to Rep. Sensenbrenner, Patriot Act Architect Criticizes NSA's Data Collection, NPR August 20th 2013.

The rationale behind this collection is therefore questionable: how is it possible to justify collection of the entire database in the first place, on the basis of establishing that a particular suspect's number has a 3-hop connection to terrorism? As expressed succinctly by one advocate: *"they were conducting suspicion-less searches to obtain the suspicion the FISA court required to conduct searches"*[32].

Problems that emerged from FISA were left to the interpretation (in secret proceedings) of the *Foreign Intelligence Surveillance Court* (FISC and the higher Review court FISCR) whose judges are appointed solely by the Chief Justice of the Supreme Court. It appears that the FISA courts agree with the government's argument that it is common in investigations for some indefinitely large corpus of records to be considered "relevant", in order to discover the actual evidence. Some official declassifications of the secret FISC(R) Opinions are in progress, but have not so far explained this logical anomaly.

2.1.3 'Direct Access' to data-centres granted for surveillance purposes?

The companies named in the PRISM slides issued prompt denials of "direct access" to their datacentres, mentioned in the "marketing" slides that revealed PRISM's existence. Their position was that they were simply complying with a mandatory court order, and they had never heard of the PRISM codename (which is not surprising since this was an NSA codeword for a Top Secret programme). Microsoft asserted that they only responded to requests referencing specific account identifiers, and Google and Facebook denied they had "black boxes" stationed in their networks giving "direct access". The companies are constrained by the secrecy provisions of s.702, on pain of contempt or even espionage charges[33]. Google and Microsoft are now suing the government for permission to publish a breakdown of the number of persons affected by FISA orders.

However there is no substantive inconsistency between the carefully wordsmithed (and apparently co-ordinated[34]) company denials and the reports of PRISM. The phrase "direct access" was likely intended to distinguish this modality from "upstream" collection (see above), not necessarily implying a literal capability to extract data without the company's knowledge. However, such literal "direct access" is not precluded by the 702 statute, and it may be that this has already occurred with some other companies, or may in future be permitted by the FISC.

A critical further development resulted from a keen observation by *The New York Times*[35] on August 8th that in the targeting procedures published on June 20th, the "selectors" used to specify the information to be accessed under 702 could include arbitrary search terms. This ought not to be surprising from a plain reading of the statute, but it emphasized that Americans' (and of course non-Americans') privacy could be implicated in arbitrary trawls through a mass of data, rather than access being confined to account identifiers judged 50% likely to be non-American. A further story disclosed[36] that at the government's request in 2011 the FISA court reversed an earlier ruling and thenceforth permitted arbitrary search terms **even if** these included targeting factors characteristic of Americans.

---

[32].https://www.eff.org/deeplinks/2013/09/government-releases-nsa-surveillance-docs-and-previously-secret-fisa-court

[33]. http://www.theguardian.com/technology/2013/sep/11/yahoo-ceo-mayer-jail-nsa-surveillance

[34]. The phrasing of statements from Google and Facebook have many concordances which strongly suggest they are derived from a common text.

[35].http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?pagewanted=1&hp

[36].http://www.washingtonpost.com/politics/federal_government/report-surveillance-court-ruling-allowed-nsa-search-of-domestic-email/2013/09/08/4d9c8bb8-18c0-11e3-80ac-96205cacb45a_story.html

Thus it appears that the theoretical protections, which in law existed only for Americans, have been very substantially undermined[37] by successively expansive government requests to the court.

2.1.4 Intelligence Agencies' 'Black Budget': scale and costs of US capabilities

On August 31st, *The Washington Post* published details from the secret ("black") budget[38] of the US intelligence community, which amounted to $50bn per annum, together with a breakdown of expenditure into various categories. It was reported that the US had spent $500bn on secret intelligence since 9/11. The NSA's budget is about $10bn per annum, but it surprised commentators that the CIA's budget has rapidly grown to $15bn, exceeding that of the NSA.

2.2. Situation of non-US citizens and residents (non 'USPERs')

It is striking that so far in the evolution of the 'Snowden affair', domestic US political commentary has almost exclusively referred to the rights of *Americans*. This is not a rhetorical trope and is meant literally - no reciprocity ought to be assumed[39] (in law or popular discourse) which extends rights further[40]. The rights of non-Americans have scarcely been mentioned in the US media[41] or legislature. It is even more surprising that careful analysis of the FISA 702 provisions clearly indicates that there exist two different regimes of data processing and protection: one for US citizens and residents ("USPERs"), another one without any protection whatsoever for non-US citizens and residents ("non-USPERs").

2.2.1 The political definitions of 'foreign information intelligence'

The FISA definition of "foreign intelligence information" has been amended several times to include specific and explicit categories for e.g. money laundering, terrorism, weapons of mass-destruction, but has always included two limbs which seem almost unlimited in scope. When the terms are unwound it includes[42]:

> *information with respect to a foreign-based political organization* ***or*** *foreign territory that* ***relates*** *to, and if concerning a United States person is* ***necessary*** *to the conduct of the foreign affairs of the United States.* [emphasis added]

This definition is of such generality that from the perspective of a non-American it appears **any data of assistance to US foreign policy is eligible, including expressly political surveillance over ordinary lawful democratic activities**.

---

[37]. Cloud, Morgan (2005), A Liberal House Divided: How the Warren Court Dismantled the Fourth Amendment, Ohio State Journal of Criminal Law, Vol 3:33 2005.

[38].http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html

[39]. Corradino, Elizabeth A., (1989), Fordham Law Review, The Fourth Amendment Overseas: Is Extraterritorial Protection of Foreign Nationals Going Too Far? Volume 57, Issue 4, Article 4, January, 1989.

[40]. Cole, David, (2003), Georgetown Law: The Scholarly Commons, Are Foreign Nationals Entitled to the Same Constitutional Rights As Citizens? 25 T. Jefferson L. Rev. 367-388.

[41].Kenneth Roth (Dir, of Human Rights Watch) 4th September 2013: "...recognize the privacy rights of non-Americans outside the United States".

[42]. 50 USC §1801(e)2(B) - http://www.law.cornell.edu/uscode/text/50/1801

2.2.2 Specific powers over communications of non-US persons

To end the public controversy[43] over "warrantless wiretapping" of Americans, the US Congress enacted[44] the interim Protect America Act (PAA) in 2007, which amended FISA 1978, and created a new power targeted at the communications of non-US persons located outside the territory of the US (i.e. the 95% of the rest-of-the-world). The most heated political difficulty was over whether telecommunications companies had broken statute law regulating the privacy of their subscribers by co-operating. Depending on the contested legitimacy of the use of the *Authorization for Use of Military Force* (AUMF) to effect surveillance, which had impinged on Americans, the companies were potentially liable for billions of dollars of damages. The telecommunications companies and the Internet service providers industry were adamant that complete civil immunity was their price for future co-operation. It is here critical to underline that this controversy was about the effects on the privacy of Americans, and that the surveillance of foreigners outside the US, through their communications routed to **or via** the US, was an assumed *fait accompli* and national prerogative[45].

