CEPS Paper in
LIBERTY and SECURITY in Europe

Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law

Didier Bigo, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Ragazzi and Amandine Scherrer

No. 61 / November 2013

Abstract

In the wake of the disclosures surrounding PRISM and other US surveillance programmes, this paper assesses the large-scale surveillance practices by a selection of EU member states: the UK, Sweden, France, Germany and the Netherlands. Given the large-scale nature of these practices, which represent a reconfiguration of traditional intelligence gathering, the paper contends that an analysis of European surveillance programmes cannot be reduced to a question of the balance between data protection versus national security, but has to be framed in terms of collective freedoms and democracy. It finds that four of the five EU member states selected for in-depth examination are engaging in some form of large-scale interception and surveillance of communication data, and identifies parallels and discrepancies between these programmes and the NSA-run operations. The paper argues that these programmes do not stand outside the realm of EU intervention but can be analysed from an EU law perspective via i) an understanding of national security in a democratic rule of law framework where fundamental human rights and judicial oversight constitute key norms; ii) the risks posed to the internal security of the Union as a whole as well as the privacy of EU citizens as data owners and iii) the potential spillover into the activities and responsibilities of EU agencies. The paper then presents a set of policy recommendations to the European Parliament.

This study was commissioned as a Briefing Paper by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs. The original document entitled "National Programmes of Mass Surveillance of Personal Data in the EU Member States and their Compatibility with EU Law", can be downloaded from the European Parliament's website (www.europarl.europa.eu/studies). It is republished by the Centre for European Policy Studies with the kind permission of the European Parliament.

ISBN 978-94-6138-364-8

Available for free downloading from the CEPS website (http://www.ceps.eu)

Contents

Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law

Didier Bigo, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Ragazzi and Amandine Scherrer

CEPS Paper in Liberty and Security in Europe No. 61 / November 2013

Executive Summary

Surveillance of population groups is not a new phenomenon in liberal regimes and the series of scandals surrounding the surveillance programmes of the National Security Agency (NSA) in the US and the UK's Government Communications Headquarters (GHCQ) only reminds us of the recurrence of transgressions and illegal practices carried out by intelligence services. However, the scale of surveillance revealed by Edward Snowden should not be simply understood as a routine practice of intelligence services. Several aspects emerged from this series of revelations that directly affect EU citizens' rights and EU institutions' credibility in safeguarding those rights.

First, these revelations uncover **a reconfiguration of surveillance that enables access to a much larger scale of data** than telecommunications surveillance of the past. Progress in technologies allows a much larger scope for surveillance, and platforms for data extraction have multiplied.

Second, the distinction between targeted surveillance for criminal investigation purposes, which can be legitimate if framed according to the rule of law, and large-scale surveillance with unclear objectives is increasingly blurred. **It is the purpose and the scale of surveillance that are precisely at the core of what differentiates democratic regimes from police states**.

Third, the intelligence services have not yet provided acceptable answers to the recent accusations directed at them. This raises the **issue of accountability of intelligence services and their private-sector partners** and reinforces the need for a strengthened oversight.

In light of these elements, the briefing paper starts by suggesting that an **analysis of European surveillance programmes cannot be reduced to the question of a balance between data protection versus national security**, but has to be framed in terms of collective freedoms and democracy (section 1). This section underlines the fact that it is the scale of surveillance that lies at the heart of the current controversy.

The second section of this paper outlines the main characteristics of large-scale telecommunications surveillance activities/capacities of five EU member states: the UK, Sweden, France, Germany and the Netherlands (section 2). This section reveals in particular the following:

- Practices of so-called 'upstreaming' (tapping directly into the communications infrastructure as a means to intercept data) characterise the surveillance programmes all the selected EU member states, with the exception of the Netherlands for which there is, to date, no concrete evidence of engagement in large-scale surveillance.
- The capacities of Sweden, France and Germany (in terms of budget and human resources) are low compared to the magnitude of the operations launched by GCHQ and the NSA and cannot be considered on the same scale.
- There is a multiplicity of intelligence/security actors involved in processing and exploiting data, including several, overlapping transnational intelligence networks dominated by the US.
- Legal regulation of communications surveillance differs across the member states examined, but in general legal frameworks are characterised by ambiguity or loopholes as regards large-scale communications surveillance, while national oversight bodies lack the capacity to effectively monitor the lawfulness of intelligence services' large-scale interception of data.

This empirical analysis furthermore underlines the two key issues that remain unclear given the lack of information and the secretive attitude of the services involved in these surveillance programmes: i) what/who are the ultimate targets of this surveillance exercise, and ii) how are data collected, processed, filtered and analysed?

The paper then presents modalities of action at the disposal of EU institutions to counter unlawful large-scale surveillance (section 3). This section underlines that even if intelligence activities are said to remain within the scope of member states' exclusive competences in the EU legal system, this does not necessarily means that member states' surveillance programmes are entirely outside the remits of the EU's intervention. Both the European Convention on Human Rights and the EU Charter of Fundamental Rights could play a significant role here, especially given the fact that, from a legal point of view, EU surveillance programmes are incompatible with minimum democratic rule-of-law standards and compromise the security and fundamental human rights of citizens and residents in the EU. The forthcoming revision of Europol's legal mandate appears to be a timely occasion to address the issue of EU competence and liability in sharing and exploiting data generated by national large-scale surveillance operations and to ensure greater accountability and oversight of this agency's actions.

The paper concludes that a lack of action at the EU level would profoundly undermine the trust and confidence that EU citizens have in the European institutions. A set of recommendations is outlined, suggesting potential steps to be taken by the EU and directed in particular at the European Parliament.

Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law

Didier Bigo, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Ragazzi and Amandine Scherrer*

CEPS Paper in Liberty and Security in Europe No. 61 / November 2013

Introduction

Scope of the problem

Following the revelations of Edward Snowden, a former contractor working for the US National Security Agency (NSA), published in The Guardian and the Washington Post on 6 June 2013, concerning the activities of the NSA and the European services working with them, it appears that:

- First, the US authorities are accessing and processing personal data of EU citizens on a large scale via, among others, the NSA's warrantless wiretapping of cable-bound internet traffic (UPSTREAM)[1] and direct access to the personal data stored in the servers of US-based private companies such as Microsoft, Yahoo, Google, Apple, Facebook and Skype[2] (PRISM). This allows the US authorities to access both stored communications as well as to perform real-time collection on targeted users, through cross-database search programmes such as X-KEYSCORE.[3] UPSTREAM, PRISM and X-KEYSCORE are only three of the most publicised programmes and represent the tip of the iceberg of the NSA's surveillance.[4]
- Second, the UK intelligence agency, the Government Communications Headquarters (GCHQ), has cooperated with the NSA and has initiated actions of interception under a programme code-named TEMPORA. Further reports have emerged implicating a handful of other EU member states (namely Sweden, France and Germany) that may be running or developing their own large-scale internet interception programmes (potentially the Netherlands), and collaborating with the NSA in the exchange of data.

---

* Didier Bigo is Director of the Centre d'Etudes sur les Conflits, Liberté et Sécurité (CCLS) and Professor at Sciences-Po Paris and King's College London. Sergio Carrera is Senior Research Fellow and Head of the Justice and Home Affairs Section, Centre for European Policy Studies. Nicholas Hernanz is Research Assistant, Justice and Home Affairs Section, CEPS. Julien Jeandesboz is Assistant Professor at the University of Amsterdam and Associate Researcher at CCLS. Joanna Parkin is a Researcher, Justice and Home Affairs Section, CEPS. Francesco Ragazzi is Assistant Professor in International Relations, Leiden University. Amandine Scherrer is European Studies Coordinator and Associate Researcher at CCLS.

The authors would like to thank the following experts who have contributed to the research of this paper: Axel Arnbak, cybersecurity and information law researcher at the Institute for Information Law, University of Amsterdam; Jelle van Buuren, Leiden University, Center for Terrorism and Counter-terrorism; Ot van Daalen, Bits of Freedom; and Mark Klamberg, Senior Lecturer at the Department of Law of Uppsala University.

This paper supplements the previous research of Caspar Bowden by looking at the connection between the European programmes and the US surveillance programme. See Caspar Bowden, "The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights", Study for the European Parliament, PE 474.405, September 2013.

[1] The UPSTREAM programme was revealed as early as 2006, when it was discovered that the NSA was tapping cable-bound internet traffic in the very building of the SBC Communications in San Francisco. See "AT&T Whistle-Blower's Evidence", *Wired*, 17 May 2006 (http://bit.ly/17oUqIG).

[2] Through the NSA's programme Planning Tool for Resource Integration, Synchronisation, and Management (PRISM).

[3] *The Guardian*, 7 June 2013 and 8 June 2013.

[4] Other high-profile NSA electronic surveillance programmes include: Boundless Informant, BULLRUN, Fairview, Main Core, NSA Call Database and STELLARWIND.

- Third, EU institutions and EU member state embassies and representations have been subjected to US-UK surveillance and spying activities. The European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) recently received testimony on how the UK GCHQ infiltrated the systems of Belgacom in what was codenamed 'Operation Socialist' to gain access to the data of the European institutions.[5] A letter from Sir Jon Cunliffe, the UK Ambassador to the EU, stated that the GCHQ chief would not appear (at the hearing) since "the activities of intelligence services are… the sole responsibility of EU member states".[6]

The questions opened by these NSA activities and the European services working with them directly affect the EU institutions and necessitate a specific inquiry by the European Parliament, given that these matters clearly affect EU affairs and interact with EU competence.

Beyond the specific case of the attacks against the EU institutions, these secret operations impact, first, the daily life of all the individuals living inside the European Union (citizens and permanent residents) when they use internet services (such as email, web browsing, cloud computing, social networks or Skype communications – via personal computers or mobile devices), by transforming them into potential suspects. Second, these operations may also influence the fairness of the competition between European companies and US companies, as they have been carried out in secret and imply economic intelligence; third, some governments of the EU were kept unaware of these activities while their citizens were subject to these operations. An inquiry is therefore central and needs to be supported by further in-depth studies, in particular in the context of EU developments in the area of rule of law.

In addition to the fact that these operations have been kept secret from the public, from companies and branches of governments affected by them (with the possible exception of the intelligence communities of some European countries), the second salient characteristic of these operations is their 'large-scale' dimension, which changes their very nature, as they go largely beyond what was previously called 'targeted surveillance' or a non-centralised and heterogeneous assemblage of forms of surveillance.[7] These operations now seem to plug in intelligence capacities on these different forms of surveillance via different platforms and may lead to data-mining and mass surveillance. The different interpretations of what constitutes large-scale surveillance are discussed in details below.

A large part of the world's electronic communications transiting through cables or satellites, including increasingly information stored or processed within cloud computing services (such as Google Drive or Dropbox for consumers; Salesforce, Amazon, Microsoft or Oracle for businesses) i.e. petabytes of data and metadata, may become the object of interception via technologies put in place by a transnational network of intelligence agencies specialised in data collection and led by the NSA. The NSA carries out surveillance through various programmes and strategic partnerships.[8] While the largest percentage of the internet traffic is believed to be collected directly at the root of the communications infrastructure, by tapping into the backbone of the telecommunications networks distributed around the world, the recent exposure of the PRISM programme has revealed that the remaining traffic is tapped through secret data collection and data extraction of nine US-based companies: Microsoft, Google, Yahoo, Facebook, Paltalk, Youtube, Skype, AOL and Apple.[9] The surveillance programmes therefore imply not only governments and a network of

---

[5] In a post published on 20 September 2013, Spiegel journalists who had access to Snowden documents stated: "According to the slides in the GCHQ presentation, the attack was directed at several Belgacom employees and involved the planting of a highly developed attack technology referred to as a 'Quantum Insert' (QI). It appears to be a method with which the person being targeted, without their knowledge, is redirected to websites that then plant malware on their computers that can then manipulate them." (See www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html).

[6] Letter from John Cunliffe to MEP Juan Lopez Aguilar (www.europarl.europa.eu/document/activities/cont/201310/20131003ATT72276/20131003ATT72276EN.pdf).

[7] K. Haggerty and R. Ericson, (2000), "The Surveillant Assemblage", *British Journal of Sociology*, 51(4): pp. 605-622. See also D. Bigo (2006), "Intelligence Services, Police and Democratic Control: The European and Transatlantic Collaboration", in D. Bigo and A. Tsoukala (eds), *Controlling Security*, Paris: L'harmattan.

[8] The NSA functions in particular as the centre of the network codenamed 'Five Eyes' (US, UK, Canada, Australia, New Zealand). See Glenn Greenwald, Laura Poitras and Ewen MacAskill, "NSA shares raw intelligence including Americans' data with Israel", *The Guardian*, 11 November 2013 (http://bit.ly/1gEJI84).

[9] See Bill Binney, "Democracy and Surveillance Technology", *Congress on Privacy and Surveillance*, 30 September 2013 (http://slideshot.epfl.ch/events/cops).

intelligence services, but they work through the 'forced' participation of internet providers as a hybrid system, as part of a Public-Private-Partnership (PPP) whose consent is limited.

On the basis of the provisions of the US Foreign Intelligence Surveillance Act (FISA), the NSA, with an annual 'certification' of the FISA court, can target any non-US citizen or non-US legal resident located outside the territory of the US for surveillance.[10] These data, once intercepted, are filtered and the suspicious ones are retained for further purposes by the NSA and GCHQ. The stored data can then be aggregated with other data, and be searched via specifically-designed programmes such as X-KEYSCORE.

Furthermore, internet access providers in the US (but also in Europe) are under the obligation to keep their data for a certain period, in order to give law enforcement agencies the possibility to connect an IP address with a specific person under investigation. The legal obligations concerning access to data and privacy law derogations vary for the internet providers and the intelligence services, depending on the nationality of the persons under suspicion.

This has very important consequences for the European citizen using cloud computing or any internet service that transits through the US cable communications systems (possibly all internet traffic) on various levels:

- At present, the debate in the US on PRISM has centred on the right of American citizens to be protected from illegitimate purposes of data collection by NSA and other US intelligence agencies, with a focus on the US Patriot Act and FISA reforms. But the debate has been confined to US citizens in the context of US institutions and Constitutional frameworks. The implications for EU citizens need to be addressed too.
- As explained in a previous study by Caspar Bowden,[11] it is quite clear that European citizens whose data are processed by US intelligence services are not protected in the same way as US persons under the US Constitution in terms of guarantees concerning their privacy. Consequently the data of European data subjects are 'transferred' or 'extracted' without their authorisation and knowledge, and a legal framework offering legal remedies does not currently exist.

Under European law, the individual owns his/her own data. This principle is central and protected by the EU Charter of Fundamental Rights and the Treaty on the European Union. This aspect raises important legal issues that will be tackled in section 3 of this study: Can we consider unauthorised access to data as 'theft' (of correspondence)? Currently, channels permitting lawful search exist, such as the EU-US Mutual Legal Assistance Agreement (MLAA), which covers criminal investigations and counter-terrorism activities. However, in light of recent revelations, have the US services and their European member state partners followed the rules of this agreement? Moreover, and contrary to the US legislation, the EU Charter of Fundamental Rights requires data protection for everyone, not just EU citizens. The European Convention on Human Rights (ECHR) also guarantees the right to privacy for everyone not just nationals of contracting parties. Thus the overall framework of the right to privacy and data protection in the EU cannot be limited to EU citizens alone. However, protection arising from national constitutions could be also limited.

To solve this profound inequality of treatment, it would require either a change of US laws offering the same privacy rights to any data subject intercepted by their systems, regardless of their nationality, or an international treaty specifying a digital bill of rights concerning all data subjects, whatever their nationality.

The structure of the study

The study starts by shedding light on the Snowden's revelations and highlights to what extent we are witnessing a reconfiguration of surveillance that enables access to a much larger scale of data than telecommunication surveillance of the past. 'Large-scale' surveillance is at the heart of both a scientific controversy about what the different technologies of interception of digital messages can do when they are organised into platforms and planning tools in terms of the integration of data, and a political and ethical controversy about the use of these technologies by the intelligence services. The two controversies are often interwoven by the different actors in order to argue over the legitimacy of such practices.

---

[10] See section 702 of the FISA Act (http://bit.ly/1gEIXf5).

[11] Caspar Bowden (2013), "The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights", Study for the European Parliament, PE 474.405, Brussels, September. See the developments concerning the fact that under the FISA Act, section 702, non-US citizens are excluded from the scope of the 4th Amendment.

These preliminary remarks are critical for the second part of the study that deals with a comparative approach to European programmes of surveillance. Since the publication of the first revelations on the US PRISM programme, disclosures and allegations relating to large-scale surveillance activities by EU member states have emerged as a result of both the Snowden leaks and wider investigative journalism. Section 2 draws on a country-by-country overview of large-scale telecommunications surveillance activities/capacities of five EU member states: the UK, Sweden, France, Germany and the Netherlands (set out in Annex 1 of this study). The section draws a set of observations concerning the technical features, modalities and targets pursued by the intelligence services of these EU member states in harvesting large-scale data, and examines the national and international actors involved in this process and the cooperation between them. It highlights the commonalities, divergences and cross-cutting features that emerge from the available evidence and highlights gaps in current knowledge requiring further investigation.

These empirical examples are followed by an investigation of modalities of actions at the disposal of EU institutions concerning large-scale surveillance (section 3). This section tackles the EU competences concerning NSA surveillance programmes and general oversight over EU member state programmes of surveillance. It assesses the relationship between surveillance programmes and EU competence, employing three legal modalities of action to critically examine EU surveillance programmes from an EU law viewpoint.

The study concludes with a set of recommendations addressed to the European Parliament with the aim of contributing to the overall conclusions and the next steps to be drawn from the LIBE Committee's inquiry.

Methodological note

The exercise of piecing together the extent of large-scale surveillance programmes currently conducted by selected EU member states is hampered by a lack of official information and restricted access to primary source material. The empirical evidence gathered for the purpose of this study and presented in Annex 1 therefore relies on three broad forms of evidence:

1. ***Reports and testimony of investigative journalists***. Much of the publicly available evidence covering EU member states' engagement in mass surveillance-like activities stems from revelations of investigative journalists and their contacts with whistleblowers – current or former operatives of intelligence agencies. Press reports are in some cases very concrete in their sources (e.g. quoting from specific internal documents), while others are more ambiguous. Where possible we provide as much information concerning the journalistic sources used in this study; however, a cautious approach must be taken to material that researchers have not viewed first hand.
2. ***Consultation and input of experts via semi-structured interviews and questionnaires***. Experts consulted for this study include leading academic specialists whose research focuses on the surveillance activities of intelligence agencies in their respective member states and its compatibility with national and European legal regimes.
3. ***Official documents and statements***. Where possible, the study makes reference to official reports or statements by intelligence officials and government representatives which corroborate/counter allegations concerning large-scale surveillance by intelligence services of EU member states.

1. Controversy between the actors about the scale of the problem

KEY FINDINGS

- The PRISM scandal in the US and disclosures by Edward Snowden only serve to recall the recurrence of transgressions and illegal practices carried out by intelligence services.
- Surveillance of individuals or groups is not a new phenomenon in liberal regimes. It is the purpose and the scale of surveillance, however, that fundamentally differentiate democratic regimes and police states.
- Intelligence services have adopted several strategies to avoid the accusation of privileging security over liberty.
- There is a growing consensus that the attitudes of the NSA and the GCHQ, as well as other secret services in Europe, are no longer acceptable in a democratic society.
- Therefore, the analysis of European surveillance programmes cannot be reduced to the question of a balance between data protection versus national security, but has to be framed in terms of collective freedoms and democracy.

A scientific controversy, which has central implications in terms of politics and ethics in democracy, revolves around the idea that large-scale surveillance has to be contained. It implies a discussion about the role of technological developments historically and the use of these technologies in the service of intelligence services. These questions tackle the legitimacy of such operations, their impact in terms of data protection, privacy and discrimination between individuals. They also affect the question of the structure of democracy and collective freedoms. Therefore the key question is: What nature, scale and depth of surveillance can be tolerated in and between democracies?

The objective of this note is not to take sides or to arbitrate who is telling the truth in these controversies, as the time constraint make it impossible to have a clear view of what is knowledge and what are allegations.[12]

This is why it is important to take into account the methodological note set out in the introduction outlining the limits of the knowledge accumulated and to acknowledge the speculative part of the argument. Nevertheless, these limits, once accepted, do not hamper the possibility for the note to propose as a main objective to find solutions that can be accepted despite the discrepancy between these strongly opposing interpretations.

This study suggests that the controversy over large-scale harvesting of data has to be understood along a continuum of intelligence services activities: 1) counter-terrorism activities that follow a criminal justice logic, 2) counter-terrorism activities that try to monitor the future by profiling suspects, 3) cyber-spying activities that target specific groups in a military strategic approach and 4) electronic mass surveillance activities carried out without clear objectives.

We aim to devise a 'red-line' approach that would be accepted by all the actors involved. The actors would agree not to cross this line in the future, to fully respect democratic rules, while pursuing their mission of protection against crime and terrorism.

1.1 Large-scale electronic surveillance in democracies: Compatibility or not?

The characteristics of large-scale electronic surveillance differ in many ways from traditional intelligence activities. This section aims at highlighting how the possibilities opened up by the ever-increasing digitalisation of human activity redefine the scale of surveillance, its rationale and its underlying logic.

[12] D. Omand (2008), "Can we have the Pleasure of the Grin without Seeing the Cat? Must the Effectiveness of Secret Agencies Inevitably Fade on Exposure to the Light?", *Intelligence and National Security*, Vol. 23, No. 5, pp. 593-607.

1.1.1 Surveillance, Intelligence services and democracy

Surveillance of certain population groups is not a new phenomenon in liberal regimes. Specific groups of individuals have often been targeted by intelligence services, because they were suspected of conducting criminal activities (including political violence). Even if democratic regimes have not gone as far as authoritarian ones, whose intelligence bodies spy systematically on their own populations in order to detect dissent in political opinions in the name of a doctrine based on the idea of 'enemies within' (such as the STASI in the former Democratic Republic of Germany, the *Securitate* in Romania or the UDBA in former Yugoslavia), they still have a history of large-scale surveillance.

It is precisely the purposes and the scale of surveillance that differentiates democratic regimes from police states. Even if there have been transgressions in the past, intelligence services in democratic regimes in principle do not collect data in mass on large groups of the population, and if surveillance is undertaken of specific individuals, it is on the ground that collection of data is deemed necessary to detect and prevent violent actions in the making, not to gather information on life styles or political opinions. At least this has worked as a kind of 'agreement', a shared understanding between the State and the citizens, which is well captured in this quote:

> 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.[13]

Nevertheless, when the ramparts against full surveillance are not checked regularly, they may stop operating. In the name of the development of high technologies and their use by 'enemies', intelligence services have crossed these boundaries in the pursuit of their missions. This is frequently accompanied by a redefinition of who is the enemy (or the suspect) and how far s/he has already infiltrated the territory, which overstretches the notion of national security. In a democracy, however, the separation of power exists, and the excess of intelligence services have been regularly denounced when their unlawful activities, often concealed behind a veil of secrecy that characterises intelligence-led policing, have been uncovered.

The PRISM scandal in the US and the recent revelations by Edward Snowden only remind us of the recurrence of wrongdoings and illegal practices in 'targeted surveillance' carried out by intelligence services as well as the resistance of the political authorities to recognise that the services went too far. In the past and prior to PRISM et al.,[14] US authorities have been condemned on numerous occasions for the surveillance and infiltration of large groups of individuals by law enforcement authorities. Activists in the civil rights movement and the Communist Party of the United States were the targets of the 1950s and the anti-war movement in the 1960s and the 1970s. Secret programmes were in place with an extensive use of informants, intercepted mail and phone calls and engineered break-ins.[15] COINTELPRO in the late 1950s, CHAOS and MINARET in the 1960s and 1970s were all recognised as unlawful surveillance programmes and specific rules have been elaborated to protect US citizens from this political surveillance.

The Foreign Intelligence Surveillance Act (FISA) court was specifically designed in 1978 to counterbalance the intelligence powers and to give the judiciary the power to oversee alleged 'foreign intelligence' activities, especially if they were affecting fundamental rights of US citizen. As detailed elsewhere, this court has constantly seen its powers undermined, even more so after 9/11 and the launch of the war on terror.[16] The court's scope is also limited to the protection of US citizens, and does not include non-US persons even though the latter are also the victims of unlawful surveillance. The current PRISM and other NSA activities and their relationship to other intelligence services and private companies in the US further illustrates the limitations of powers of the judiciary over intelligence activities, as well as the difficulty to implement

---

[13] A. Dulles (1963), *The Craft of Intelligence*, New York, NY: Harper&Row, p. 257.

[14] Even if we acknowledge that PRISM is only a small programme within the broader NSA programmes of surveillance, and that other meaningful programmes have been exposed – such as XKeyscore, we will keep 'PRISM et al.' as a generic reference to designate NSA programmes to ensure clarity.

[15] See G.T. Marx (1989), *Undercover: Police Surveillance in America*, Berkeley, CA: University of California Press.

[16] On FISA loopholes and the court's limitations, see the note produced by Caspar Bowden (2013), "The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights", Study for the Committee on Civil Liberties, Justice and Home Affairs, European Parliament, PE 474.405, Brussels, September.

parliamentary oversight over such activities, including the participation of private actors having a global reach in surveillance.

In Europe, a series of scandals emerged when the practices of undercover policing and surveillance of political parties endangered civil liberties, but they were more connected with infiltrations and undercover operations than mass surveillance. In Spain the creation of the GAL (Grupos Antiterroristas de Liberación) to fight ETA ended up, after many years of procedure, with the condemnation of the former Minister of Interior and his imprisonment in 1996. In France, the *Renseignements Généraux* were threatened to be shut down after a series of illegal activities involving illegal phone-taps and the presumed assassination of a gay activist in the 1990s, the Pasteur Doucé. More recently, in June 2013, Luxembourg's Prime Minister Juncker officially announced he would resign following a spying scandal, involving the illegal bugging of politicians.

By the late 1990s, the need for oversight of intelligence activities by parliamentary or judicial authorities has progressively been widely accepted, but not without difficulties. French intelligence services only recently agreed to an external procedure of control. The *Renseignements Généraux* have partly survived under the DCRI,[17] but their missions have been re-oriented. These services always insisted that they either focused on very specific cases connected with spying or political violence, or that they were *only* undertaking better 'opinion polls' than the researchers and private companies providing similar 'services'. As detailed later in this study, the specificity of large-scale surveillance considerably challenges these supposedly reassuring statements and raises the question of the connections between the services in charge of anti-terrorism and the services in charge of collecting data for large-scale surveillance.

The 'war on terror' launched after the events of 9/11 somehow shook the fragile consensus according to which democracies do not carry out mass surveillance and any surveillance activities should be subject to some form of oversight. In the US, and to a lesser degree in Europe, a series of programmes have been initiated, in secret, using all existing resources of modern information technology. The possibilities of surveillance have increased at the same pace of the increase of data availability. Regular increases in bandwidth have enabled new uses of the Internet, such as mass storage and processing of personal, private and governmental data through cloud computing. The development of mobile computing devices (e.g. smartphones and tablets) has similarly provided a wealth of new geo-localised, personal information.

Each time a scandal occurs, as in the Swift and Terrorist Finance Tracking Programme (TFTP) scandals and their repercussions in EU-US relations,[18] the demand for an oversight of intelligence activities by parliamentary and/or judicial authorities gains more legitimacy. Clearly the modalities of oversight remain challenging and their implementation highly problematic, because surveillance programmes are often transnational and have a global reach, but also because of the ability of these services to cloak their activities with a veil of secrecy (the 'classified information' argument). The alleged difficulty to draw the line between the interests of the State, those of a specific government or of a specific political group (when these are not purely private interests) only adds to the current problem.[19] In addition, when the programmes are using world-wide surveillance on citizens of other states, without the knowledge of these citizens, and even sometimes without the knowledge of their governments, the question is no longer one of data protection and the privacy of an individual versus the state, it becomes a question of democracy itself where systematic surveillance of a 'mass' of people may undermine the regime, while arguing that it is for its protection (see section 3).

1.1.2 Large-scale surveillance and mass surveillance: What is at stake?

This study insists on the difference that exists between the scale and depth of the programmes that are connected to PRISM et al. and the programmes previously undertaken in counter-terrorism and counter-

[17] DCRI (Central Directorate of Interior Intelligence) is the French government agency responsible for counter-espionage and counter-terrorism. It will soon to be replaced by the General Direction of Interior Security (DGSI).

[18] A. Amicelle (2011), "The Great (Data) Bank Robbery: Terrorist Finance Tracking Program and the 'SWIFT Affair'", Research Question 36, CERI, Sciences-Po, Paris.

[19] See P. Gill (2012), "Intelligence, Threat, Risk and the Challenge of Oversight", *Intelligence and National Security*, 27:2, pp. 206-222; see also A. Wills, M. Vermeulen, H. Born, M. Scheinin, M. Wiebusch and A. Thornton (2011), Parliamentary Oversight of Security and Intelligence Agencies in the EU, Note for the European Parliament (PE 453.207), Brussels, 15 June.

spying. What has to be questioned here is the possible transformation of large-scale surveillance into what can be called a 'cyber-mass surveillance' that enables access without warrant to a much larger scale of data than telecommunications surveillance of the past, such as ECHELON.

Ironically, it was the European Parliament's inquiries about NSA's ECHELON programme in 2000 and 2001 that already revealed that surveillance programmes capable of interception and content inspection of telephone calls, fax, e-mail and other data traffic globally through the interception of communication bearers including satellite transmission were in place.[20] As reported to the European Parliament by the then whistle-blower Duncan Campbell, ECHELON was one part of a global surveillance system involving cooperation of satellite stations run by the UK, Canada, Australia and New Zealand.[21] Concern was aroused in particular by the assertion in Campbell's report that ECHELON had moved away from its original purpose of defence against the Eastern bloc and was being used for purposes of industrial espionage.[22]

Other US programmes that were denounced by watchdogs can be mentioned, such as CAPPS I & II (Computer-Assisted Passenger Pre-Screening System) and US-Visit related Personal Name Records (PNR), which gather personal information from unidentified government databases as well as commercial data sources to set up no-fly and terrorist watch lists; NIMD (Novel Intelligence from Massive Data), an initiative of the secretive intelligence community's Advanced Research and Development Activity (ARDA), which focuses on 'massive data'; and MATRIX (Multistate Anti-Terrorism Information Exchange), a state-level programme supported by the US Department of Justice. MATRIX aims to give state law-enforcement agencies across the United States a powerful new tool for analysing the personal records of both criminals and ordinary Americans. According to an article published in the *Washington Post*, the programme "would let authorities (...) instantly find the name and address of every brown-haired owner of a red Ford pickup truck in a 20-mile radius of a suspicious event".[23]

This reminder of such surveillance programmes and the intelligence activities they authorised sheds a particular light over the Snowden revelations. Two main aspects should be underlined here: PRISM et al. should not be considered as an abrupt departure from past practices (even though their magnitude is quite unique), nor as an isolated set of initiatives, as many other parts of the world develop similar programmes, as described in section 2.

A series of programmes have been initiated, using all existing resources of the Internet, both in the US and in Europe, after 2004 with the development of integrated platforms, the breaking of software encryption keys and the development of new software that permits the routine filtering, visualising and correlating unprecedented amounts of data and metadata. These new resources for surveillance, the widespread use of smart phones and the development of cloud computing have blurred the line between 'targeted surveillance' – justified by the fight against crime – and data mining, which carries the risk of extending the scale and the purpose of surveillance. These programmes have been justified by the intention to protect the population from crimes, and were tailored to provide tools for the profiling of categories of people likely to commit such crimes. However, once data are available to search and extraction, they may be put to other purposes.

---

[20] On ECHELON, see European Parliament (2001), "Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))", PE 305.391 A5-0264/2001. See resolutions on the right to privacy and data protection, in particular that of 5 September 2001 on the existence of a global system for the interception of private and commercial communications (Echelon interception system) OJ C 72 E, 21.3.2002, p. 221.