2.2.3 The Fourth Amendment does not apply to non-USPERs outside the US

The connection between the controversy over the s.215 PATRIOT Act power and the use of the FISA 702 power in the PRISM programme can now be explained. The database of 5 years of details of domestic and international calls was used to establish a counter-terrorist justification (according to the "three hops" principle). A second database was then checked of a directory the NSA maintains of telephone numbers believed to belong to Americans. If that check indicated the number was probably not that of an American, then the contents of that telephone call could be listened to with any further authorisation, under the FISA 702 law. Otherwise, if the number seemed probably that of an American, a further particular warrant for the interception would have to be obtained (under a different section of FISA), justifying the intrusion to a much higher legal standard, and with reference to the circumstances of the individual case.

However a close reading of the s.215 shows that an alternative purpose (other than a connection to terrorism) is *"to obtain foreign intelligence information not concerning a United States person"*[46]. From a non-US perspective this may be an important point which has not so far featured in any of the analysis made in the US, nor is it clear how this provision would interact with the already tangled skein of contested legality. However it is **a further illustration of US legislation, which discriminates between the protections afforded by the Constitution to its own citizens, and everybody else**.

Some remarkable interviews have been given by former NSA Director Gen. Hayden, in which he stressed that "*the Fourth Amendment* - that prohibits unreasonable searches and seizures and requires any warrant to be judicially sanctioned and supported by probable cause - *is not an international treaty*"[47], and that the US enjoys a "home field advantage" of untrammelled access to foreign communications routed via US territory, or foreign data stored there.

---

[43]. Bloom, Stephanie Cooper (2009), What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform, Public Interest Law Journal Vol 18:269.
[44]. Congressional Research Service (2007), P.L. 110-55, the Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act, August 23, 2007.
[45]. Congressional Research Service (2007), P.L. 110-55, the Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act, August 23, 2007 and Congressional Research Service – Liu, Edward C. (2013), Reauthorizattion of the FISA Amendments Act, 7-5700, R42725, January 2, 2013.
[46]. http://www.law.cornell.edu/uscode/text/50/1861
[47]. CBS News 30th June 2013; for further discussion see YOUNG (2003) Op.cit.

These statements sit uncomfortably with speeches and statements made by US State Department officials prior to 2012 at fora including the Council of Europe's "Octopus" conference on Cybercrime, and the annual International Conference of Privacy and Data Protection Commissioners. These statements lauded the protections afforded by the Fourth Amendment[48], and since they were directed at an international audience to provide re-assurance about America's respect for privacy, in retrospect they can only be construed as deceptive[49]. The author publicly challenged one representative in 2012 to state categorically that the Fourth Amendment applied to non-US persons (located outside the US), and they fell silent.

2.2.4 Cloud computing risks for non-US persons

The interim Protect America Act of 2007 law mentioned above was set to expire shortly before the Presidential election of 2008, and its scope was limited to interception of telephony and Internet access providers. Candidate-in-waiting Obama gave his approval to a bipartisan agreement to put PAA and its immunities for telecommunications companies on a permanent basis with the FISA Amendment Act 2008, which was enacted in July 2008.

When FAA was introduced, it contained an extra three words that apparently went unnoticed and unremarked by anyone[50]. By introducing "remote computing services" (a term defined in ECPA 1986 dealing with *law enforcement* access to stored communications), **the scope was dramatically widened from Internet communications and telephony to include Cloud computing.**

Cloud computing can be defined in general terms as the distributed processing of data on remotely located computers accessed through the Internet. From 2007 Internet industry marketing evangelized the benefits of Cloud computing to business, governments and policy-makers, beginning with Google and then rapidly followed by Microsoft and others, becoming a new business software sector.

In 2012 the LIBE Committee commissioned a briefing Note on "Fighting Cybercrime and Protecting Privacy in the Cloud" from the *Centre for European Policy Studies* (CEPS) and the *Centre d'Etudes sur les Conflits, Liberté et Securité* (CCLS), to which the author was invited to contribute[51]. Sections of the Note **clearly asserted that Cloud computing and related US regulations presented an unprecedented threat to EU data sovereignty**.

The Note specifically underlined[52] the following:

- *(Cloud providers) cannot fulfil any of the privacy principles on which Safe Harbour is founded. This was never satisfactorily resolved by the Commission before the agreement was hastily concluded over the objections of European DPAs. As a result many US cloud providers advertise Safe Harbour certification with insupportable*

---

[48]. See: Medina, M. Isabel, (2008) Indiana Law Journal, Exploring the Use of the Word "Citizen" in Writings on the Fourth Amendment Volume 83, Issue 4, Article 14, January, 2008.

[49]. In U.S. Ambassador to the EU (2012), Remarks by William E Kennard, Forum Europe's 3rd Annual European Data Protection and Privacy Conference, December 4, 2012, the assurances given regarding criminal law do not apply to FISA, which is unmentioned, see similarly: US State Department (2012), Five Myths Regarding Privacy and Law Enforcement Access to Personal Information in the EU and the US.

[50]. For discussion of RCS under ECPA see: Pell, Stephanie K. (2012), Systematic government access to private-sector data in the United States, International Data Privacy Law, 2012, Vol. 2, No. 4.

[51] . Bigo Didier, Boulet Gertjan, Bowden Caspar, Carrera Sergio, Jeandesboz Julien, Scherrer Amandine (2012), Fighting cyber crime and protecting privacy in the cloud, Study for the European Parliament, PE 462.509.

[52]. Similar strong warnings were given by Hoboken, J.V.J., Arnbak, A.M., Van Eijk, N.A.N.M (2012), Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act, IVIR, Institute for Information Law, University of Amsterdam, November 2012 (English Translation). See also warnings of FAA incompatibility with ECHR in 2010: LoConte, Jessica (2010), FISA Amendments Act 2008: Protecting Americans by Monitoring International Communications--Is It Reasonable?, Pace International Law Review Online Companion 1-1-2010.

claims that this legalizes transfers of EU data into US clouds, and since 2009 several have altered their self-certification filings to claim the oxymoronic status of Safe-Harbour-as-a-Processor. The Article 29 Data Protection Working Party (WP29) have clarified that this is insufficient their recent opinion

- *Cloud providers are transnational companies subject to conflicts of international public law. Which law they choose to obey will be governed by the penalties applicable and exigencies of the situation, and in practice the predominant allegiances of the company management. So far, almost all the attention on such conflicts has been focussed on the US PATRIOT Act, but there has been virtually no discussion of the implications of the US Foreign Intelligence Surveillance Amendment Act of 2008. §1881a of FAA for the first time created a power of mass-surveillance specifically targeted at the data of non-US persons located outside the US, which applies to Cloud computing. Although all of the constituent definitions had been defined in earlier statutes, the conjunction of all of these elements was new.....the most significant change escaped any comment or public debate altogether. The scope of surveillance was extended beyond interception of communications, to include any data in public cloud computing as well. This change occurred merely by incorporating "remote computing services" into the definition of an "electronic communication service provider"*