[21] Duncan Campbell (2000), "Inside Echelon: The history, structure, and function of the global surveillance system known as Echelon", *Telepolis* (www.heise.de/tp/artikel/6/6929/1.html); Duncan Campbell (1999), "The state of the art in communications intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems and its applicability to COMINT targeting and selection, including speech recognition", Part 2/5, in STOA (ed.), *Development of Surveillance Technology and Risk of Abuse of Economic Information*, October, Study for the Committee on Civil Liberties, Justice and Home Affairs, European Parliament, Brussels (PE 168.184).

[22] See Final Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)), PE.305.391.

[23] "U.S. Backs Florida's New Counterterrorism Database: 'Matrix' Offers Law Agencies Faster Access to Americans' Personal Records", The Center for Investigative Rerporting, 5 August 2013 (http://bit.ly/1gEOGBR).

One such attempt, the "Total Information Awareness" (TIA) programme, has been precisely rejected by the US Congress on this ground in 2003 and (at least publicly) limited to Terrorism Information Awareness. Yet the idea of warrantless wiretapping was accepted at that time, as well as blanket data searches. Revealed in 2005 by the *New York Times*, this programme was strongly denounced, but it was not dismantled and was de facto legalised in 2007 by the *Protect America Act*.

The developments raise a number of questions: How far do PRISM in the US and Tempora in the UK follow or not the same logic as TIA? Do they maintain a purpose limited to terrorism and crime or are the data used also for tax evasion, for advantaging some private companies in their contracts, for profiling the political opinions of groups considered as suspect, for elaborating scenarios concerning political conflicts and international situations?

Concerns increasingly arise that these programmes are in addition interconnected and that some European member state services participate in these extractions of Internet data for multi-purpose 'explorations'. Snowden indeed claimed that data collected by the Tempora programme are shared with the NSA and that no distinction is made in the gathering of data between private citizens and targeted suspects.[24] But GCHQ has strongly insisted that they were not using data for indiscriminate searches,[25] and that this use was restricted for national security and the detection and prevention of crime. One may ask: Precisely where is the 'red line' that intelligence services in democratic regimes should not cross when they use cyber-surveillance and do the US and the EU have a shared understanding as to where that red line is?

1.2 Political and ethical controversies regarding the use of these technologies by intelligence services: The question of legitimacy

1.2.1 The position of the security services

Intelligence services have adopted several strategies in order to avoid the accusation of privileging security over liberty and threatening the nature of democratic regimes:

- Some security services have insisted that they follow specific protocols, with the full knowledge of their other European partners. They argue that surveillance has been strictly limited to counter-terrorism operations and that surveillance took place on a small scale. When they do acknowledge that they run large-scale surveillance programmes, they insist that they use data only to confirm information they already have in their possession, and that this surveillance only targets small groups of individuals or IP addresses. Therefore, according to them, this cannot be assimilated to data-mining.
- Other services or other persons in the same services assert that they were not carrying out counter-terrorism operations, but cyber-security and cyber-defence and that they have the right to conduct such activities beyond the scope of the EU-US Mutual Legal Assistance Agreement (MLAA),[26] that they have their own right to define what were the boundaries of their national security and that they were not constrained by any international agreement.[27] They also consider that these activities do not violate Article 4.3 of the Treaty of the EU concerning the loyalty of the member states to the principles of the EU Charter, and that they were fully covered by Articles 4.2 and 72 that reserves intelligence activities to the member states only. In their views, impunity prevails.

---

[24] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, "GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications", *The Guardian*, 21 June 2013.

[25] Tempora is considered as a 'buffer', which keeps the Internet data passing through the cable for a couple of days, in order to give more time to the teams who search suspects to have a 'line' of conversation. They extract data from the cable to find IP locations and emails associated, but they do not retain the data in mass or use them for general profiling.

[26] See section 3 for more discussion of the MLAA.

[27] Gen. Keith Alexander, Director of the NSA and Chief of the Central Security Service (CHCSS) as well as Commander of the United States Cyber Command, has made the link between the new project of cyber defence that he defended on 12 March 2013 before the US Congress and the Snowden 'leak' which in his view undermines the capacity of the US to respond to foreign nations' cyber attacks. See M. Mazzetti and D. Sanger, "Security Leader Says U.S. Would Retaliate Against Cyberattacks", *The New York Times*, 12 March 2013; E. Nakashima, "NSA chief defends collecting Americans' data", *The Washington Post*, 25 September 2013.

Security services and several academics working on intelligence often refer to the fact that open societies also have enemies, including internal enemies, and that the secret services have been set up to act beyond the legal framework, not to be prisoner of it. They consider that only their own government, and often only the president or the prime minister, has the right to know what they do. They also deny the fact that the international or European Courts may have a say on this matter. It is a strong professional habit and a discourse largely shared by different US and European services, especially the ones that are not often in touch with the judiciary. This attitude and the series of beliefs it implies constitute the heart of the general problem of the different interpretations of the legitimacy of the practices revealed by Snowden on PRISM.

1.2.2 The position of the other actors

Clearly, **not all branches of government accept** the attitude of the secret services. The considerations of a government tied by the rule of law differ from one country to another one. Some have a more 'permissive' legal environment than others. Most, but in practice not all, governments of the EU considered that they have to respect the decisions of the European courts – Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR) concerning the right to life, torture or data protection and privacy even when they limit their so-called 'freedom of action'. The US does not seem ready to accept any constraint of that sort if the principles do not exist in its own Constitution.

In the case of the PRISM affair, and previously in the case of TFTP, Commissioner Viviane Reding wrote a letter to the US Attorney General, Eric Holder, raising European concerns and asking for clarification and explanations regarding PRISM and other such programmes involving data collection and searching, and the laws under which such programmes may be authorised. A detailed answer from the US authorities is still pending months after the events, despite the discussions which took place at the EU-US Justice Ministerial meeting in Dublin on 14 June 2013.

Some lawyers, civil servants, NGOs and journalists have considered that these permanent delays in answering, and the silence of the intelligence services in the matter, further legitimise the need to take urgent action against the double standards that the US government imposes on its partners. They consider that the US government maintains the fiction of a global collaboration against crime and terrorism while applying a strategy of full spectrum dominance, which is increasingly aggressive and they consider their technological advances as a strategic advantage against their allies. In this case, the image of a community of nations is clearly undermined in favour of a revival of national struggles for dominance and a clash of sovereignties. This reformulation affects US-EU relations, but also the internal relations between member states in the EU. As we will see in section 3, respect for other country's sovereignty is one of the key questions emerging from the PRISM affair and other programmes carried out by European services, inside Europe and in the context of transatlantic collaboration.

In this context, a lack of action on the part of the European Parliament would profoundly undermine **the trust and confidence** that EU citizens have in the European institutions, and especially in the European Parliament to safeguard and protect the most fundamental freedoms related to their private and family lives.

Actors of civil societies, especially journalists of the most-respected newspapers in the world, and human rights NGOs consider that the attitudes of the NSA and GCHQ, but also those of other secret services in Europe, are not acceptable. In the case of the GCHQ in the UK, civil society actors consider that their actions could be labelled as acts of cyber warfare aggression, as a form of treason of European member states' services spying on other EU citizens on the behalf of their US counterparts, and that if it is not treason per se, it is a breach of trust and confidence in terms of solidarity with the EU, by placing other allegiances with third parties against that with the EU.

Other European secret services also have to be watched. They may not be directly connected with the transnational network of the NSA, but they may try to build their own apparatus. France and Germany have developed on a smaller scale some equivalent capabilities and reportedly access transnational electronic communications without a regular warrant but on the basis of special courts. They also share data with other countries. These aspects are further developed in section 2.

The reaction from a part of the civil society has been stronger than the political reactions that always tend to minimise the possible transatlantic rift. Most of the newspapers (especially in the comments left by readers) and internet blogs have spoken favourably in favour of Snowden and other whistleblowers. And they have encouraged an anxiety concerning the rise of surveillance which often mixes facts and fears concerning a

totalitarian future, with references to Georges Orwell, Philip K. Dick or an easy reading of Michel Foucault. These reactions are for the moment concentrated in the 'infosphere' of Internet bloggers, but after the arrest of David Miranda, the partner of the journalist Glenn Greenwald of the Guardian by GCHQ, a large part of the world's investigative journalists have started to share the image of a 'state of exception' in the making, or of a 'surveillance state'.[28] Journalists and human rights NGOs have joined the more marginal scenes of the infosphere in favour of freedom of the Internet. Many activists consider that the easy availability of surveillance technologies cannot be a justification for their use and some of them regularly use the formula that we are "sleepwalking into a surveillance state". Joined by an increasing number of persons, they refuse to accept such a disproportion between the massive collection of data and metadata, the length of their retention in regards to the so-called 'objective of preventing terrorism', which has become a blanket excuse for mass data collection used for many other purposes.

For these reasons, an analysis of Europe's surveillance programmes cannot be reduced only to the question of the proper balance between data protection and national security and to technical capabilities understood by experts. Rather, it has to be framed in terms of collective freedoms and the nature of democratic regimes.

If derogations to data protection exist, national security cannot be a justification for a structural transformation of the rule of law and democratic expressions of civil societies in an open world of information.

If future inquiries show that most of the actions undertaken by the NSA, GCHQ and other European services – in collaboration or in competition between them but using the same practices – have not only focused on counter-terrorism activities, but also on economic espionage, illegal bugging of political leaders and EU institutions, and possibly on data mining for purposes of total information awareness, as well as on manipulation of opinion and strategies to influence life styles and consumption habits, then the responsibility of these services and their governments has to be dealt with from a judicial perspective. Even if future research may show that the different EU member states' intelligence services have restricted their activities to counter-terrorism and not mass surveillance, this does not prevent the need for principles of necessity and proportionality.

In this context, we next try to answer the following key questions:

- Among the various surveillance programmes in place in Europe, which ones share a similar logic as informs the NSA's logic? Which ones involve forms of cooperation with the NSA?
- How do surveillance programmes fit into the idea of a European Union in solidarity in terms of foreign affairs but also in terms of shared fundamental rights equally available for all citizens?
- If the question of the use of technologies of surveillance is a political one, then who should address it: the member states or all the institutions within the EU that are involved in protecting the open nature of the societies comprising the population of Europe?

[28] Edwy Plenel, "Contre l'Etat d'exception", *Mediapart*, 10 August 2013 (http://bit.ly/1gETpDB).

2. EU member state practices in the context of the revelations of NSA large-scale operations

KEY FINDINGS

- The overview of publicly available knowledge on large-scale surveillance activities by five EU member states – the UK, Sweden, France, Germany and the Netherlands – reveal evidence of engagement in the large-scale interception and processing of communications data by four of those member states. Further investigation and research are required in order to gain a better understanding of the techniques, capacities and lawfulness of these programmes.
- Practices of so-called 'upstreaming' (tapping directly into the communications infrastructure as a means to intercept data) characterise the surveillance programmes of all the selected EU member states, with the exception of the Netherlands for which there is no concrete evidence of engagement in large-scale surveillance.
- The capacities of Sweden, France and Germany (in terms of budget and human resources) are low compared to the magnitude of the operations launched by GCHQ and the NSA and cannot be considered on the same scale.
- There is a multiplicity of intelligence/security actors involved in processing and exploiting data, including several, overlapping transnational intelligence networks dominated by the US.
- Legal regulation of communications surveillance differs across the member states examined. In general, however, legal frameworks are characterised by ambiguity or loopholes as regards large-scale communications surveillance, while national oversight bodies lack the capacities to effectively monitor the lawfulness of intelligence services' large-scale interception of data.

The following section draws on the evidence presented in Annex 1 on practices of large-scale surveillance being conducted by the intelligence services of EU member states. Annex 1 conducts an in-depth assessment of five countries where existing evidence (drawn from investigative journalism, academic analysis and official documentation) indicates large-scale electronic surveillance practices that may be classified as mass surveillance: the UK, Sweden, France, Germany and (potentially in the future) the Netherlands.

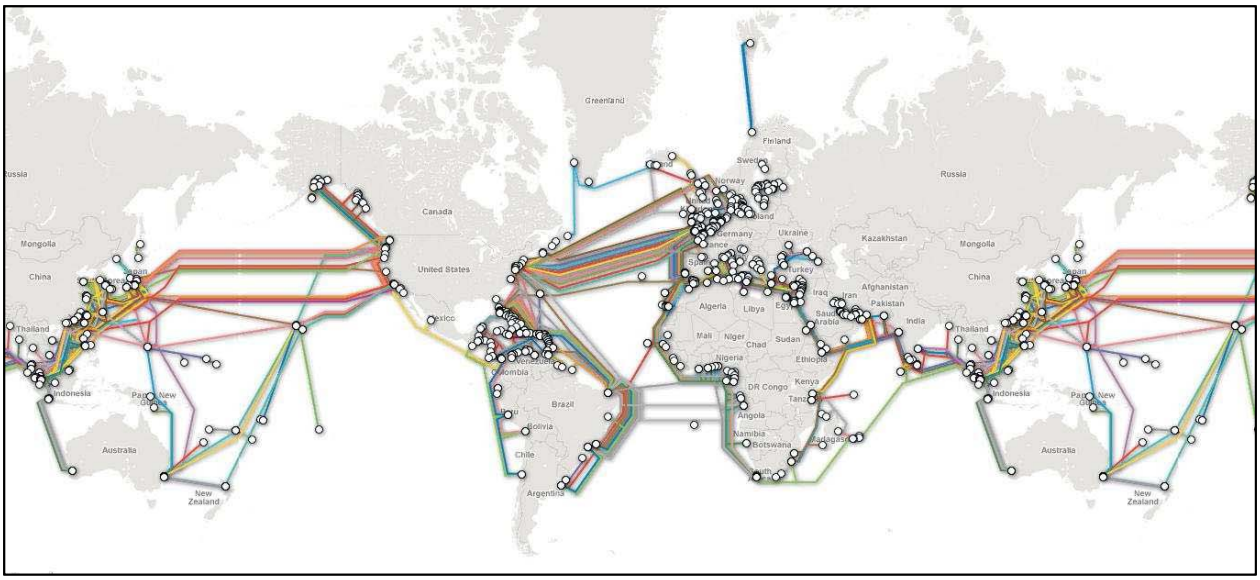
Disclosures since June 2013 surrounding the activities of the UK's GCHQ indicate a range of programmes and projects linked to the mass interception, storage and processing of telecommunications data, at the core of which is the so-called 'Tempora' programme (see section 1, Annex 1). These revelations were followed in September 2013 by reports focusing on the activities of Sweden's National Defence Radio Establishment (FRA). Operations and programmes for the mass collection of data by the FRA are reportedly elevating this agency to an increasingly important partner of the global intelligence network (section 2, Annex 1). Evidence has simultaneously emerged concerning similar projects for the large-scale interception of telecommunications data by both France's General Directorate for External Security (DGSE) (section 3, Annex 1) and Germany's Federal Intelligence Service (BDE) (section 4, Annex 1). There are strong suggestions to indicate that several if not all of these member states are engaging in exchanging this intercepted data with foreign intelligence services, namely the NSA. In addition, other EU member states are currently in the process of expanding their signals intelligence capabilities, with the Netherlands' establishment of a new Joint Sigint Cyber Unit (JSCU) (section 5, Annex 1) providing a prime example.

Each of these five member states is examined considering the following criteria: the basic technical features of large-scale surveillance programmes; stated purpose of the programmes, targets and types of data collected; actors involved in collection and use, including evidence of cooperation with the private sector; cooperation or exchange of data with foreign intelligence services, including the NSA; and the legal framework and oversight governing the execution of the programme(s). On the basis of these criteria, do surveillance programmes run by EU member states share commonalities with those executed by the NSA? How do they compare in terms of scale, technical features and the degree of accountability and oversight? The member state by member state overview in Annex 1 reveals several common features/points of diversion and cross-cutting issues, as discussed below.

2.1 Technical features

As documented in Annex 1, the practice of so-called 'upstreaming' – tapping directly into the communications infrastructure as a means to intercept data – appears to be a relatively widespread feature of surveillance by several EU member states, namely the UK, Sweden, France and Germany. Disclosures by The Guardian in July 2013 on GCHQ's so-called 'Tempora' programme allege that the UK intelligence service have placed interceptors on approximately 200 undersea fibre-optic cables which arrive at the south-west coast of Britain.[29] These revelations were followed in September by a renewed focus on the activities of Sweden's FRA, which has seen intermittent reports over the last five years concerning the interception and storage of communications data from fibre-optic cables crossing Swedish borders from the Baltic Sea.[30] The last three months have also seen reports citing France and Germany as relying on upstreaming methods as a means to gather bulk data.[31] This method of interception is believed to be a relatively recent addition to the surveillance arsenal of these member states' intelligence services, with most programmes dating from around the late 2000s (see Annex 1). They therefore are understood to complement the more established satellite interception programmes pursued by US and EU intelligence services (UK, Sweden, France) of which the most extensive is FORNSAT, the successor of the ECHELON programme, as the main networked foreign satellite collection system coordinated by 'Five Eyes' (see section 2.5 below).[32]

Figure 1. Map showing concentration of global submarine cables



Source: Telegeography - Global Bandwidth Research Service (http://www.submarinecablemap.com/)

At the same time, there is little evidence (with the exception of reports concerning Germany)[33] that the intelligence services of EU member states are currently engaged in collecting data directly from the servers of private companies, as employed in NSA's PRISM programme. For the moment at least, this practice appears to be restricted to the US. However, given the secrecy surrounding intelligence services activities, and the allegations concerning cooperation between Germany's BND and private internet service providers, it would require further in-depth investigation to draw any firm conclusions.

---

[29] E. MacAskill et al. (2013), "GCHQ taps fibre-optic cables for secret access to world's communications", *The Guardian*, 21 June.

[30] N. Nielsen (2013), "EU asks for answers on UK snooping programme", *EU Observer*, 26 June.

[31] J. Follorou and F. Johannes, "Révélations sur le Big Brother français", *Le Monde*, 4 July 2013; Spiegel Online, "100-Millionen-Programm: BND will Internet-Überwachung massiv ausweiten", 16 June 2013.

[32] Statement by Duncan Campbell at the European Parliament's LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, 1st Hearing, 5 September 2013.

[33] P. Beuth, "Wie der BND das Netz überwacht", *Zeit Online*, 18 June 2013.

2.2 Scale

Given the scarcity of information concerning the programmes detected, and particularly the programmes by EU member states, it is difficult to draw firm conclusions concerning the relative scale of these practices. Nevertheless, a clear distinction can be made between the US/UK mass interception and data analysis programmes (such as PRISM, Upstream and Tempora) and the surveillance practices by other EU intelligence services. In terms of budgetary allocation, human resources and the quantity of data collected and analysed, it appears unlikely that the programmes of EU member states such as Sweden, France and Germany come close to the sheer magnitude of the operations launched by GCHQ and the NSA.

First, the capacities of the aforementioned EU member states' intelligence services are relatively limited, with annual budgets of around €500 million[34] (see Annex 1) as opposed to the $10 billion annual budget of the NSA.[35] The PRISM programme is relatively low cost (an estimated $20 million), because much of the financial burden of data collection and processing falls on the companies themselves (Apple, Google, Facebook, etc.). Nevertheless, there is evidence that the NSA makes a substantial budgetary outlay on electronic large-scale surveillance, for instance spending $250 million a year on programmes to circumvent encryption technologies.[36] GCHQ meanwhile is reported to have invested approximately £1 billion (€1.2 billion) in its 'Mastering the Internet' project, which allegedly provides the overarching framework for Tempora as well as several other telecommunications surveillance programmes (see Annex 1).[37]

We can also infer from the relatively low staffing capacities of the key EU intelligence services under scrutiny (generally in the low thousands as opposed to the NSA's 30,000-40,000 employees[38] – see Annex 1) that the surveillance practices undertaken by these member states are relatively modest. The processing and analysis of mass data requires a significant human resources investment, as indicated by reports that the NSA has allocated 850,000 of its operatives and external contractors to process the data captured by surveillance activities (including data intercepted and shared by GCHQ).[39] However, this observation raises several further questions, if we consider reports of growing technical capacities of intelligence services of EU member states such as Sweden and France for gathering bulk data (e.g. from upstream interception techniques): without the organisational capacity to process mass data, how is this data handled, is it for purposes of internal processing or exchange with foreign intelligence services?

2.3 Data types and data targets

Commonalities can be traced in the types of data targeted by programmes pursued by both the NSA and EU member states' intelligence services. As in the case of the NSA, the UK and Sweden collect both metadata and content, with the storage and handling of data differentiated depending on whether it consists of metadata or content.[40] In France, reports only allude to the collection of metadata while in Germany information pertaining to the type of data collected is unavailable.

In certain EU member states (UK, Sweden and Germany), programmes nominally target so-called 'external communications'.[41] Hence, the official targets of surveillance programmes are those communications that

---

[34] Both Germany's BND and Sweden's FRA were allocated annual budgets of approximately €500 million in 2012. GCHQ's annual budget is reported to be approximately €1 billon. See Annex 1.

[35] B. Gellman and G. Miller, "U.S. spy network's successes, failures and objectives detailed in 'black budget' summary", *Washington Post*, 29 August 2013 (http://www.washingtonpost.com/wp-srv/special/national/black-budget/).

[36] J. Ball, J. Borger and G. Greenwald, "Revealed: how US and UK spy agencies defeat internet privacy and security", *The Guardian*, 6 September 2013 (http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security).

[37] D. Leppard and C. Williams, "Jacqui Smith's secret plan to carry on snooping", *The Sunday Times*, 3 May 2009.

[38] M. Rosenbach, "Prism Exposed: Data Surveillance with Global Implications", *Der Spiegel*, 10 June 2013 (http://www.spiegel.de/international/world/prism-leak-inside-the-controversial-us-data-surveillance-program-a-904761-2.html); NSA (2012), "60 Years of Defending our Nation" (http://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf).

[39] MacAskill et al. (2013), op. cit.

[40] See Annex 1 (sections 1 and 2).

[41] See Annex 1 (sections 1, 2 and 4).

take place outside the territory of the member state in question (but which are routed through the national communications infrastructure) or that take place between a resident of that member state and a foreign contact. This is a consequence of national legal regimes which limit or place more stringent safeguards on the monitoring of internal communications. As a consequence, parallels can be drawn with the discriminatory approach taken by the NSA under FISA in only targeting those communications by non-US nationals as they pass through communications infrastructure on US territory. However, although the UK, Swedish and German large-scale surveillance programmes in principle intend to intercept only external communications, in practice interception is likely to be less discriminate given that internal communications are often routed outside a member state's territory. As a consequence, all users of telecommunications (email, phone, social media, etc.) may potentially fall victim to having their communications data intercepted. What is currently not clear is whether the internal communications that are unintentionally intercepted are systematically disregarded or whether they are (illegally) retained and processed by intelligence services.

The lack of information on how data are analysed and processed once collected makes it difficult to shed light on the ultimate targets of this surveillance exercise. A common feature of the surveillance programmes identified in the EU and the NSA programmes is the lack of clearly delineated set of objectives, or grounds justifying the resort to electronic surveillance. There is no evidence across the member states selected for examination that surveillance programmes are restricted to counter-terrorist operations or countering external (military) threats. Rather, it appears from the available evidence that the ultimate data subjects targeted by these programmes are broad. For instance, the UK's GCHQ acknowledge that the targets of its programmes "boil down to diplomatic/military/commercial targets/terrorists/organised criminals and e-crime/cyber actors".[42]

2.4 Processing and analysis of data

The scale of the big data collected from upstream interception requires establishing systematic methods, techniques and infrastructure to filter such large flows of information. Electronic large-scale surveillance implies data extraction, data comparison, data retention and the use of a great variety of databases. Concrete and detailed information on how data collected via the programmes discussed in Annex 1 are processed, filtered and analysed is currently unavailable, although hints as to the methods used to filter metadata and content are cited in reports and expert statements (see Annex 1).

These include the use of so-called 'Massive Volume Reduction' employed by the UK's GCHQ to reduce bulk data by removing 30% of less intelligence-relevant data such as peer-to-peer downloads ('high-volume, low-value traffic').[43] Reports with regard to UK and German programmes also cite the use of 'selectors' (e.g. keywords, email addresses, phone numbers of targeted individuals) to search data.[44] These 'selectors' allegedly allow intelligence services to access the content of an individual's communications, gather information about anyone that individual communicates with and track locations online and offline, in turn permitting intelligence services to create sophisticated graphs of targets' social networks, associates, locations and movements.[45]

However, the lack of further detail leaves an important gap in our understanding of the practices that intelligence services are engaging in to exploit the bulk data collected. These details would be critical to determine operational legitimacy and interaction with national legal frameworks regulating surveillance (see section 2.6 below). For instance, must operatives first register an authorised initial target before launching a search or do they have a wide margin of manoeuvre when searching data? Do intelligence services engage in statistical analysis of the data gathered, and if so, based on which criteria? Are private companies engaged to collaborate in the engineering and design of algorithms and specific software that enable the compilation and

---

[42] E. MacAskill et al., "Mastering the internet: how GCHQ set out to spy on the world wide web", *The Guardian*, 21 June 2013 (http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet).

[43] MacAskill et al. (2013), op. cit.

[44] Ibid. and Spiegel Online, "100-Millionen-Programm: BND will Internet-Überwachung massiv ausweiten", 16 June 2013 (www.spiegel.de/politik/deutschland/internet-ueberwachung-bnd-will-100-millionen-investieren-a-905938.html).

[45] J. Risen and L. Poitras, "N.S.A. Gathers Data on Social Connections of U.S. Citizens", *New York Times*, 28 September 2013 (http://mobile.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html).

classification of specific trends, patterns and profiles? More information as regards these questions would be essential in order to establish to what degree the exploitation of bulk data manifests characteristics of data-profiling and data-mining, which has so far been vigorously denied by intelligence service officials.[46]

What is clear, however, is that data appear to serve 'multi-purpose' ends. This can be inferred from the multiplicity of actors engaged in using data from European surveillance programmes once processed and filtered (see below).

2.5 Cooperation between national and international security actors

A cross-cutting feature of the surveillance programmes examined is the multiplicity of intelligence/security actors involved in processing and exploiting data. For instance, in Germany and France, the evidence indicates that large-scale surveillance programmes constitute intelligence platforms that feed multi-level exchange of data between national law enforcement and security bodies.[47] Intelligence reports drawn from Sweden's surveillance programme also feed at least eight different 'customer' organisations ranging from defence agencies to law enforcement and customs bodies.[48] The large number of organisations with access to metadata or as recipients of intelligence drawn from this data again reflects the indication that data are being used for a wide range of security purposes far beyond the narrow focus of counter-terrorism and defence, which have traditionally formed the primary focus of national intelligence activities.

Cooperation with foreign intelligence services also appears to be a common feature of the member states' programmes outlined in Annex 1. In certain cases, there are reports/allegations of large-scale data exchange with the NSA (the UK, Sweden and Germany). Cooperation with the US also appears to extend to collaboration/sharing of research to advance the technological means of mass surveillance. This may provide a partial explanation for why several of these mass surveillance programmes appear to date from around the same time period (mid-late 2000s).

Disentangling cooperative relationships between different EU and US intelligence services indicates a complex web of multiple, overlapping networks. First among these networks is the above-mentioned 'Five Eyes' (composed of the US, UK, Canada, Australia and New Zealand) that originated from a 1946 multilateral agreement for cooperation in signals intelligence,[49] and which has extended over time in terms of activities (Echelon, and now Fornsat) and in terms of privileged partners. Sweden is one of these new partners which, according to Duncan Campbell, now permits Five Eyes to gain access to fibre optic-cables from the Baltic states and Russia.[50] In addition, the US also engages in cooperative relationships with 'second' and 'third-tier' partners such as France and Germany.[51] They engage with these partners in more ad hoc collaborations, but also offensive espionage, as reflected in the recent disclosures from the NSA whistleblower Edward Snowden published in *Le Monde* suggesting that the NSA had been intercepting French phone traffic on "a massive scale".[52] The latter revelation provides an illustration of dual networks between intelligence services – one collaborative and one aggressive – and raises the question of whether the EU member state government concerned (in this case, France) has full oversight and awareness of what the various transnational intelligence networks in which its services participate are doing. Overall, the picture emerges of a US that effectively dominates the diplomacy of surveillance, in ways that disrupt the cohesion of the EU in the security field.

---

[46] For instance, US Director of National Intelligence, Washington, D.C., 8 June 2013: Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act.

[47] See Annex 1 (sections 3 and 4).

[48] See Annex 1 (section 2).

[49] This agreement, known as the UKUSA Agreement, was declassified in 2010 and is now publicly available on the NSA's website (www.nsa.gov/public_info/declass/ukusa.shtml).

[50] Statement by Duncan Campbell at the European Parliament's LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, 1st Hearing, 5 September 2013.

[51] Ibid.

[52] Le Monde reported that more than 70 million French phone calls had been recorded in one 30-day period in late 2012. See J. Follorou and G. Greenwald, "France in the NSA's crosshair: phone networks under surveillance", *Le Monde*, 21 October 2013.

2.6 Legal regimes and oversight

The legal regulation of communications surveillance differs across the five EU member states examined, and there is significant variation as regards the strength of oversight to which intelligence agencies are subject when they intercept telecommunications data.

Some legal regimes operate on the basis of orders issued by special courts (Sweden), others on the basis of warrants issued by the government (the UK and the Netherlands) or by an authorising role accorded to specially appointed oversight bodies (Germany, France and the Netherlands). However, as in the US where the loopholes of the existing regulations were denounced prior to the PRISM scandal, there is often a lack of legal clarity in member states' legislative frameworks where collection of mass internet data is concerned. Thus for instance, the UK Parliament's Intelligence and Security Committee concluded following an investigation into GCHQ activities under the PRISM programme that while "GCHQ has not circumvented or attempted to circumvent UK law, it is proper to consider further whether the current statutory framework governing access to private communications remains adequate". In particular the Committee underlines that "in some areas the legislation is expressed in general terms".[53]

The implementation of programmes for interception via 'up-streaming' by EU member states indicates that law-making has not kept pace with the technological developments seen in surveillance practices in recent years, often designed for traditional intelligence techniques such as wiretapping, rather than the mass 'dragnet' approach that appears to be increasingly adopted by US and EU intelligence agencies. Thus in France, a senior representative of the intelligence services is reported to claim that the collection of meta-data by the DGSE is not illegal but a-legal, conducted outside the law.[54] Further, the lower levels of legal protection accorded to the collection of metadata in certain member states (e.g. the UK and Sweden) does not take into account that this information can nevertheless be extremely revealing about individuals' lives. The exception here is the Netherlands, where the current legislative framework does not permit the Dutch intelligence services to wiretap "cable-bound communications" under any circumstance.[55] However, a modification to the law is expected in order to allow the establishment and activities of the JSCU.[56]

As discussed above, the legislative frameworks of the UK, Sweden and Germany restrict the warrantless collection of data where it concerns internal communications between residents of those member states, echoing the US restrictions on intercepting data between US citizens under FISA. However, evidence revealing data exchange between Western intelligence services raises a number of questions as to whether intelligence agencies share data in order to plug the gaps or circumvent the legal frameworks/safeguards intended to protect the rights of individuals in their national jurisdictions. This would point to a potential scenario of privacy shopping by services to exploit regimes with the weakest protection/oversight or with the greatest legal loopholes. Such a scenario is to some extent reflected in reports indicating that GCHQ marketed itself to the NSA on the basis of the UK's weak regulatory and oversight regime.[57]

As regards oversight, in several member states, oversight bodies are faced with constraints that hamper their ability to apply sufficient scrutiny to intelligence agencies' surveillance practices. In Sweden, the two main oversight institutions, the intelligence court (UNDOM) and the Inspection for Defence Intelligence Operations (SIUN), are deemed to be insufficiently independent.[58] In France the main oversight body, the CNCIS, is found to be substantially constrained in its reach due to its limited administrative capacity.[59] There are gaps also in the UK's intelligence oversight regime, as evidenced by the statement released in July by the

---

[53] Intelligence and Security Committee of Parliament, Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme, 17 July 2013 (http://isc.independent.gov.uk/files/20130717_ISC_statement_GCHQ.pdf).