- *...very strong implications on EU data sovereignty and the protection of its citizens' rights. The implications for EU Fundamental Rights flow from the definition of "foreign intelligence information", which includes information with respect to a foreign-based political organization or foreign territory that relates to the conduct of the foreign affairs of the United States. In other words, it is lawful in the US to conduct purely political surveillance on foreigners' data accessible in US Clouds. The root problem is that cloud computing breaks the forty year old legal model for international data transfers. The primary desideratum would be a comprehensive international treaty guaranteeing full reciprocity of rights, but otherwise exceptions ("derogations") can be recognized in particular circumstances providing there are safeguards appropriate to the specific situation. Cloud computing breaks the golden rule that "the exception must not become the rule". Once data is transferred into a Cloud, sovereignty is surrendered. In summary, it is hard to avoid the conclusion that the EU is not addressing properly an irrevocable loss of data sovereignty, and allowing errors made during the Safe Harbour negotiations of 2000 to be consolidated, not corrected.*

- *Particular attention should be given to US law that authorizes the surveillance of Cloud data of non-US residents. The EP should ask for further enquiries into the US FISA Amendments Act, the status of the 4th Amendment with respect to NONUSPERS, and the USA PATRIOT Act (especially s.215).*

- *The EP should consider amending the DP Regulation to require prominent warnings to individual data subjects (of vulnerability to political surveillance) before EU Cloud data is exported to US jurisdiction. No data subject should be left unaware if sensitive data about them is exposed to a 3rd country's surveillance apparatus. The existing derogations must be dis-applied for Cloud because of the systemic risk of loss of data sovereignty. The EU should open new negotiations with the US for recognition of a human right to privacy which grants Europeans equal protections in US courts.*

- *The EU needs an industrial policy for autonomous capacity in Cloud computing. The DG INFSO Communication of October 2012 is on this matter not in tune with the*

challenges analysed in this study. A target could be that by 2020, 50% of EU public services should be running on Cloud infrastructure solely under EU jurisdictional control.

The study also underlined that since the SWIFT affair, an EU "High-Level Contact Group" has been conducting talks in 2011 with the US authorities on an "Umbrella" agreement intended to cover transfers of data for law enforcement purposes. So far, the US has been adamant that these will not cover access to EU data from US private parties by US authorities, and thus would exclude precisely the situation of Cloud computing[53].

2.2.5 There are no privacy rights recognised by US authorities for non-US persons under FISA

The acquisition of *foreign intelligence information* under the PRISM programme requires adherence to "minimization"[54] and "targeting"[55] procedures, which were revealed (unredacted) by *The Guardian* on 20th June. Together these provide strong evidence that there are no privacy rights for non-Americans recognized by the US authorities under PRISM and related programmes. The revealed documents are heavily tautologous and replete with bureaucratic jargon, but a close reading does not discover any acknowledgement of rights for non-Americans whatsoever. One therefore suspects that **US operational practice places no limitations on exploiting or intruding a non-US person's privacy, if the broad definitions of *foreign intelligence information* are met.**

Moreover in a May 2012 letter to the Congress intelligence review committees[56] the government states that:

> *Because NSA has already made a "foreignness" determination for these selectors·in accordance with its FISC-approved targeting procedures, FBI's targeting role differs from that of NSA. FBI is not required to second-guess NSA's targeting determinations...*

The versions of the targeting procedures released are generic, but the American Civil Liberties Union (ACLU)[57] obtained redacted copies of slides related to FBI staff training that referred specifically to FISAAA for counter-terrorism purposes. The letter continues:

> *Once acquired, all communications are routed to NSA. NSA also can designate the communications from specified selectors acquired through PRISM collection to be "dual-routed" to other intelligence Community elements.* (emphasis added)

This means that agencies such as the CIA, amongst others of the sixteen agencies of the US intelligence community, can receive their own streams of data to store and analyse, which the NSA has roughly filtered for a 50% likelihood of "foreignness". No reporting on documents from Snowden, or other commentary, has referred to this "dual-routing" or their mission purposes.

According to the leaked "targeting procedures" (dated 2009) of FAA, an NSA database of telephone numbers and Internet identifiers[58] is used to eliminate known Americans from

[53]. EU-US Data Protection Non-Paper On Negotiations During 2011
[54]. http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document
[55]. http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document
[56].https://www.aclu.org/files/assets/ltr_to_hpsci_chairman_rogers_and_ranking_member_ruppersberger_scan.pdf (declassified 21st Aug 2013)
[57].ACLU FOIA request (2010), Introduction to FISA Section 702, (2010), US Dept. of Justice, decl.December 2010.

being inadvertently targeted by s.702. Analysts may only proceed to access "content data" under the 702 power if there is more than a 50% likelihood the target is not American and located outside the US, because the Fourth Amendment was held not to apply. Otherwise a particular warrant must be applied for under a different section of FISA.

This shows that the "probable cause" requirement for evidence of a 50% likelihood of *criminality* was converted into a 50% probability of *nationality*. This interpretation was first visible in a FISA Court of Review (FISCR) decision of 2008, released briefly in redacted form in 2010, and then apparently withdrawn from the official website (but a copy[59] had been kept by a transparency NGO).

The reasoning of FISCR was that **foreign intelligence surveillance of targets reasonably believed to be outside of the US qualifies for a "special needs" exception[60] to the Fourth Amendment warrant requirement.** The constitutionality of that judgement is being contested in a number of lawsuits brought by US civil liberties organisations, because this "coin-flip" criterion implies many unconstitutional searches of Americans' communications.

2.3. Data export: false solutions and insufficient safeguards

In order to conclude this section, the author would like to draw the Parliament's attention to certain difficulties with current derogations and/or safeguards proposed as solutions to the implications for EU Citizens underlined above. This subsection aims to highlight the loopholes and gaps in several mechanisms that have been put in place for data export. In the author's view, these mechanisms should not be seen as guarantees for the protection of EU citizens' rights.

2.3.1 Safe Harbour, BCRs for processors and Cloud Computing

The EU/US Safe Harbour Agreement of 2000 implemented a process for US companies to comply with the EU Directive 95/46/EC on the protection of personal data. If a US company makes a declaration of adherence to the Safe Harbour Principles then an EU Controller may export data to that company (although a written contract is still required).

Sometimes described as a 'simultaneous unilateral declaration', the Agreement left ambiguous whether it covered the situation of remote processing of data inside the US, on instruction from Controllers inside the EU. Especially in the case of Cloud computing, such remote processors were most unlikely to be capable of giving effect to the Safe Harbour Principles, which, the US argued, thus became void. Did the deal still apply, for unrestricted export of EU data for remote processing under essentially a self-regulatory framework? In 2000, the EU Commission over-ruled objections from civil society and some DPAs, to conclude a deal.

The US negotiators in the Department of Commerce worked closely with US trade lobbies, on a series of "FAQs" for US companies to interpret the Agreement to marginalize EU privacy rights, building in loopholes on such questions as what counted as identifiable data, refusing rights of access, and avoiding any duty of finality or right-of-deletion. Safe

---

[58]. This appears to be a different database, a directory, rather than the metadata controversially acquired under s.215. It is not known how this is compiled (for example from network surveillance) or under what authority, but evidently it is more than commercial telephone directories.

[59]. www.fas.org/irp/agency/doj/fisa/fiscr082208.pdf

[60]. Anzalda, Matthew A. and Gannon, Jonathan W. (2010), In re Directives...: Judicial Recognition of Certain Warrantless Foreign Intelligence Surveillance (paywall), Texas Law Review, Vol 88:1599 2010.

Harbour proved so Byzantine that no EU citizen navigated the bureaucracy to lodge a complaint for many years.

The official EU review study[61] on Safe Harbour of 2004, in a slight treatment of FISA, did not parse the political non-USPER meanings of *foreign intelligence information* discussed above, and stated that *"the controversial provisions of the USA PATRIOT Act are essentially irrelevant for Safe Harbour data flows"*.

Much of the legal analysis supporting the theory that Safe Harbour applies to Cloud computing can be traced to the work of Dr. Christopher Kuner[62], for many years the organizer of a Brussels lobby of privacy officers from predominantly US multinational companies, which became influential with the Commission and DPAs. Dr. Kuner also represented the International Chamber of Commerce in EU discussions over data protection, and has advised major Internet companies as clients. Kuner's textbook of Data Protection commercial law was cited in a Microsoft-sponsored study[63], arguing that Safe Harbour sufficed for Cloud processing. The US recently re-iterated this view expressly[64].

Against this background, a working group of DPAs began discussions about 2009 with major Internet companies on a new proposed derogation which could subsume Cloud computing. This became known as *Binding Corporate Rules for data processors*.

The concept was that a US (or other Third Country) Cloud service vendor could obtain a security accreditation for an entire software platform from a reputable auditor, and together with a "check-list" of organizational procedures drafted by WP29[65], an EU Controller could then lawfully export personal data outside the EU into the foreign-controlled Cloud. The checklist imposed (and in limited respects strengthened) similar conditions and wording to that which had already been created by the Commission for "model" clauses (see below).

Perhaps in response to warnings about FISA, two months before Snowden, WP29 issued an apparently minor "clarification", adding[66] that the checklist

> "***only*** *creates an information process that does not legitimate transfers per se. In the case of a conflict of laws,* ***one*** *shall refer to the international treaties and agreements applicable to such matter*" [emphasis added].

It does not seem very prudent to place the burden of responsibility for such a critical evaluation[67] of conflicts of international law on a foreign corporation with strong vested interests, that may be subject to espionage charges for compliance with EU law.

---

[61]. Dhont J., Asinari M.V.P., Poullet Y., Reidenberg J., Bygrave L. (2004), Safe Harbour Decision mplementation Study, European Commission, Internal Market DG Contract PRS/2003/A0-7002/E/27.

[62] . Kuner, Christopher (2008), Membership of the US Safe Harbor Program by Data Processors, The Center For Information Policy Leadership, Hunton & Williams LLP.

[63]. Hon, W. Kuan and Millard, Christopher (2012), Data Export in Cloud Computing - How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing, Part 4, QMUL Cloud Legal Project: "There is some uncertainty regarding whether the Safe Harbor framework applies to transfers to a US processor (as opposed to controller), such as a cloud provider. The better view is that it does...". See also Walden, Ian (2011), Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent, QMUL Cloud Legal Project, Research Paper No. 74/2011, footnote 119.

[64]. US Department of Commerce International Trade Administration (2013), Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing.

[65]. ART29WP - Article 29 Data Protection Working Party (2012), Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 195 Adopted on 6 June 2012.

[66]. ART29WP - Article 29 Data Protection Working Party (2013), Explanatory Document On The Processor Binding Corporate Rules, WP 204, Adopted On 19 April 2013.

[67]. For relevant discussion of such conflicts see: Radsan, John A. (2007), The Unresolved Equation of Espionage and International Law, Michigan Journal of International Law, Vol 28:595 2007.

BCRs-for-processors might sound like a variant of the existing BCRs (for Controllers), but in actuality they are vastly more risky for Europeans' privacy. The strategic risk to EU data sovereignty, which arises directly from the concept of BCRs-for-processors, is that the global Cloud industry is dominated by software "platforms" from Microsoft, Google, Amazon, and a few others. Microsoft's goal for its public-sector sales-force from 2010 was to compete for every contract for data processing by governments[68]. The cost savings for Cloud processing can be massive (sometimes one tenth the cost of processing "on-premise" by the Controller according to industry marketing claims). The cost savings are from equipment, overhead, operational staff (increasingly expensive for leading cyber-security expertise), and the major Cloud providers can take advantage of economies of scale, and higher average utilization by spreading processing loads across time-zones globally. Therefore there is already, and will be further, a competitive imperative to migrate European "on-premise" data to Cloud processing, and so far the EU has almost no significant indigenous software platforms that can compete (on cost, features, or reliability) with the leading US providers. The exception to this gloomy picture is free and open-source software, which has produced powerful Cloud "stacks" competitive with proprietary software and services.

In this light, BCR-for-processors can be seen as an expedient strategy both for the Commission and for Data Protection Authorities (DPAs) who wish to maintain the semblance of legal control over EU data, and for the Cloud providers who find the existing EU Data Protection regime generally inconvenient, especially for tax purposes[69]. The Commission promoted the legal status of the BCR-for-processors concept in the text of the new draft Regulation[70]. Subsequently, national DPAs have no alternative but to accept their validity once issued. So far, only a few dozen of the existing Controller BCRs have been approved[71], and the standard of compliance already is not reassuring[72].

2.3.2 Model Contracts

From 2001 the EU Commission drafted approved "model" clauses for inclusion in contracts both for Controllers and Processors located outside the EU, intended to guarantee privacy rights for individuals comparable to those they would have if the data remained inside the EU.

The conceptual flaw in this general approach is the supposition that computer systems can be "audited" to guarantee the three essential requirements of information security: Confidentiality, Integrity and Availability. Whilst integrity[73] and availability of data are technically and logically verifiable properties, confidentiality is not. It is impossible to know with certainty whether either an "insider" or external

---

[68]. The author was Chief Privacy Adviser to Microsoft's forty National Technology Officers (in charge of government liaison) until 2011, and received special sales training emphasizing the Cloud goal of competing for all government business, irrespective of the sensitivity of the data. On querying whether this was a mistake, the goal was reaffirmed.

[69]. Large US Internet companies tend to "forum-shop" for MS with low-tax and low-privacy regimes. If these do not coincide, corporate attorney must draft onerously complex contracts to comply with the technicalities of "model" contracts

[70]. BCRs (Art.43) are no longer categorized as a "derogation" (Art.44), see: European Commission (2012), Proposal for a General Data Protection Regulation, 25.1.2012, COM(2012) 11 final 2012/0011.

[71]. A rough sample of a dozen of these companies showed that most do not provide the actual BCR terms online as required.