[54] Statement by Jacques Follorou at the European Parliament's LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, 1st Hearing, 5 September 2013.

[55] See Annex 1, section 5.

[56] Ibid.

[57] N. Hopkins and S. Ackermann, "Flexible laws and weak oversight give GCHQ room for manoeuvre", *The Guardian*, 2 August 2013.

[58] See Annex 1 (section 2).

[59] See Annex 1 (section 3).

ISC on GCHQ's alleged interception of communications under the PRISM programme. The Committee, chaired by former Foreign Secretary Sir Malcolm Rifkind, took detailed evidence from GCHQ for its investigation, including a list of counter-terrorist operations for which the UK was able to obtain intelligence from the US, and found that GCHQ had acted within the law. The statement[60] however remains quite vague on what information it gained access to. Moreover, it indicates that the members of the committee had no prior knowledge of GCHQ's activities in the PRISM programme.

Finally, in terms of oversight, it is worth considering the oversight mechanisms potentially built in to systems and databases used to process and search data collected. The only indication in this regard concerns the GCHQ's Tempora Programme, which requires that in order to target an individual's data via a 'selector' – the operative will have to type into a box on his or her computer screen a Miranda number, to show that the process is taking place in response to a specific request for information, and will also need to select a justification under the Human Rights Act from a drop-down menu.[61] However, without further information (e.g. how detailed these justifications are), it is difficult to judge to what degree these mechanisms represent an administrative 'tick-box exercise' or whether they operate as a genuine safeguard. In any case they cannot substitute for a strong institutional oversight framework, which currently appears lacking in the member states examined here.

[60] Intelligence and Security Committee of Parliament, Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme, op. cit.

[61] J. Lancaster, "The Snowden files: why the British public should be worried about GCHQ", *The Guardian*, 3 October 2013.

3. Legal modalities of action at EU level and compatibility with EU law

KEY FINDINGS

- Surveillance programmes in EU member states are incompatible with minimum democratic rule of law standards derived from the EU Charter of Fundamental Rights and the European Convention of Human Rights, and are in turn essential components of their national constitutional traditions.
- European fundamental rights commitments, enshrined and developed in the case law of the ECtHR and the CJEU, constitute key standards of the concept of national security in EU law to be used in reviewing evolving secretive surveillance practices.
- The member states' surveillance programmes equally jeopardise the EU principle of 'sincere cooperation', enshrined in Article 4.3 of the Treaty on the European Union, as they compromise: first, the compliance with existing EU-level mutual assistance and cooperation legal regimes and lawful searches between EU member states and with the US; second, the coherency in the EU's external relations with the US and other third countries; and third, the internal security of the Union as a whole. They also jeopardise the privacy of EU nationals as data owners.
- Large-scale electronic surveillance blurs the line between national sovereignty and matters relating to EU competence as it potentially spills over into the security activities of the EU institutions and their agencies. More precisely, EU liability may be invoked where EU agencies become implicated in sharing and exploiting data generated by national surveillance operations.
- The boundary between domestic and foreign interception is blurred by data exchange between intelligence services. At the same time, member states' domestic legal regimes that distinguish between the guarantees applied to national citizens and those of other EU citizens may raise questions of discrimination.

Under European law, the individual has ownership of his data (unlike the US where ownership belongs to the company or service that assembled the data). This principle is central and protected by the EU Charter and the Treaty. Therefore, it can be contended that transnational programmes linking NSA with a series of European intelligence services and facilitating data exchange, could potentially be considered as a 'theft' (of correspondence) on top of the potentially illegal access, collection and processing of data, if this has been done without the authorisation and/or knowledge of the national authorities in charge of the management of these electronic data. Only the latter may authorise derogations of national security with respect to existing bilateral, European and international agreements.

A legal framework of the EU-US Mutual Legal Assistance Agreement (MLAA) has been ratified by the Union and the US Congress to permit collaboration in criminal investigations and counter-terrorism activities in search of evidence for law-enforcement purposes. It stipulates the modalities for gathering and exchanging information, and for requesting and providing assistance in obtaining evidence located in one country to assist in criminal investigations or proceedings in another.[62] The channels permitting lawful search are therefore organised (and, it should be noted, critiqued by NGOs and journalists for accepting too readily the logic of the global counter-terrorism initiated by the US and its limitations to privacy). But it is not clear from the revelations of the activities conducted by the NSA that the US services and their European member state partners have followed the rules of this agreement. The evidence indicates, in fact, they have bypassed or ignored these channels in favour of covert cooperation that goes beyond counter-terrorism collaboration and serves a multitude of other purposes. The journalist John Lanchester, who is one of the rare persons to have read the GCHQ files whose UK copy The Guardian was forced to destroy, expresses clearly what is at stake. Certainly democratic states need intelligence services, open societies have enemies, and tools of electronic surveillance are useful against them. It is for this reason that the right to privacy needs to

[62] Agreement on Mutual Legal Assistance between the European Union and the United States of America, OJ L 181/34, 19 July 2003.

be qualified in the interest of security, but the question arises when the technologies give the possibility of mass capture of data and that they are used for strategic surveillance, as in that case security without limits may put democracy at risk.[63]

The relationship between communications surveillance programmes and EU competences remains a contested one. Intelligence activities are said to remain within the scope of member states' exclusive competences in the EU legal system.[64] Yet, are member states' large-scale surveillance programmes outside the remit of EU intervention? This section develops three main legal modalities of action to assess and critically examine EU mass-surveillance programmes from an EU law viewpoint: i) the concept of national security in a democratic rule of law framework (section 3.1); ii) the insecurity of the Union and its citizens (section 3.2); and iii) the activities of home affairs agencies (section 3.3).

3.1 National security and democratic rule of law

There are strong tensions between large-scale surveillance programmes implemented by some EU member states and EU founding commitments, principles and legal obligations, as outlined in Article 2 TEU. This provision identifies a set of principles deemed to be common to all EU member states and which include, amongst others, respect of democracy, rule of law and human rights. It is argued that EU surveillance programmes are incompatible with minimum democratic rule of law standards, which are in turn central components of national constitutional traditions. This argument is premised on an understanding of rule of law as the legally-based rule of a democratic state, which delivers fundamental rights. O'Donnell has argued that the rule of law should not only be understood as a generic characteristic of the legal system and the performance of the courts, but also as the legally-based rule of a democratic state, which delivers fundamental rights (and limits the use of discretion or 'exceptionalism') by state authorities.[65] According to the 'democratic rule of law', the legal system needs to be in itself democratic and there must be mechanisms of accountability and supervision by an independent judiciary at the heart of the system.

The notion of 'national security' as framed and understood by some intelligence communities and certain national governments in PRISM-like EU programmes does not correspond to the democratic understanding of national security as foreseen in member states' constitutional systems, where a key element of constitutionality remains in the effective judicial control and supervision of executive or governmental actions, including those circumscribed under the boundaries of the State's national security.[66]

---

[63] John Lanchester, "The Snowden files: why the British public should be worried about GCHQ", *The Guardian*, 3 October 2013 (http://bit.ly/17oYoB8).

[64] This is founded in Article 4.2 Treaty on European Union (TEU) which emphasises:

> The Union shall respect…their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order, and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.

In the same vein, Article 72 of the Treaty on the Functioning of the European Union (TFEU) stipulates that

> This Title shall not affect the exercise of the responsibilities incumbent upon Member States within regard to the maintenance of law and order and the safeguarding of internal security.

[65] G. O'Donnell (2004), "The Quality of Democracy: Why the Rule of Law Matters?", *Journal of Democracy*, Vol. 15, No. 4, October.

[66] Refer for instance the Case *Binyam Mohamed v. The Secretary of State for Foreign and Commonwealth Affairs*, 10.2.2010, where the England and Wales Court of Appeal ruled that (Paragraphs 132 and 133):

> The ultimate decision whether to include the redacted paragraphs into the open version of the first judgment is a matter for judicial, not executive, determination (...) it is ultimately for a judge, not a minister to decide whether a document must be disclosed, and whether it can be referred to, in open court. That decision is for a judge, not a minister, not least because it concerns what goes on in court, and because a judge is better able to carry out the balancing exercise (...) Furthermore, practically any decision of the executive is subject to judicial review, and it would seem to follow that a minister's opinion that a document should not be disclosed in the national interest is, in principle, reviewable by a court. (...) What is included in, or excluded from, a judgment is self-evidently a matter for a judge, not a minister. *It is another aspect of the separation of powers that the executive cannot determine whether certain material is included in, or excluded from, the open material in a judgment.* That must be a decision for the judge giving the judgment in issue, subject of course to the supervisory jurisdiction of any competent appellate court. (Emphasis added).

National constitutional traditions not only formally foresee the democratic and rule of law foundations of the state, where 'the arbitrary' is carefully limited (so there exists an adequate level of protection against abuse of power) and must be read from the perspective of the separation of powers principle. Government and law enforcement are in this way under scrutiny of the judiciary and open justice. Member states' constitutions now also feature European fundamental human rights commitments and standards emerging from the European Convention of Human Rights and the EU Charter of Fundamental Rights. These bring the jurisprudence and transnational supervision from the Strasbourg Court (section 3.1.1) and the Court of Justice of the European Union (section 3.1.2) at the core of the evolving national practices and concepts of 'national security'.

3.1.1 National Security and the ECHR

There is a significant body of jurisprudence by the European Court of Human Rights (ECtHR) on what constitutes interference "*prescribed by law*" in the context of secret surveillance and information gathering. The judge-made requirements of "*in accordance to the law*" and "*necessary in a democratic society*" have consolidated themselves as key testing standards in determining the lawfulness and proportionality of government's interferences with fundamental human rights, such as those foreseen in Article 8 of the European Convention of Human Rights (ECHR), which lays down the right to respect for family and private life.

A key issue of contestation before Strasbourg has been the extent to which national governments' justifications to interfere with ECHR rights have been "in accordance with the law" or "prescribed by the law", pursue a legitimate aim and are necessary in a democratic society. In its landmark judgment *Weber and Saravia v. Germany* of 2006,[67] the Court examined the legality of the extension of the powers of the German Federal Intelligence Service with regard to the recording of telecommunications in the course of so-called 'strategic monitoring',[68] as well as the use of personal data obtained and its transmission to other authorities. The Court dismissed the applicants' complaints under Article 8 ECHR on the basis that the German legislation[69] provided adequate and effective guarantees against abuses of the State's strategic monitoring powers, and the interference with the secrecy of telecommunications was necessary in a democratic society in the interests of national security and for the prevention of crime.

However, the Court established in the *Weber* case a set of criteria for determining the lawfulness of secret surveillance and interference of communications and to avoid 'abuse of powers' and arbitrariness. The Court underlined that the risks of arbitrariness are particularly evident in those cases where a power vested in the executive is exercised in secret, and held:

> It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated... The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures...[70]

In particular, the following minimum safeguards were highlighted, which should be set out in statute law in order to avoid abuses of power: first, the nature of the offences which may give rise to an interception order; second, a definition of the categories of people liable to have their telephones tapped; third, a limit on the duration of telephone tapping; fourth, the procedure to be followed for examining, using and storing the data obtained; fifth, the precautions to be taken when communicating the data to other parties; and sixth, the

---

See also German Federal Constitutional Court, Press Release No. 31/2013, 24 April 2013, Counter-Terrorism Database in its Fundamental structures compatible with the Basic Law, but not regarding specific aspects of its design.

[67] *Weber and Saravia v. Germany*, No. 54934/00, 29 June 2006, § 80. See also Association for European Integration and Human Rights and Ekimzhiev, cited above, §§ 75-77.

[68] "Strategic monitoring is aimed at collecting information by intercepting telecommunications in order to identify and avert serious dangers facing the Federal Republic of Germany, such as an armed attack on its territory or the commission of international terrorist attacks and certain other serious offences." See § 4 and paragraphs 18 et seq. of the judgement.

[69] *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*), also called "the G 10 Act", as modified by the Fight against Crime Act of 28 October 1994 (*Verbrechensbekämpfungsgesetz)*.

[70] Weber and Saravia v. Germany, op. cit. §93.

circumstances in which recordings may or must be erased or the tapes destroyed.[71] In this respect, the ECtHR added:

> … *it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power.* Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.[72] (Emphasis added)

The ECtHR found the UK's secret interception of communications to be in violation of Article 8 of the ECHR in the case *Liberty v. UK*.[73] In contrast with the situation addressed in Weber, the Court considered that UK domestic law did not provide sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. It therefore found the UK to be in violation of Article 8 and that the interference with the applicants' rights was not "in accordance with the law".

The ECtHR paid especial attention to the requirement of foreseeability, i.e. the extent to which UK domestic law was adequately accessible and formulated with sufficient precision as to be foreseeable. The authorities' conduct was not "in accordance with the law" because it was unsupported by any predictable legal basis satisfying the accessibility principle.[74] The ECtHR stated that "The expression "in accordance with the law" under Article 8 § 2 requires, first, that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be compatible with the rule of law and accessible to the person concerned, who must, moreover, be able to foresee its consequences for him" [75] The ECtHR noted the Government's concern that "the publication of information regarding the arrangements made by the Secretary of State for the examination, use, storage, communication and destruction of intercepted material during the period in question might have damaged the efficacy of the intelligence-gathering system or given rise to a security risk". Nevertheless, it stated:

> …the German authorities considered it safe to include in the G10 Act, as examined in Weber …, express provisions about the treatment of material derived from strategic interception as applied to non-German telephone connections. In particular, the G10 Act stated that the Federal Intelligence Service was authorised to carry out monitoring of communications *only with the aid of search terms which served, and were suitable for, the investigation of the dangers described in the monitoring order and which search terms had to be listed in the monitoring order*. Moreover, *the rules on storing and destroying data obtained through strategic monitoring were set out in detail in section 3(6) and (7) and section 7(4) of the amended G10 Act*. … The G10 Act further set out *detailed provisions governing the transmission, retention and use of data obtained through the interception of external communications*.[76] (Emphasis added).

In *Kennedy v. UK*[77] the ECtHR further examined the extent to which the secret interception of communications by the UK security services was in accordance with the law and necessary in a democratic society. The Court acknowledged that the Contracting States enjoy *a certain margin of appreciation* in assessing the existence and extent of such necessity, but stressed that this margin is nonetheless subject to European supervision. It also pointed out that "the values of a democratic society must be followed as

---

[71] § 95.

[72] § 94.

[73] *Liberty and Others v. the United Kingdom*, No. 58243/00, 1/10/2008.

[74] § 56 of Liberty v. UK.

[75] The Court recalled its findings in previous cases (see *Weber and Saravia v. Germany* (dec.), No. 54934/00, 29 June 2006, § 78) "that the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them", § 59. See, among other authorities, Kruslin v. France, judgment of 24 April 1990, Series A No. 176-A, § 27; Huvig v. France, judgment of 24 April 1990, Series A No. 176-B, § 26; Lambert v. France, judgment of 24 August 1998, Reports of Judgments and Decisions 1998-V, § 23; Perry v. the United Kingdom, No. 63737/00, § 45, ECHR 2003-IX; Dumitru Popescu v. Romania (No. 2), No. 71525/01, § 61, 26 April 2007.

[76] § 68 of Liberty v. UK.