[72]. The author filed a test complaint to the Luxembourg DPA about lack of any knowledge about BCRs by PayPal's privacy support staff (PayPal cannot comply with the terms of the BCR if their staff are unaware even of its existence or obligations). Despite several reminders, after one year there is still no news of the outcome of the investigation.

[73]. To check integrity, a "hash function" is computed over the data which functions as a verifiable "fingerprint".

unauthorised party has seen or copied data. Even if data is encrypted with a mathematically strong cipher, the algorithm implementation may have software defects, or the key may be leaked or stolen secretly.

The revelations about PRISM dramatically illustrate the folly of this legal stratagem. No force of law operating in civil cases on private parties can guarantee privacy rights in the face of an adversary such as the NSA trying to breach them, and operating lawfully in it own terms.

Clause.5(d)1[74] provided that the processor had to tell the EU exporter about any "legally binding request" for data ***unless*** that was prohibited, such as a prohibition under criminal law to preserve the confidentiality of a criminal investigation. The wording "such as" invites a reading that national security laws *a fortiori* overrides any contractual obligation. Although the EU retained powers to terminate the transfers, this required a basis of evidence to do so, and thus the structural temptation for turning a blind-eye was incorporated.

Every organizational actor has an incentive to turn a blind-eye under these arrangements. The Commission so they can maintain "high standards" of data protection are observed, DPAs so as not to expose their technical limits and exhaust their limited resources in expensive legal actions, Member States whose security hierarchies benefit from access to US counter-terror information, and business in EU and the US who simply want to transact without awkward questions of state mass-surveillance continually arising. Even EU civil society[75] seemed quiescent since ECHELON, and has mostly focussed on consumer rights[76] instead of meaningfully questioning the implications for Fundamental Rights and sovereignty in commercial data-flows to the US.

As a legal mechanism for guaranteeing rights and obtaining damages for poor security or privacy practices, such contracts (and their "model" clauses) have proved useless in so far as they have not given rise to litigation. In most situations where an EU Controller might want to obtain monetary damages from a Third Country processor/controller, the reputation damage they could suffer in the marketplace (e.g. from a data breach becoming known) would be very unlikely to be recouped. In theory, this disincentive would be removed by the new draft Regulations' requirement[77] to notify DPAs of data breaches, but DPAs have signalled that they will not necessarily require data subjects to be informed (and thus effectively make the incident public knowledge), partly in order to shield Controllers from disproportionate reputation damage. When disputes are settled out of court without publicity, it undercuts the function that contract litigation would perform, of informing Controllers about the reliability of those to whom they might export data. Data subjects of course have no idea when their rights may have been infringed under this approach.

---

[74]. Commission decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (2002/16/EC).
[75]. The notable exception is the Chaos Computer Club of Germany.
[76]. With promising exceptions such as the short-lived International Campaign Against Mass Surveillance of 2005 (website now defunct – but a copy preserved here), and the generally high level of civil society vigilance in Germany, which must be taken as read for avoidance of repetition
[77].The current breach notification requirement under the revised e-Privacy Directive only applies to telecommunications companies and Internet Services Providers, not to information society services provided through websites like social networks and search engines and general data Controllers.

3. STRATEGIC OPTIONS AND RECOMMENDATIONS FOR THE EUROPEAN PARLIAMENT

3.1. Reducing exposure and growing a European Cloud

As explained earlier, the mechanism of BCRs-for-processors, apparently tailor-made to ease the flow of EU data into Third Country cloud computing, is not sufficient to safeguard rights. It contains a loophole that condones unlawful surveillance. It is thus quite surprising that at various stages of development, the concept has been endorsed by the Article 29 Data Protection Working Party[78] (WP29), the European Data Protection Supervisor[79] (EDPS), and the French *Commission Nationale de l'Informatique et des Libertés* (CNIL) which led their formulation. No evidence has emerged that these DPAs understood the structural shift of data sovereignty[80] implied by Cloud computing. Rather, an unrealistic and legalistic view has allowed the protection of EU citizens to be neglected.

Recommendations:

- Prominent notices should be displayed by every US web site offering services in the EU to inform consent to collect data from EU citizens. The users should be made aware that the data may be subject to surveillance (under FISA 702) by the US government for any purpose which furthers US foreign policy. A consent requirement will raise EU citizen awareness and favour growth of services solely within EU jurisdiction. This will thus have economic impact on US business and increase pressure on the US government to reach a settlement.
- Since the other main mechanisms for data export (model contracts, Safe Harbour) are not protective against FISA or PATRIOT, they should be revoked and re-negotiated. In any case, the requirement above for informed consent after a prominent warning notice should apply to any data collected, in the past or in the future, by a public or private sector EU controller, before it can be exported to the US for Cloud processing.
- A full industrial policy for development of an autonomous European Cloud computing capacity based on free/open-source software should be supported. Such a policy would reduce US control over the high end of the Cloud e-commerce value chain and EU online advertising markets. Currently European data is exposed to commercial manipulation, foreign intelligence surveillance and industrial espionage. Investments in a European Cloud will bring economic benefits as well as providing the foundation for durable data sovereignty.

3.2. Reinstating 'Article 42'

The published[81] new Regulation omitted 'Art.42' (according to the numbering of a draft[82] leaked two months before the final version), reportedly after very heavy lobbying by US

---

[78] ART29WP - Article 29 Data Protection Working Party (2012), Opinion on Cloud Computing, WP 196, Adopted July 1st 2012

[79]. European Data Protection Supervisor - Hustinx, Peter (2010), Data Protection and Cloud Computing Under EU Law, speech, Third European Cyber Security Awareness Day, BSA, European Parliament, 13 April 2010, Panel IV: Privacy and Cloud Computing.

[80]. De Filippi, Primavera, and McCarthy, Smari (2012), Cloud Computing: Centralization and Data Sovereignty, European Journal of Law and Technology 3, 2.

[81]. European Commission (2012), Proposal for a General Data Protection Regulation, 25.1.2012, COM(2012) 11 final 2012/0011.

[82]. European Commission (2011), [Draft] Proposal for a General Data Protection Regulation

interests[83]. Article 42 prohibits Third Countries (such as the United States and other non-EU Member States) from accessing personal data in the EU where required by a non-EU court or administrative authority without prior authorization by an EU Data Protection Authority. The article has been described as the "anti-FISA clause".

Recommendations: The deterrent effect of 'Art.42' should be assessed before it is reinstated, and in particular, the following issues should be addressed:

- Even though Art.42 in principle mitigates controversial aspects of FISA, it is doubtful that this measure would be effective, because compliance would expose the leadership of US companies to charges of espionage. As the Yahoo CEO declared recently: "*we faced jail if we revealed NSA surveillance secrets*"[84].
- The efficiency of sanctions as a compliance mechanism should also be evaluated from the perspective of net economic gains and losses. As an illustration, the EU competition authority prosecuted a long case against Microsoft for its monopoly of local-area networking, resulting in a fine of $1bn (the largest ever applied by the EU). The corporate attorney responsible for that strategy was not fired for incompetence but promoted to a Deputy General Counsel. The reason is that Microsoft's profits over the previous decade from the monopoly were conservatively twenty times the size of the enormous fine, and this was foreseen by Microsoft's legal strategists.
- If a major Cloud provider failed to comply with Art.42, it could result in irreversible but secret violation of the fundamental rights of millions of citizens, and the Regulation ought to make this a serious criminal offence. At the moment, most MS transpositions of EU 95/46 treat DP offences as minor matters, and some MS do not implement criminal sanctions at all. That is no deterrent against a calculated strategy to ignore EU law, weighed against the penalties applicable under US law.
- At a general level and beyond the specific scope of Art.42, the level of fines for infractions of the new Data Protection Regulation also need to be substantially increased. They were reduced to a 2% fine on the revenue of a corporation, from higher levels in leaked drafts. The example above of the Microsoft competition case shows that some companies have enormous resources and deep strategies that anticipate and incorporate even billion-dollar fines into their business plans. A fine level of 20% of global revenue may be needed to persuade such corporations to reckon seriously with Art.42 compliance.
- Even after BULLRUN, cryptography is probably intact in theory[85], however it is not known which encryption implementations and products may have been rendered insecure. **Therefore consideration should be given to extending the scope of 'Art.42' also to cover vendors of systems/products (as well as Controllers/Processors) in EU markets.** Existing encryption security product accreditations, especially if influenced by NSA or GCHQ, must be regarded as suspect.

[83]. Washington pushed EU to dilute data protection, *Financial Times* 12th June 2013,
[84]. The Guardian 12th September 2013, http://www.theguardian.com/technology/2013/sep/11/yahoo-ceo-mayer-jail-nsa-surveillance?CMP=twt_gu
[85] Otherwise the NSA would not expend so many resource to by-pass it by indirect means (unless that is a deception plan on an immense scale)

3.3. Whistle-Blowers' Protection and Incentives

Recommendation: Systematic protection and incentives for whistle-blowers should be introduced in the new Regulation. Whistle-blowers should be given strong guarantees of immunity and asylum, and awarded 25% of any fine consequently exacted[86]. The whistle-blower may have to live in fear of retribution from their country for the rest of the lives, and take precautions to avoid "rendition" (kidnapping). Ironically, US law already provides rewards of the order of $100m for whistle-blowers exposing corruption (in the sphere of public procurement and price-fixing)[87].

3.4. Institutional Reform

At a very early stage of consultation the EU Commission rejected the option of establishing a new central pan-European Data Protection Authority, because this appeared disproportionate to the requirement for Member States' subsidiarity. The option was chosen for an evolutionary development of WP29 into the new Data Protection Board. However an intermediate option could have been considered: the creation of a new central authority for cases involving major Third Country data-flows.

Recommendation: a central investigative service for cases involving major Third Country data-flows should be created. This service should be given authority and resources to initiate complex prosecutions against transnational companies, who often employ large legal teams to delay and appeal decisions over many years. National DPAs would retain jurisdiction over purely national affairs, and according to the principle of subsidiarity, could initiate their own national investigations, or refer a case to the central service.

3.5. Data Protection Authorities and Governance

The PRISM scandal and Snowden's revelations have not been the first warnings to EU Institutions in relation to EU citizens' rights. Privacy activists for instance warned the Commission in 2000 that the Safe Harbour Agreement contained dangerous loopholes[88]. More recently, the above-mentioned note produced on Cloud Computing for the European Parliament's LIBE Committee clearly highlighted the loopholes of FISA and their consequences on EU citizens' rights and protection[89].

The Committee even held a hearing[90] for the presentation of the Note, following a session on the EU Cybersecurity strategy on Feb 20th 2013. Afterwards MEPs asked for immediate proposals to meet the LIBE amendment deadline[91] on the Data Protection Regulation. However, from March onwards, the level of interest in the Note declined, and there seemed only a remote possibility that Parliament would support fundamental revisions of the DP regulation. Thanks to the PRISM scandal and Snowden's revelations, such warnings and related concerns have gained a new legitimacy. The question remains why DPAs did not react.

In one hundred and fifty Opinions of WP29 issued since 9/11, only the first mentions the PATRIOT Act (in a footnote), and none FISA, or even the term 'foreign intelligence'.

---

86. This principle has a long history in law under the term Qui Tam.
87. http://www.theguardian.com/business/2010/oct/27/glaxosmithkline-whistleblower-wins-61m
88. The author (then as Director of FIPR) and others raised the question of whether Safe Harbour permitted "ECHELON"-type mass-surveillance with officials but received no answer.
89. Bigo Didier, Boulet Gertjan, Bowden Caspar, Carrera Sergio, Jeandesboz Julien, Scherrer Amandine (2012), Fighting cyber crime and protecting privacy in the cloud, Study for the European Parliament, PE 462.509.
90. 20.2.13 European Parliament LIBE hearing on Cybercrime/Cloud Report (video from 17:08:18)
91. LIBE amendments 806/2531/2748/2950 of the new Regulation are derived from these proposals

National DPAs[92], the EDPS[93], and other institutions[94] seemed to be unaware of US legislation or that PRISM was legally possible. They failed to sound the alarm for EU citizens, despite warnings[95], and of course the widely reported US scandal before 2008. This may be because DPAs, ENISA[96], and the Trust and Security Unit of DG-CONNECT[97], are ambivalent whether the "national security" exemption of EU competency means they are – or are not - required to defend their citizens' privacy from Third Country intelligence agencies.

In their last state-of-play comments before Snowden, the EDPS noted the above mentioned LIBE proposed amendment for a drastic warning to data subjects before giving consent to Cloud transfers, but rejected[98] this on the grounds that it was not "technology neutral".

It appears the EU DPA institutions have some structural difficulties that need to be addressed. In particular, DPAs clearly lack capacities in technical expertise. Only a few dozen DPA staff (out of about two thousand across Europe) has an informatics background, let alone a post-graduate degree related to the computer and engineering science of privacy. There is a deeply-rooted view that because in general it is preferable to draft laws in a technology-neutral[99] way, this excuses regulators from understanding technical matters. For example, WP29 has never conducted any survey of advanced privacy-enhancing technologies, or issued any Opinion mandating their use, even in the face of persistent evidence of market failure for their voluntary adoption.