[77] *Kennedy v. the United Kingdom*, No. 26839/05, 18.8.2010.

faithfully as possible in the supervisory procedures, if the bounds of necessity are not to be exceeded".[78] It also stated that in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it was in principle desirable to entrust supervisory control to a judge,[79] and that sufficient detail should be provided of the nature of the offences in question.[80]

In contrast to the *Liberty and Others* case, which concerned the legislation on interception of communications between the United Kingdom and any other country (external communications), *Kennedy* concerned 'internal communications' which comprise communications within the UK. The Court recalled that under UK law "Indiscriminate capturing of vast amounts of communications is not permitted under the internal communications provisions of RIPA".[81] The ECtHR restated the three criteria according to which an interference with an ECHR right may be justified and legitimate: First, the impugned measure must have some basis in domestic law. Second, the domestic law must be compatible with the rule of law and accessible to the person concerned. Third, the person affected must be able to foresee the consequences of the domestic law for him.[82] The ECtHR also insisted that powers to instruct secret surveillance of citizens are only tolerated under Article 8 "to the extent that they are strictly necessary for safeguarding democratic institutions", which in practice means that

> … there must be *adequate and effective guarantees against abuse*. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law.[83] (Emphasis added).

The Court has repeatedly stressed in its case law the importance of giving a narrow interpretation to exceptions to basic fundamental human rights envisaged in the ECHR, in particular to protect the individual against any abuse of power and in what concerns human rights where no exceptions are allowed (absolute in nature). Cases related to the so-called 'extraordinary renditions and secret detentions' have been illustrative in this regard and have developed democratic rule-of-law standards, which establish the boundaries of lawfulness of secret intelligence activities in a democratic society. As a way of illustration, the Court ruled in *El-Masri v. Macedonia* that an essential object of Article 8 ECHR "is to protect the individual against arbitrary interference by the public authorities" and that the interference must be "in accordance with the law".[84] In respect of the violation of Article 5 ECHR (right to liberty and security), the Court held:

> Although the investigation of terrorist offences undoubtedly presents the authorities with special problems, that *does not mean that the authorities have carte blanche* under Article 5 to arrest suspects and detain them in police custody, *free from effective control by the domestic courts and, in the final instance, by the Convention's supervisory institutions*, whenever they consider that there has been a terrorist offence.[85] (Emphasis added).

In *Nada v. Switzerland* of 2012,[86] the ECtHR dealt with the review of the sanctions regime established by Security Council Resolution 1267 (1999) to freeze the funds and other financial resources of the individuals and entities identified by the Security Council's Sanctions Committee as being associated with Osama bin Laden, al-Qaeda or the Taliban, and the human rights consequences of the inability of the listed persons to challenge effectively the decision to list them. The Court held that an interference with ECHR rights could be considered "necessary in a democratic society" for a legitimate aim "if it answers a "pressing social need" and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are "relevant and sufficient".[87] It added that for a measure to be regarded as

---

[78] § 154. See also *Kvasnica v. Slovakia*, No. 72094/01, § 80, 9 June 2009.

[79] § 167. See *Klass and Others*, § 56.

[80] § 159.

[81] Liberty and Others, § 64.

[82] See for instance *Rotaru v. Romania*, § 52; *Liberty and Others*, § 59; and *Iordachi and Others*, § 37.

[83] See § 153. *Klass and Others*, cited above, §§ 49 to 50; and *Weber and Saravia*, cited above, § 106.

[84] El-Masri v. Macedonia, No. 39630/09, 13 December 2012.

[85] El-Masri v. Macedonia, op. cit., § 232.

[86] Nada v. Switzerland, No. 10593/08, 12 September 2012.

[87] § 180. See also S. and Marper, cited above, § 101, and Coster v. the United Kingdom [GC], No. 24876/94, § 104, 18 January 2001.

proportionate and as necessary in a democratic society, there must be the possibility of recourse to an alternative measure that would cause less damage to the fundamental right at issue whilst fulfilling the same aim. Moreover, the ECtHR reiterated that in any event the final evaluation of whether the interference is necessary remains subject to review by the Court for conformity with the requirements of the Convention.[88]

3.1.2 National security and the EU Charter of Fundamental Rights

A second legal modality of action when assessing EU large-scale surveillance programmes in EU member states is their relationship with the EU Charter of Fundamental Rights. The EU Charter has been recognised as having the same legal value as the Treaties since the entry into force of the Lisbon Treaty. The EU Charter comes along a set of EU general principles some of which find their origins in national constitutional traditions and others have been further developed by the CJEU jurisprudence. The national constitutional traditions of EU member states illustrate a progressive 'process of constitutionalisation' of the EU Charter in their domestic legal systems. This has been confirmed by the European Commission's 2012 Annual Report on the Application of the EU Charter,[89] which covered an assessment of the member states' frameworks of judicial reviews of 'constitutionality', and which concluded:

> The analysis of court rulings referring to the Charter further suggests that national judges *use the Charter to support their reasoning, including when there is not necessarily a link with EU law*. There is also some evidence of an incorporation of the Charter *in the national systems of fundamental rights protection*.[90] (Emphasis added)

The CJEU pointed out in *Fransson*[91] that "outside the scope of EU law" national authorities and courts remain free to apply national standards of protection of fundamental rights, provided that the level of protection offered by the Charter, as interpreted by the Court, and the primacy, unity and effectiveness of European law are not compromised. The CJEU has in this way held that the EU Charter is becoming a constitutive component of "the national constitutional traditions" of EU member states. As Vice-President of the European Commission Viviene Reding has stated:[92]

> The concept of national security does not mean that "*anything goes*": States do not enjoy an unlimited right of secret surveillance. In Europe, also in cases involving national security, every individual – irrespective of their nationality – can go to a Court, national or European, if they believe that their right to data protection has been infringed. *Effective judicial redress is available for Europeans and non-Europeans alike*. *This is a basic principle of European law*. (Emphasis added).

---

[88] § 184. However,

> A margin of appreciation must be left to the competent national authorities in this connection. The breadth of this margin varies and depends on a number of factors including the nature of the Convention right in issue, its importance for the individual, the nature of the interference and the object pursued by the interference (see S. and Marper, § 102).

The Court concluded:

> the restrictions imposed on the applicant's freedom of movement for a considerable period of time did not strike a fair balance between his right to the protection of his private and family life, on the one hand, and the legitimate aims of the prevention of crime and the protection of Switzerland's national security and public safety, on the other. Consequently, the interference with his right to respect for private and family life was not proportionate and therefore not necessary in a democratic society. § 198.

[89] European Commission, 2012 Annual Report on the Application of the EU Charter of Fundamental Rights, 2013, European Commission, DG for Justice (http://ec.europa.eu/justice/fundamental-rights/files/charter_report_2012_en.pdf).

[90] Ibid., p. 15. Reference was in particular made to the Austrian Constitutional Court, Cases U 466/11 and U 1836/11, 14.3.2012, where according to the European Commission, the Constitutional Court

> … recognised the very special role of the Charter within the EU legal system, and its different nature compared to the body of rights and principles which the Court of Justice of the EU has been developing throughout the years. It took the view that the Charter is enforceable in the proceedings brought before it for the judicial review of national legislation, and therefore individuals can rely upon the rights and the principles recognised in the Charter when challenging the lawfulness of domestic legislation. The Austrian Constitutional Court identified strong similarities between the role played by the Charter in the EU legal system and that played by the ECHR under the Austrian Constitution, according to which the ECHR has force of constitutional law.

[91] Case C-617/10, *Fransson*, 26 February 2013.

[92] V. Reding, "PRISM scandal: The data protection rights of EU citizens are non-negotiable", Press Conference, EU-U.S. Justice and Home Affairs Ministerial, Dublin, 14 June 2013.

In the same vein, Reding reiterated the relevance of the EU Charter presentation on 19 June 2013 at the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament.[93] During the question and answer period, and following questions from MEPs referring to the lack of EU competence over intelligence services activities, Reding stated:

> … "intelligence" of course is not in our remit, but … even in questions of intelligence the fundamental rights which are inscribed in our basic text are not eliminated but they are also to be considered. So the position of the European Commission and the defence of the fundamental rights of the citizens is without any doubt in that respect. (Emphasis added).

The relevance of effective and open justice was underlined by the CJEU in the case *ZZ v. Secretary of the State of Home Department* C-300/11, of 4 June 2013, which confirmed that the provision of effective judicial review is a central component even within the scope of member states' measures adopted on the basis of 'State security'.[94] The CJEU was of the opinion that "although it is for Member States to take the appropriate measures to ensure their internal and external security, the mere fact that a decision concerns State security cannot result in European Union law being inapplicable".[95] It added that in those circumstances where a national authority opposes precise and full disclosure to the person concerned of the grounds constituting a decision refusing entry in a member state for reasons of State security,[96] member states are required to

> … first, to provide for effective judicial review both of the existence and validity of the reasons invoked by the national authority with regard to State security and of the legality of the decision taken under Article 27 of Directive 2004/38 and, second, to prescribe techniques and rules relating to that review, as referred to in the preceding paragraph of the present judgment.[97]

The CJEU concluded that the contested regulations, which did not provide for any remedy in respect of the freezing of assets, were in breach of fundamental rights and were to be annulled. Here also, the relevance of effective judicial review and scrutiny was identified as a central component of an EU understanding of rule of law. The Luxembourg Court held that such review should be seen as a "*constitutional guarantee*" forming part of the very foundations of the Community and added:

> … *the Community is based on the rule of law*, inasmuch as neither its Member States nor its institutions *can avoid review of the conformity of their acts with the basic constitutional charter, the EC Treaty*, which established a complete system of legal remedies and procedures designed to enable the Court of Justice to review the legality of acts of the institutions.[98] (Emphasis added).

3.2 Whose security? Sincere cooperation and citizens' liberties compromised

The legal tensions between large-scale surveillance and democratic rule of law with fundamental rights endanger the security of the Union and that of its citizens, and unleash insecurity for the Union as a whole. The intelligence communities' understandings and practices of national security and member states' surveillance programmes equally jeopardise the EU principle of 'sincere cooperation', as they make it more

---

[93] See www.europarl.europa.eu/news/en/news-room/content/20130617IPR12352/html/PRISM-EU-citizens'-data-must-be-properly-protected-against-US-surveillance.

[94] See also the Kadi Judgement on judicial supervision (http://curia.europa.eu/juris/document/document.jsf?text=&docid=139745&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=205883) Paragraphs 326 and 327.

[95] See Case C-387/05 Commission v Italy [2009] ECR I-11831, paragraph 45.

[96] Paragraph 57 states:

> However, if, in exceptional cases, a national authority opposes precise and full disclosure to the person concerned of the grounds which constitute the basis of a decision taken under Article 27 of Directive 2004/38, by invoking reasons of State security, the court with jurisdiction in the Member State concerned must have at its disposal and apply techniques and rules of procedural law which accommodate, on the one hand, legitimate State security considerations regarding the nature and sources of the information taken into account in the adoption of such a decision and, on the other hand, the need to ensure sufficient compliance with the person's procedural rights, such as the right to be heard and the adversarial principle.

[97] Paragraph 58. See also paragraphs 65 and 66.

[98] Paragraph 281. Case 294/83 Les Verts v Parliament [1986] ECR 1339, paragraph 23.

difficult to carry out the tasks flowing from the Treaties and put at risk the attainment of the Union's objectives, including those in external relations and the common foreign and security policy.[99]

The violations of democratic rule of law and fundamental rights inherent to large-scale surveillance, and their supranational nature and fundamentals, affect the security of the Union as a whole. They also jeopardise the use of legally established channels at EU level, some of which have been concluded with the US. As Reding said in the above-mentioned intervention in the EP LIBE Committee in June 2013, "if you don't go through the MLA and directly to companies asking data of EU citizens that is a violation of international law (Recital 90 of Regulation)".

According to a Council of the EU Discussion Paper on COSI and terrorism:

> Regardless of this [i.e. Article 4.2 TEU], the transnational nature of terrorism and its perpetrators makes it a clear threat also *to the common internal security of the Union*. It is therefore important that the work against terrorism, at least *when it affects the EU as a whole*, is coordinated so that it can be conducted efficiently and focused on common identified and prioritised threats. [100] (Emphasis added).

A similar argument could be used in light of the nature of some of the EU large-scale surveillance programmes operating in a number of member states. Just as 'acts of political violence' are said to be increasingly supranational, so the process of 'intelligence gathering' is supranational as well, coming from a variety of sources abroad or 'at home'. Its supranational nature and implications make the national security as framed and understood by certain actors in the 'intelligence communities' not only in tension with the security of that state based on democratic rule of law, but also that of the other member states and the Union as a whole.

Large-scale EU surveillance programmes also compromise the security and fundamental human rights of citizens and residents in the Union, in particular those related to privacy and effective legal protection. The involvement of certain EU member states in NSA programmes deprive EU citizens of their ownership of their personal and private data, and subject them to discriminatory treatment, i.e. nationals of other EU member states are subject to a disproportionately larger impact of large-scale surveillance programmes, as they are unjustifiably less-favourably treated than nationals as privacy holders in interceptions of 'internal communications'. For example, Privacy International has argued that the UK Tempora programme involves unjustified discrimination against non-UK nationals and EU citizens. In its submission, Privacy International highlighted:

> Further, the operation is in breach of Article 12(1) TFEU. The Tempora operation has a disparate adverse impact on EU citizens who are not nationals of the United Kingdom. This is because a certification under section 8(4) of RIPA 2000 can only be granted in respect of the interception of external communications, which are more likely to be made by non-UK citizens. Union citizens who are not UK citizens are far more likely to have their communications intercepted, searched and retained. Both UK citizens and non-UK citizens pose risks to national security. Accordingly, such differences in treatment are not justifiable

---

[99] Refer to Article 4.3 TEU which states:

> Pursuant to the principle of sincere cooperation, the Union and the Member States shall, in full mutual respect, assist each other in carrying out tasks which flow from the Treaties. The Member States shall take any appropriate measure, general or particular, to ensure fulfilment of the obligations arising out of the Treaties or resulting from the acts of the institutions of the Union. The Member States shall facilitate the achievement of the Union's tasks and refrain from any measure which could jeopardise the attainment of the Union's objectives.

See also Article 24.3 TFEU which stipulates:

> The Member States shall support the Union's external and security policy actively and unreservedly in a spirit of loyalty and mutual solidarity and shall comply with the Union's action in this area. The Member States shall work together to enhance and develop their mutual political solidarity. They shall refrain from any action which is contrary to the interests of the Union or likely to impair its effectiveness as a cohesive force in international relations.

[100] Council of the EU (2013), Discussion Paper on COSI and Terrorism, 10162/13, Brussels, 3 June 2013, p. 3. See also Council of the EU, Standing Committee on Operational Cooperation on Internal Security (COSI), Summary of Discussions, 11265/13, Brussels, 24 June 2013, p. 5, where it states:

> The Swedish discussion paper on the COSI competences and tasks with regard to terrorism (doc. 10612/12) was welcomed by various delegations. Several delegations suggested having a wider debate at some stage on whether COSI is fulfilling its mandate and where it could provide added value, including in the context of the Council's JHA structures (CATS, SCIFA). Delegations felt that COSI could address the topic of terrorism but with due respect to the provisions of the Treaty and Member States' competences. Delegations also highlighted that duplication of efforts with other working parties such as the Terrorism Working Party and COTER should be avoided.

> or lawful. A systematic scheme of processing of personal data primarily directed at non-UK nationals cannot be justified under EU law.[101]

There is also a fundamental gap in the current EU legal framework that increases the vulnerability of citizens' privacy-related rights and liberties, as additionally alleged by Privacy International in its complaint before the Strasbourg Court of July 2013.[102] It highlighted in particular that those differences between foreign and domestic interception and information-gathering regimes lead to an absence of legal protection when information is shared between countries.

PRISM-like surveillance programmes challenge this premise (a central distinction has been made between foreign and domestic interception and secret information-gathering regimes) and reveal a gap in protection and accountability in the EU. Are the distinctions between internal and external communications still relevant in warrant schemes for interceptions in the legal systems of EU member states?[103]

3.3 Home affairs agencies

Another means by which large-scale surveillance practices blur the lines between national sovereignty and matters relating to EU competence is their potential spillover into the security activities of the EU institutions and its agencies. More precisely, EU liability may be invoked where the EU's institutions and its agencies become implicated in sharing and exploiting data generated by national large-scale surveillance operations.