Recommendations: A reform of the EU Data Protection Authorities appointment system should be implemented. The new Regulation does not address this aspect. This is critical in order to prevent inertia and deadlock regarding technology-specific questions. Some options to improve the EU Data Protection governance and capacities could include:

- inclusion in the Data Protection Board of at least one special Commissioner with a mandate prioritizing defence of citizens' rights, with a small independent staff, perhaps directly elected by popular (but apolitical) vote at the time of European elections, or by the Parliament;
- inclusion of a special technical Commissioner, nominated from the functional constituency of academic computer scientists specializing in privacy, and potentially another Commissioner from the field of Surveillance Studies, also with small independent staffs;
- a requirement that DP Commissioners must be appointed by national Parliaments

[92]. With the exception of German DPAs have who been vigilant. See: Weichert, Thilo (2011), Cloud Computing and Data Privacy, The Sedona Group Conference Working Group Series, February 2011. See also: International Working Group on Data Protection in Telecommunications (2012), Working Paper on Cloud Computing - Privacy and data protection issues - Sopot Memorandum, 51st meeting, 23-24 April 2012.
[93]. Bowden, Caspar (2012), Is EU data safe in US Clouds? (slides), Academy of European Law, Trier September 2012. Both the EDPS and Deputy were present, as well as senior officials from the Council, Commission and other DPAs, who were emailed a copy afterwards.
[94]. See: 28.6.12 - Green party hearing on DP (slides) (video t=2h43m); See also:10.10.12 LIBE Interparliamentary Forum
[95]. Bowden, Caspar (2011), Government Databases and Cloud Computing (slides), The Public Voice, Mexico, October 2011.
[96]. On 14.6.13 ENISA Press Office replied to a question from the author to the Director, that defence against the NSA was outside their mandate, but probably realizing this position is untenable, on 6.9.13 issued a statement finessing the issue and incorrectly implying (footnote 21) that ENISA had warned of FISA-type risks in 2009.
[97]. Statement made by responsible DG-CONNECT official at Cloud security workshop 28.5.13 convened to discuss author's warnings just before Snowden.
[98]. European Data Protection Supervisor (2013), Additional EDPS Comments on the Data Protection Reform Package.
[99]. European Data Protection Supervisor (2011), Opinion on the Communication - "A comprehensive approach on personal data protection in the European Union", Brussels, 14 January 2011.

and not the executive;

- a minimum quota for DPAs of 25% technical staff with suitable qualifications (or equivalent experience) with a career path[100] to the most senior positions;
- a subvention of funds to support the civil society sector, although great care must be taken to ring-fence this allocation. Funds should be distributed fairly and on merit, but avoiding the stifling effect of bureaucracy and the danger of institutional capture[101]. In the United States, the culture of philanthropy and mass-membership civil society supports four highly professional national NGOs[102], with diverse approaches, which litigate test cases in privacy and freedom of information, and conduct world-class technical critique of government policies. In contrast, the EU still has a patchwork of dozens of NGOs, who with few resources and lacking the consistent capacity of a permanent research staff, did not campaign on FISA before Snowden

CONCLUSION

As noted earlier, one of the most extraordinary aspects of the PRISM affair is that not only have the rights of non-Americans not been discussed in the US, they were not even discussed by the European media until well after the story first broke. The rights of non-Americans were rarely raised, and a casual reader would not understand that the intended target of surveillance was non-Americans, and that they had no rights at all.

It seems that the only solution which can be trusted to resolve the PRISM affair must involve changes to the law of the US, and this should be the strategic objective of the EU. **Furthermore, the EU must examine with great care[103] the precise type of treaty instrument proposed in any future settlement with the US**. Practical[104] but effective mechanisms are also needed to verify that disclosures of data to the US for justifiable law enforcement investigations are not abused.

In assessing the impact of the revelations, three technical considerations should be borne in mind in the search for effective responses.

(1) Data can only be processed whilst decrypted, and thus any Cloud processor can be secretly ordered under FISA 702 to hand over a key, or the information itself in its decrypted state. Encryption is futile to defend against NSA accessing data processed by US Clouds (but still useful against external adversaries such as criminal hackers). Using the Cloud as a remote disk-drive does not provide the competitiveness and scalability benefits of Cloud as a computation engine. **There is no technical solution to the problem[105].**

(2) Exposing data in bulk to remote Cloud mass-surveillance forfeits data sovereignty, so confining data to the EU is preferable pending legal solutions. Although NSA has extensive

---

[100]. DPAs object they are unable to hire or retain technical staff with current knowledge because their salaries cannot compete with the private sector. DPA career tracks could ensure a reasonable parity of remuneration between technical and legal staff, which would ameliorate this problem.

[101].for example the EU's "No Disconnect" strategy, obliges NGOs use consultants to prepare micro-managed formal bids, which effectively excludes small NGOs and is alienating to the spirit of civil society.

[102]. The Electronic Frontier Foundation (EFF), The Electronic Privacy Information Center (EPIC), the American Civil Liberties Union (ACLU), and the Center for Democracy and Technology (CDT).

[103]. Regarding "inherent" Presidential powers without Congressional authority, see: Fein, Bruce (2007), Presidential Authority to Gather Foreign Intelligence, Presidential Studies Quarterly, March 2007.

[104]. Wills Aidan and al., Parliamentary Oversight of security and Intelligence Agencies in the EU, Note for the European Parliament, PE 453.207

[105]. The exotic technique of "homomorphic encryption" is sometimes proposed as solution but has no commercial relevance since its systematic adoption would be uncompetitive, as it would slow down processing by many orders of magnitude

capabilities to target particular systems inside the EU, this is harder and riskier to do. However basic reforms to the new Regulation are needed, otherwise *in practice* these two situations will be treated as equivalent, and Cloud business will go to lowest bidder.

(3) Although an EU-based company transacting in the US is also subject to conflicts between EU DP and the FISA law, in practice it is less likely they will be served with such secret orders, because the legal staff and management would be more likely to resist, and as EU-nationals are less threatened by US espionage laws. "Clouds" can be confined to a location, and arguments this would "balkanise[106] the Internet confuses issues of censorship with the problem of keeping data private.

* * *

The thoughts prompted in the mind of the public by the revelations of Edward Snowden cannot be unthought. We are already living in a different society in consequence. Everybody now knows, that the US intelligence community might know any personal secret in electronic data sent in range of the NSA. These developments could be profoundly destabilising for democratic societies, precluding exercise of basic political and human rights, and creating a new form of instantaneous and coercive Panoptic power.

There is a historical symmetry between the incursions on the Fourth Amendment rights of Americans, and the disregard for the human right to privacy of everyone else in the world. In the period leading up the US War of Independence the British used "general warrants" which authorised any search without suspicion, and it was resentment[107] against this power and its abuse that motivated the subsequent Fourth Amendment to the US Constitution.

FISA 702 (aka *§1881a*) is a general warrant to collect data and trawl for information related to US foreign affairs, but Americans' privacy is legallly sacrosanct (albeit in theory) unless the high legal threshold of "necessity" is met. What particularly galled the American revolutionaries was that ten years earlier a famous case in English law[108] had prohibited such general warrants. They regarded it as hypocrisy that laws they did not write, and could not change, protected the privacy of their rulers, but not colonial subjects. The same principle is at stake today.