This is particularly relevant as regards the activities of EU Home Affairs agencies which play a central role in putting into practice the "comprehensive model for information exchange" which resides at the heart of the EU's Internal Security Strategy.[104] Europol and INTCEN (and to a lesser extent Eurojust, Frontex and OLAF) are key actors at the forefront of gathering, exchange and processing of information, often based on consolidated versions of reporting and contributions from member states' national security and intelligence agencies.

Europol for instance relies to a large degree on the input of member states' intelligence services for its strategic analysis products, such as the annual EU Terrorism and Situation and Trend Reports (TE-SAT).[105] Similarly the EU Intelligence Analysis Centre (INTCEN) within the European External Action Service

---

[101] Privacy International submission to the Investigatory Powers Tribunal, "Statement of Grounds", 8 July 2013, paragraph 57 (www.privacyinternational.org). Reference was here made to the Case C-524/06 *Huber v Germany* [2008] ECR I-9705 at [69-81].

[102] In this context, Privacy International argued as follows:

> With communication being increasingly global, and vast amounts of personal data being transferred and stored around the world, there is an obvious gap in legal protection to ensure respect for private life. The regimes in both the US and the UK governing the interception, obtaining, and storing of material deal differently with foreign and domestic interception and information gathering (in the UK the difference depends on whether communication is regarded as "internal" or "external" and in the US on whether or not the person targeted is a non-US citizen located outside the US). Those differences between foreign and domestic interception and information gathering regimes lead to an absence of legal protection when information is shared between countries. UK authorities can intercept communications sent or received by individuals located in the US (and which will be regarded as "external" for the purposes of RIPA), which happen to pass through UK fibre cables, and hand them over to US authorities, thus avoiding the US rules governing interception of those located within the country. The NSA can intercept an email under FISA section 1881a which is sent between two individuals in London because it happens to travel through the US as it will be regarded as "foreign intelligence material" as far as the US authorities are concerned, and it can then be handed over to the UK authorities without their having to comply with any of the requirements governing interception set out in RIPA and the Code of Practice. The same is true of private information about UK residents stored by internet companies in the US. Ibid., paragraph 45.

[103] In *Liberty vs. UK*, it was argued:

> 14. The IPT found that the difference between the warrant schemes for interception of internal and external communications was justifiable, because it was more necessary for additional care to be taken with regard to interference with privacy by a Government in relation to domestic telecommunications, given the substantial potential control it exercised in this field; and also because its knowledge of, and control over, external communications was likely to be much less extensive.

[104] E. Guild and S. Carrera (2011), "Towards an Internal (In)security Strategy for the EU?", CEPS Paper in Liberty and Security in Europe, CEPS, Brussels, January.

[105] See Europol, *TE-SAT 2013 – EU Terrorism Situation and Trend Report.*

(EEAS) acts as "a single entry point in the EU for classified information coming from Member States' civilian intelligence and security services" and on this basis produces intelligence analyses, early warnings and situational awareness for the EEAS, EU decision-making bodies and member states.[106]

The processes surrounding the exchange of intelligence between the member states and EU home affairs agencies like Europol and INTCEN are notoriously opaque.[107] There is no mechanism to verify the nature of data and information transferred to EU level, nor to ensure that the sources and means by which such data are generated are legitimate and in compliance with the national laws of the member state in question and EU fundamental rights standards. Europol Director Rob Wainwright, during the European Parliament Hearing of 24th September 2013, stressed that the EU's law enforcement agency "has no contacts at all with the NSA or CIA".[108] However, he conceded that data dealt with by Europol agents and received directly from the member states may originate from EU intelligence agencies, and even the NSA. The lack of clarity in his response is in keeping with the gaps in oversight that characterise much of the flow of information within the agency: a significant proportion of the data that passes through Europol are understood to be exchanged bilaterally between national liaison officers stationed in Europol, but the agency provides little reassurance as to the trusted nature of Europol's information sources.

There is therefore a strong possibility that tainted information – i.e. data gleaned from unlawful mass surveillance or exchanged without due regard to compliance with fundamental rights, data protection and privacy standards, would enter the AFSJ and be shared and processed at EU level. This possibility should suggest a number of concerns to EU lawmakers. It implies a degree (however limited) of complicity by EU agencies in practices that contradict fundamental EU legal principles and human rights standards. EU agencies could therefore share in any liability resulting from the mis-use of this data.

The liability incurred by EU agencies raises an important side issue about the data handled by these organisational actors and the justification for their access to often sensitive information. As Geyer notes, when considering the risk that EU institutions and agencies have handled intelligence resulting from extraordinary rendition and the torture of terror suspects, information processed at EU level does not serve to avoid 'imminent security threats' but rather serves mid- and long-term policy objectives or – as in the case of Europol and INTCEN – the creation of risk analysis, strategic reports and threat assessments. In this light, the already questionable argumentation brought forward at national level to justify the use of large-scale surveillance techniques, i.e. to counter direct threats to national security, is even less applicable to the access and use of such information at EU level.[109]

Finally, the sharing of intelligence with EU agencies such as Europol further blurs the question of legal competence. Europol is established under Article 88 of the Lisbon Treaty under Chapter V on Police Cooperation, and its legal mandate establishes the agency as a law-enforcement body. However, the sharing of information with Europol by national intelligence services not only potentially compromises the agency's integrity, it also renders indistinguishable the boundaries of what is police cooperation and what is intelligence at EU level. The tendency reflects the merging of police, military and intelligence logics and practices that we've seen at national level in the operation of large-scale surveillance programmes (see section 2) and creates a legal insecurity and uncertainty in the actions of EU agencies. This could partly be addressed during the forthcoming revision of Europol's legal mandate, in order to ensure greater accountability and oversight of this agency's actions. Despite claims as to the necessity of such non-transparency/autonomy as being central to the functioning of EU home affairs agencies, the application of a 'balanced approach' is not applicable in light of the profound implications the activities of these agencies hold for human rights and liberties.

---

[106] EU Intelligence Analysis Centre (EU INTCEN), Factsheet (www.asktheeu.org/en/request/637/response/2416/attach/5/EU%20INTCEN%20Factsheet%20PUBLIC%20120618%201.pdf).

[107] J. Parkin (2012), "EU Home Affairs Agencies and the Construction of EU Internal Security", CEPS Paper in Liberty and Security in Europe, CEPS, Brussels December; and C. Jones (2013), "Secrecy reigns at the EU's Intelligence Analysis Centre", Statewatch Analysis, London.

[108] European Parliament, LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, 23 September 2013.

[109] F. Geyer (2007), "Fruit of the Poisonous Tree - Member States' Indirect Use of Extraordinary Rendition and the EU Counter-Terrorism Strategy", CEPS Working Document No. 263, Centre for European Policy Studies, Brussels, 3 April.

4. Conclusions and recommendations: Implications of large-scale surveillance for freedom, fundamental rights, democracy and sovereignty in the EU

4.1 General conclusions

This paper argues that the various programmes involving practices of large-scale surveillance have to be carefully examined from a fundamental rights perspective. The implications are far-reaching and go beyond the traditional dilemma between the rights of citizens to data protection and the right of the state to depart from the rule of law in the name of national security. They raise questions about the fundamental character of our political regimes and the nature of sovereignty.

Most European services involved in the fight against terrorism and organised crime have used the large-scale collection of metadata as a way to 'connect the dots' between the activities of suspects in criminal investigations. They have used surveillance in order to reconstitute networks of possible suspects associated with their main target, drawing both on real-time and stored data. In this case, even if large-scale collection is taking place, it may be considered as 'targeted surveillance'. Based on warrants and on clear purposes that can be overseen at a later date, it can be justified. This is the kind of surveillance that the legal framework of the EU-US Mutual Legal Assistance Agreement (MLAA) has organised. Even if some lawyers consider that this scope is already a problem for data protection and privacy, this agreement at the very least allows room for negotiation.

However, the case of European services collaborating with the NSA through the different surveillance programmes is markedly different. These collaborations have been kept secret and go beyond the legality of the agreements in place. They may have implied forms of spying activities against European companies in favour of US companies. One can also presume they may have breached the solidarity principle between European countries in favour of other alliances, notably by sending data of other European citizens without the knowledge of their own state to the NSA and its allies of the enlarged 'Five Eyes' network. One can wonder if routine practices have exceeded mere targeted surveillance and whether intelligence services have violated principles of rule of law. The questions remain: How far does this surveillance go? How are the data obtained by such surveillance exploited?

Once extracted, data may be used for multiple purposes either by intelligence services, Internet providers or their subcontractors. Some journalists and observers have pointed out that large-scale surveillance expands the number of persons put on watch lists around the world, with the tendency to consider that the best platform for watch lists is one with the "most people in it", without further considering the quality of the information on which such lists are based. To what extent can these forms of profiling and strategic surveillance be considered as data-mining?

It seems that NSA surveillance programmes resemble the TIA: they are multi-purpose, warrantless and may imply forms of data-mining. They are not just anti-terrorist programmes set up to detect plotters working against the national interests of the United States – despite the US Director of National Intelligence's claim that this was the case.[110] We still do not know if it is the case or not, but if data-mining and predictive analytics are involved, the analysis of the different programmes involving large-scale surveillance cannot be reduced to a question of a balance between security and privacy, nor to a question of asymmetry of sovereignties in diplomatic alliances. It is a question of whether security measures are putting democracy at risk. A first challenge for the future is therefore to discuss the legitimacy of such programmes and to prevent the path leading to data mining.

A second challenge is to assess the efficiency of this type of surveillance. At a very pragmatic level, large-scale surveillance appears to have strong limitations and is certainly not key in crime prevention. Such surveillance creates a double tendency. The first tendency is to collect data extensively and retain them over a long period of time in order to establish trends that facilitate big-data correlations and hierarchies. The question of data retention is thus significant, and raises considerable legal challenges. The second tendency

[110] NSA Press Release "DNI Statement on Recent Unauthorized Disclosures of Classified Information", 6 June 2013.

is to create additional categories that encapsulate series of criteria of profiling, in order to target specific groups of individuals that can be managed by human beings. The question of human resources managing these data thus becomes an important one too. These retention and selection processes are supposedly in place to ensure the *quality* of the information, whereas the sheer *quantity* can generate errors (false negatives and false positives). However, one can easily see that even if algorithms can help to connect a series of elements, this will not necessarily give a meaningful result in terms of prevention. Even if cyber surveillance can help to 'connect the dots', most of the time such gathering of information becomes meaningful only *after* a specific event has occurred, not *before*. Stella Remington, former Director General of MI5, illustrated this point with reference to the Boston bombings in April 2013.[111] She explained that despite the fact that the intelligence services in Boston had information on the Chechen perpetrators, they were unable to anticipate the attack and therefore the services in charge could not be held responsible for what happened. She explicitly made the point that, even with computer programmes, it was not possible to put under effective surveillance a group of people with less than five agents on each case. In light of the numerous uncertainties that surround cyber/communications surveillance, she also expressed doubts and concerns about the cost of investments in this kind of surveillance, as it is impossible to "keep tabs on every suspect".[112] In addition mass surveillance via data-mining may be a strategy for retrofitting evidence into a case after having exercised undue surveillance, possibly resulting in disrupting the process of criminal justice rather than accelerating it. In that case, large-scale surveillance is not oriented towards finding evidence, but towards an array of presumptions, which are justified *ex-post* through allegations of contacts between individuals that may be removed from each other by three levels of association.

A third challenge is to revisit US-EU relationships in the field of surveillance. At a diplomatic level, the US largely dominates the diplomacy of surveillance, in ways that clearly disrupt the cohesion of the EU in the field. The US surveillance agencies have maintained a matrix of cooperation inherited from the cold war with three different layers:

- The 'Five Eyes' network (US, UK, Canada, Australia and New Zealand) originated from a 1946 multilateral agreement for cooperation in signals intelligence, with which the US partly cooperates in collecting information and sharing results. The network has extended over time in terms of tasks (e.g. Echelon) and in terms of privileged partners. These include Sweden, which permits Five Eyes to gain access to internet cables from the Baltic states and Russia, as well as the special relationship of Five Eyes with Israel, which gives the network access to the Middle East region.
- A selection of EU countries with whom the US engages both in *ad hoc* collaboration but against whom campaigns of offensive espionage are also conducted (France, Germany, Italy, Benelux and Switzerland, Poland); in terms of collaborations, the DGSE in Paris was the node of a different network of 6 countries called Alliance base, regrouping four of the five eyes, but adding France and Germany. Alliance base is believed to have ended in 2009 because of tensions between the French and the US.[113] The US and France have issued mutual accusations of illicit economic espionage against the other.
- The other countries of Europe, Middle East and South America, which the US considers simply as targets for their operations and are not included in any collaborative process.

We deceive ourselves in thinking that the EU member states as a whole and moreover the EU institutions (the Council and the European Commission) can become a strong partner in negotiations with the US in the field of surveillance, despite the efforts of the EU Counter-Terrorism Coordinator. Moreover, EU member states have a different attitude towards collaborating with the US in terms of intelligence. This is reflected in their different member states' national laws that explicitly protect the collaboration between their services and the US from investigation. Therefore, large-scale communications surveillance reveals strong asymmetries at the international level.

---

[111] See R. Alexander, "Terror Watch Lists: Can You Keep Tabs On Every Suspect?", BBC News, 2 June 2013 (www.bbc.co.uk/news/magazine-22718000).

[112] Ibid.

[113] *Source*: D. Servenay, "Terrorisme: pourquoi Alliance Base a fermé à Paris", *Rue89*, 24 May 2010 (www.rue89.com/2010/05/24/terrorisme-fermeture-dalliance-base-a-paris-152349).

A fourth challenge for the future is how to tackle the involvement of private actors in these surveillance programmes. Private actors have now become a significant part of the large-scale surveillance, and play a key mediation role between the state and citizens' rights. The development of transnational platforms of exchange of information, and the participation of private actors at all stages of the process should receive the full attention of the European Parliament. The rights of citizens, but also of consumers are at stake here. As demonstrated in a previous study for the European Parliament dedicated to cloud computing,[114] the set of relationships currently defining cloud computing technologies and crime prevention encompasses negotiations and tensions between public authorities and private entities. In this set of relationships, data protection and privacy are often objects of negotiation to the detriment of individuals' rights.

In any case, it appears clear that, in a democracy, large-scale surveillance restructures the very notion of security and protection of human beings as well as the conception we have of freedom and fundamental rights. The types of profiling that large-scale surveillance generates is highly discriminatory and disrupts social cohesion. Eminent sociologists have convincingly argued that the use of statistics over specific groups of population not only undermines the idea that diversity is perfectly legitimate and desirable in a free society, but also leads to discrimination and stigmatisation.[115] Meeting the challenges underlined above are paramount for the future of our democracies, and will be with us for some time. Ignoring them would inevitably create room for new scandals and de-legitimise all the actors involved. A lack of action on the part of the European institutions will not help put an end to the controversy, while silence could be interpreted as a form of complicity.

The French *Ligue des Droits de l'Homme* has already taken action. As they underlined, these activities are no longer within the scope of anti-terrorist and counter-intelligence activities: they are a form of "fraudulent access and retention in an automated data processing system" with "illegal collection of personal data", "violation of intimacy and privacy" and "violations of the confidentiality of correspondence".[116] Other NGOs have suggested the link with cyber theft of identities. Could these surveillance activities be considered as forms of cyber crime? Rob Wainwright, Director of Europol, immediately argued that Europol "[has] no mandate to investigate any allegations of unauthorised activities by governments". [117] This significantly contrasts with Europol's retroactive position concerning the cyber-attack against Estonia, allegedly carried out by Chinese intelligence services.

National security is not the exclusive property of intelligence communities or national governments. National security interests are subject to supra-national democratic rule-of-law processes and standards, which now include human rights instruments/actors (ECHR) and post-national (fundamental rights) institutions like the European Union and its fundamental rights *acquis*. It could be argued that large-scale surveillance practices in EU member states constitute a systematic and persistent breach of the Union's values as foreseen in Article 7 TEU. Viviane Reding implicitly brought what is occurring in the UK under the remits of Article 7 TEU by stating that:

> … you certainly have noted that when a journalist is put under pressure in one of our Eastern Member States, Foreign Ministers from Germany, Britain, France, Sweden and Finland get very excited and ask the Commission to intervene. The European Parliament immediately calls for a plenary debate and tables a motion for a resolution condemning this incident. But we received not a single call from all these Foreign Ministers and all these Parliamentarians when Mr Miranda was arrested at the airport in London three weeks ago. Or when the Guardian had to destroy certain evidence on request of the British government.[118]

---

[114] D. Bigo et al. (2012), "Fighting cyber crime and protecting privacy in the cloud", Study for the European Parliament (PE 462.509), Brussels.