[106]. U.S. Commerce Department (General Counsel) – Kerry, Cameron F. (2013), Keynote Address at the German Marshall Fund of the United States, 28th August 2013
[107].https://www.eff.org/files/filenode/att/generalwarrantsmemo.pdf
[108].Entick vs. Carrington 1765

REFERENCES

- ACLU FOIA request (2010), Introduction to FISA Section 702, (2010) Course Information, US Department of Justice, published December 2010
- Anzalda, Matthew A. and Gannon, Jonathan W. (2010), In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act: Judicial Recognition of Certain Warrantless Foreign Intelligence Surveillance (paywall), Texas Law Review, Vol 88:1599 2010
- ART29WP - Article 29 Data Protection Working Party (2012), Opinion on Cloud Computing, WP 196, Adopted July 1st 2012
- ART29WP - Article 29 Data Protection Working Party (2012), Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 195 Adopted on 6 June 2012
- ART29WP - Article 29 Data Protection Working Party (2013), Explanatory Document On The Processor Binding Corporate Rules, WP 204, Adopted On 19 April 2013
- Bigo Didier, Boulet Gertjan, Bowden Caspar, Carrera Sergio, Jeandesboz Julien, Scherrer Amandine (2012), Fighting cyber crime and protecting privacy in the cloud, Study for the European Parliament, PE 462.509
- Bloom, Stephanie Cooper (2009), What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform, Public Interest Law Journal Vol 18:269
- Bowden, Caspar (2011), Government Databases and Cloud Computing (slides), The Public Voice, Mexico, October 2011
- Bowden, Caspar (2012), Is EU data safe in US Clouds? (slides), Academy of European Law, Trier September 2012
- Cloud, Morgan (2005), A Liberal House Divided: How the Warren Court Dismantled the Fourth Amendment, Ohio State Journal of Criminal Law, Vol 3:33 2005
- Cole, David, (2003), Georgetown Law: The Scholarly Commons, Are Foreign Nationals Entitled to the Same Constitutional Rights As Citizens? 25 T. Jefferson L. Rev. 367-388
- Congressional Research Service - Bazan, Elizabeth B. (2008), The Foreign Intelligence Surveillance Act: An Overview of Selected Issues, Updated July 7, 2008, RL34279
- Congressional Research Service – Liu, Edward C. (2013), Reauthorizattion of the FISA Amendments Act, 7-5700, R42725, January 2, 2013
- Congressional Research Service (2007), P.L. 110-55, the Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act, August 23, 2007
- Corradino, Elizabeth A. (1989), Fordham Law Review, The Fourth Amendment Overseas: Is Extraterritorial Protection of Foreign Nationals Going Too Far? Volume 57, Issue 4, Article 4, January, 1989
- De Filippi, Primavera, and McCarthy, Smari (2012), Cloud Computing: Centralization and Data Sovereignty, European Journal of Law and Technology 3, 2
- Desai, Anuj C. (2007), Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy, Stanford Law Review, 60 STAN L. REV. 553
- Dhont J., Asinari M.V.P., Poullet Y., Reidenberg J., Bygrave L. (2004), Safe Harbour Decision Implementation Study, European Commission, Internal Market DG Contract PRS/2003/A0-7002/E/27
- Dulles, Allen Welsh (1963), The Craft of Intelligence, New York: Harper&Row.
- European Commission (2011), [Draft] Proposal for a General Data Protection Regulation
- European Commission (2012), Proposal for a General Data Protection Regulation, 25.1.2012, COM(2012) 11 final 2012/0011
- European Commissioner - Reding, Viviane (2013), Letter to the Attorney General, Ref. Ares (2013)1935546 - 10/06/2013, Brussels, 10 June 2013
- European Data Protection Supervisor - Hustinx, Peter (2010), Data Protection and Cloud Computing Under EU Law, speech, Third European Cyber Security Awareness Day, BSA, European Parliament, 13 April 2010, Panel IV: Privacy and Cloud Computing
- European Data Protection Supervisor (2011), Opinion on the Communication - "A comprehensive approach on personal data protection in the European Union", Brussels, 14 January 2011
- European Data Protection Supervisor (2013), Additional EDPS Comments on the Data Protection Reform Package
- Fein, Bruce (2007), Presidential Authority to Gather Foreign Intelligence, Presidential Studies Quarterly,

March 2007

- Forgang, Jonathan D. (2009), "The Right of the People": The NSA, the FISA Amendments Act of 2008, and Foreign Intelligence Surveillance of Americans Overseas, Fordham Law Review, Volume 78, Issue 1, Article 6, 2009
- Hoboken, J.V.J., Arnbak, A.M., Van Eijk, N.A.N.M (2012), Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act, IVIR, Institute for Information Law, University of Amsterdam, November 2012 (English Translation)
- Hon, W. Kuan and Millard, Christopher (2012), Data Export in Cloud Computing - How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing, Part 4, QMUL Cloud Legal Project, 4 April 2012
- Hondius, Frits W (1975), Emerging data protection in Europe. North-Holland Pub. Co.
- International Working Group on Data Protection in Telecommunications (2012), Working Paper on Cloud Computing - Privacy and data protection issues - Sopot Memorandum, 51st meeting, 23-24 April 2012
- Kuner, Christopher, (2008), Membership of the US Safe Harbor Program by Data Processors, The Center For Information Policy Leadership, Hunton & Williams LLP
- LoConte, Jessica (2010), FISA Amendments Act 2008: Protecting Americans by Monitoring International Communications--Is It Reasonable?, Pace International Law Review Online Companion 1-1-2010
- Medina, M. Isabel, (2008) Indiana Law Journal, Exploring the Use of the Word "Citizen" in Writings on the Fourth Amendment Volume 83, Issue 4, Article 14, January, 2008
- Pell, Stephanie K. (2012), Systematic government access to private-sector data in the United States, International Data Privacy Law, 2012, Vol. 2, No. 4
- Radsan, John A. (2007), The Unresolved Equation of Espionage and International Law, Michigan Journal of International Law, Vol 28:595 2007
- Snider, Britt L. (1999): Unlucky SHAMROCK - Recollections from the Church Committee's Investigation of NSA
- U.S. Ambassador to the EU (2012), Remarks by William E Kennard, Forum Europe's 3rd Annual European Data Protection and Privacy Conference, December 4, 2012
- U.S. Commerce Department (General Counsel) – Kerry, Cameron F. (2013), Keynote Address at the German Marshall Fund of the United States, 28th August 2013
- US Congress (2008), Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, 122 Stat. 2436, Public Law 110-261, July 10, 2008
- US Department of Commerce International Trade Administration (2013), Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing, December 4, 2012
- US State Department (2012), Five Myths Regarding Privacy and Law Enforcement Access to Personal Information in the EU and the US
- Vandekerchkhove, Wim (2010), European whistleblower protection: tiers or tears?, in D. Lewis (ed) A Global Approach to Public Interest Disclosure, Cheltenham/Northampton MA, Edward Elgar, pp 15-35.
- Walden, Ian (2011), Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent, QMUL Cloud Legal Project, Research Paper No. 74/2011
- Weichert, Thilo (2011), Cloud Computing and Data Privacy, The Sedona Group Conference Working Group Series, February 2011
- Wills Aidan, Vermeulen Mathias, Born Hans, Scheinin Martin, Wiebusch Micha, Thornton Ashley, Parliamentary Oversight of security and Intelligence Agencies in the EU, Note for the European Parliament, PE 453.207.
- Young, Stewart M, (2003) Michigan Telecommunications and Technology Law Review, Verdugo in Cyberspace: Boundaries of Fourth Amendment Rights for Foreign Nationals in Cybercrime Cases, Volume 10, Rev. 139