[115] See H. Becker (1963), *Outsiders: Studies in the Sociology of Deviance*, New York, NY: The Free Press; D. Lyon (2003), *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*, London: Routledge; O.H. Gandy, Jr. (2002), "Data Mining and Surveillance in the Post-9.11 Environment", *IAMCR Data Mining*, 7 November.

[116] See *Libération*, "Enquête à Paris sur le programme d'espionnage américain Prism", 28 August 2013 (http://bit.ly/1euuQar).

[117] "MEPs raise suspension of EU-US bank data deal", European Parliament, Press release, 24 September 2013 (http://bit.ly/1euwVDh).

[118] http://europa.eu/rapid/press-release_SPEECH-13-677_en.htm

The controversies raised by the recent revelations will not vanish easily, even if legal actions and concrete initiatives may take time. The action, or the lack thereof, of the European Parliament will be watched carefully. With the European elections approaching, one should not underestimate the consequences this could have on voters: there is indeed a possible rise of European parties that advocate less power for EU institutions, precisely because the latter are seen as ineffective to protect their citizens and the residents living in the EU. The Commission has already asked the Director of the NSA and the UK representative in Brussels to account for what has happened. Letters have been sent but no answers have been received. The credibility of the Commission itself is at stake, and more generally that of the EU institutions.

4.2 Policy recommendations

The following recommendations explore possibilities for the European Parliament to fully exercise its responsibility to safeguard EU citizens' rights.

Recommendation 1. The European Parliament should use the powers as its disposal to require explanations from the US and to further investigate EU member state collaboration with the NSA.

It could, for instance, ask for immediate suspensions of some existing agreements, such as the TFTP Agreement.[119] It is also possible to reschedule the agenda for the negotiations for the US-EU Transatlantic Trade and Investment Partnership (TTIP).

The European Parliament could also re-introduce proposals that were discarded after intense lobbying by the US administration. The "anti-FISA clause" (the proposed Article 42 of the Data protection regulation draft[120]), in particular, would have nullified any US request for technology and telecoms companies to hand over data on EU citizens.

Finally, the European Parliament could launch an enquiry on the specific network of intelligence agencies that are working with the NSA in Europe in order to analyse more in detail what is the nature and the scale of their cooperation. A key element would be to assess if the transnational governmental networks that have a transatlantic dimension are engaging in a sort of 'privacy shopping' by exchanging targets of surveillance in order to use the loopholes created in many national privacy laws by the existing differences in terms of protection regarding the nationality or/and territory criteria of the surveillance (foreign intelligence justification).

Recommendation 2. A 'professional code for the transnational management of data' within the EU should be set up, including guidelines on how this code would apply to EU partners

Such a code could limit the unlawful practices of intelligence services without undermining their efficiency. Sir David Omand, former Director of GCHQ in 1996-97, has proposed a series of best practices that could be implemented so that intelligence services act with full respect of democratic rules.[121] These elements are central if a red line has to be agreed on, taking into account all the actors involved. These principles raised by Sir David could be used as a 'professional' charter, applied to all the services involved in the access to European data:

---

[119] The freezing or termination of the TFTP Agreement with the United States was raised by MEPs during a hearing of the LIBE Committee on 24 September 2013 (see www.europarl.europa.eu/news/en/news-room/content/20130923IPR20604/html/MEPs-raise-suspension-of-EU-US-bank-data-deal).

[120] "Article 42 requires for transfers to third countries, where no adequacy decision has been adopted by the Commission, to adduce appropriate safeguards, in particular standard data protection clauses, binding corporate rules and contractual clauses. The possibility of making use of Commission standard data protection clauses is based on Article 26(4) of Directive 95/46/EC. As a new component, such standard data protection clauses may now also be adopted by a supervisory authority and be declared generally valid by the Commission. Binding corporate rules are now specifically mentioned in the legal text. The option of contractual clauses gives certain flexibility to the controller or processor, but is subject to prior authorisation by supervisory authorities." Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (http://bit.ly/1hZGREt).

[121] David Omand, "NSA leaks: how to make surveillance both ethical and effective", *The Guardian*, 11 June 2013 (http://bit.ly/1hZI4vy).

> **There must be sufficient sustainable cause.** Any tendency for the secret world to encroach into areas unjustified by the scale of potential harm to national interests has to be checked.
>
> **There must be integrity of motive.** No hidden agendas: the integrity of the whole system throughout the intelligence process must be assured, from collection to analysis and presentation.
>
> **The methods used must be proportionate.** Their likely impact must be proportionate to the harm that is sought to be prevented, for example by using only the minimum intrusion necessary into the private affairs of others.
>
> **There must be a right and lawful authority**. There must be the right level of sign-off on sensitive operations, with accountability up a recognised chain of command to permit effective oversight.
>
> **There must be a reasonable prospect of success.** All intelligence operations need careful risk management, and before approval is given there has to be consideration of the likelihood of unintended consequences and the impact if the operation were to be exposed or otherwise go wrong
>
> **Recourse to secret intelligence must be a last resort.** There should be no reasonable alternative way of acquiring the information by non-secret methods.[122]

An additional principle should be: one should not confuse suspicious criminal activities with different life styles. This principle is central, not only because the fairness of criminal systems in our democracies is too often destabilised by such mixing, but also because a police state can easily emerge from this confusion.[123] Freedom of thought, opinion and expression is at stake here. Bans on some specific modalities of data mining have to be explored, along similar lines to those examined by the US Congress in 2003: the *Data Mining Moratorium Act* (S. 188) proposed by Sen. Russ Feingold's (D-WI) and the *Citizens' Protection in Federal Databases Act* (S. 1484) proposed by Sen. Ron Wyden's (D-OR). This has been reactivated recently with the Amash amendment, narrowly defeated, which would have required the NSA to limit its telephone data collection only to individuals "under investigation".[124]

Recommendation 3. The EP should submit a Proposal on limitation of actions of private contractors while keeping in mind the free circulation of the Internet and the possibility of a European Privacy Cloud (EPC).

As was recently recognised by the European Commission in the memo entitled "What does the Commission mean by secure Cloud computing services in Europe?",[125] the EU needs to develop its own capacities in terms of cloud computing, in order to guarantee what we could define as a European Privacy Cloud (EPC). It is clear that the modalities of the US-EU Safe Harbour agreement, presented by the US as a guarantee in terms of privacy have been gravely violated. All companies involved in the PRISM scandal (Apple, Google, Yahoo, Facebook, etc.) were members of the Safe Harbour agreement. The data protection Directive regarding the access of private providers who are routing European data to the US via cloud computing has to be revised.

A Canadian proposal may be worth exploring. This proposal elaborates a 'route tracking device', which allows internet clients to choose fast or 'secure' routes for sending emails or other communications.[126] Such a proposal would oblige the companies to offer the option to all European countries' internet users in order to keep their internal communications and data storage in Europe. If the US companies do not propose this option, they would be obliged to warn the visitors on their websites. European companies may be required to do the same and to sign a code of privacy agreement respectful of the European Charter of Human Rights. Another possibility is to ask to the open source community of software developers to find a way to organise the equivalent of what is offered by the big nine companies today.

---

[122] Ibid.

[123] B. Hudson and S. Ugelvik (2012), *Justice and Security in the 21st Century: Risks, Rights and the Rule of Law*, New York, NY: Routledge.

[124] Read more: http://www.digitaltrends.com/mobile/why-the-nsa-collects-everyones-phone-records/#ixzz2i3coVI9Y

[125] European Commission - MEMO/13/898, 15 October 2013.

[126] J. Obar and A. Clement (2013), "Internet surveillance and boomerang routine", Working Paper, University of Toronto, July.

All users, whatever their nationality, should be equally protected. Internet users should have equal rights over the confidentiality of their correspondence. Such a right is not contrary to legitimate claims of the different services for their missions concerning crime and national security.

Recommendation 4. The European Parliament should ensure that certain key provisions in the draft data protection Regulation are maintained during negotiations with Council.

The recent vote in the LIBE Committee of the European Parliament on the general data protection Regulation on 21 October 2013 has unveiled some key proposals as regards data transfers to non-EU countries that still need to be confirmed during the negotiations with member states before becoming law. The current Article 43a states that, if a third country asks a firm or organisation to disclose personal data processed in the EU, the firm or organisation needs to obtain permission from the national data protection authority and inform the person concerned before transferring any data. Failure to comply with this safeguard incurs sanctions (current Article 79 of the Regulation): for organisations, written warnings may be issued for less serious breaches, or the organisation might be subject to a data protection audit; for companies the sanctions might take the form of a fine of up to €100 million or 5% of annual worldwide turnover, whichever is greater. When imposing these penalties, the data-protection authorities would have to take into account aggravating factors such as the duration of the breach, its negligent or repetitive character, willingness to cooperate and the magnitude of damage done. It is crucial that the European Parliament considers such provisions as 'red lines' during the inter-institutional negotiations on the final text of the Regulation.

Recommendation 5. The European Parliament should propose the establishment of a policy infrastructure at EU level capable of ensuring effective follow-up of intelligence revelations.

There is a need for the European Parliament to reflect critically about the EU's institutional capacity to deal with recurrent breaches by EU and foreign intelligence agencies that clearly impinge on the rights and freedoms of European citizens. Lessons should be learned from the Echelon affair to ensure that a more systematic and sustainable policy infrastructure is put into place that can ensure genuine follow-up in the wake of intelligence scandals.

Consideration should be given to the possibility of establishing a common model of European cooperation on intelligence exchange and sharing between EU member states and with third countries, which would be particularly concerned with refusing to cooperate in cases where the information was obtained through unlawful treatment of the individual. The model should also foresee more legal certainty concerning the kind of information that is exchanged, and the parameters for it to be considered as 'intelligence', as well as a common legal definition of 'law enforcement authorities' that would clearly differentiate the roles of intelligence services and other law enforcement (police) authorities. This common model should be closely, carefully and democratically monitored at both the national and European levels. As previous research has proposed,[127] a 'yellow-card, red-card system' could be adopted, in which transmission of tainted information in breach of the common accord would first be signalled by a warning (a 'yellow card') and if repeated, by exclusion (a 'red card') from the information-sharing network.

A committee at the European level led by the European Counter-Terrorist Coordinator could be set up to address possibilities for applying EU principles in the field of data protection, privacy and collective freedoms and to propose the basis for a transatlantic digital bill of rights concerning all data subjects, regardless of their nationality. In order to be credible, it should gather not only policy-makers, but also Internet providers as well as researchers and civil society representatives.

The participation of national parliaments should be also foreseen, in light of the Brussels Declaration that emphasised the need to create a "European Intelligence Review Agencies Knowledge Network" (EIRAN), with the main goal of improving democratic accountability of the intelligence and security services in Europe. The European Parliament could use the European Parliament's inter-parliamentary arrangement with

[127] Geyer (2007), "Fruit of the Poisonous Tree", op. cit.; S. Carrera et al. (2012), "The results of inquiries into the CIA's programme of extraordinary rendition and secret prisons in European states in light of the new legal framework following the Lisbon Treaty", Study for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), June.

national parliaments for sharing information on 'good' and 'bad' practices in the scrutiny of law enforcement authorities and intelligence services and the state of affairs in domestic inquiries.[128]

Recommendation 6. The European Parliament should exercise its powers to promote minimum standards set by the European Court of Human Rights (ECtHR).

The EU and the Council of Europe are not excluded from intervening in matters of national security when they affect human rights and fundamental freedoms of European citizens and all those affected by their government's security practices.

The European Court of Human Rights has developed a substantial body of jurisprudence on what constitutes interference prescribed by the law in the context of secret surveillance and information-gathering, which effectively establishes a set of criteria for determining the lawfulness of secret surveillance and interference of communications. The European Parliament should examine these minimum safeguards and reflect on how further value could be given to those standards within the EU legal system in order to ensure that they become an integral part in defining the 'red line' that intelligence services in democratic regimes cannot cross when they use large-scale surveillance.

A new study should be conducted to explore in detail the legal implications of ECtHR jurisprudence on intelligence-related activities over the EU's Internal Security Strategy and EU home affairs activities. Closer cooperation between the European Parliament and the Council of Europe (and its Parliamentary Assembly, PACE) would also be welcomed here.

Recommendation 7. Ensure more effective scrutiny and monitoring of EU home affairs agencies in the field of security and information exchange.

There are no mechanisms in place to ensure that EU home affairs agencies such as Europol (and Intsen in so far as it can be classified as an EU 'agency') have not received, processed or used information or intelligence that was illegally obtained by national authorities or third countries.

The forthcoming revision of Europol's mandate should be taken as an opportunity to address the accountability issues raised above. An independent evaluation could also be conducted about the extent to which any EU agencies may have known or received any sort of information relating to large-scale surveillance programmes by the EU member states. To understand the risks of EU home affairs agency (indirect) involvement in programmes of communications surveillance, a mapping could be undertaken of the points of intersection of national (intelligence) and law enforcement agencies that may have been involved in large-scale surveillance and the EU intelligence or information-exchange architecture. These points of intersection should be subjected to sensitive, democratic, legal and judicial controls.

As a means to ensure democratic accountability and oversight, the European Parliament could establish a special (permanent) inter-parliamentary committee on EU regulatory agencies, with a special focus on EU home affairs agencies working in the field of security and information exchange for law-enforcement purposes. This committee could be run by the European Parliament's LIBE Committee, with the participation of other relevant committees and representatives from corresponding committees of national parliaments. Its mandate would include the possibility of setting up 'confidential working groups' that would have access to the secret/non-publicly disclosed information. It should have the power, resources and expertise to initiate and conduct its own investigations and inquiries, as well as full and unhindered access to the information, officials and installations necessary to fulfil its mandate.

Recommendation 8. European Parliament to explore the potential for an EU-level protection for whistle-blowers.

Consideration should be given to whether systematic protection for whistle-blowers could be introduced in the EU-level legal framework, potentially including strong guarantees of immunity and asylum.

Recommendation 9. Further research should be commissioned by the European Parliament on large-scale surveillance practices by EU member states.

The evidence presented in this paper opens a set of new and pressing questions on the activities of European intelligence services and their compatibility with EU law, demonstrating that further research is needed in

[128] See also Carrera et al. (2012), Ibid.

this area. The European Parliament should commission an in-depth research study to examine the specific features and techniques of large-scale surveillance by EU member states, and their lawfulness under current domestic legal regimes as well as their compatibility with EU legal principles and standards.

Academic references

Amicelle, A. (2011), "The Great (Data) Bank Robbery: Terrorist Finance Tracking Program and the 'SWIFT Affair'", Research Question 36, CERI, Sciences-Po, Paris.

Becker, H. (1963), *Outsiders: Studies in the Sociology of Deviance*, New York, NY: The Free Press;

Bigo, D. (2006), "Intelligence Services, Police and Democratic Control: The European and Transatlantic Collaboration", in D. Bigo and A. Tsoukala, *Controlling Security,* Paris: L'harmattan.

Bigo, D. et al. (2011), "Towards a New EU Legal Framework for Data Protection and Privacy: Challenges, Principles and the Role of the European Parliament", Study for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), Brussels, November.

_____.(2012), "Fighting cyber crime and protecting privacy in the cloud", Study for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), PE 462.509, Brussels.

Bowden, C. (2013), "The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights", Study for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), PE 474.405, Brussels September.

Campbell, D. (1999), "The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems and its applicability to COMINT targeting and selection, including speech recognition", Part 2/5, in: STOA (Ed.), *Development of Surveillance Technology and Risk of Abuse of Economic Information*, October, PE 168.184, European Parliament.

Carrera, S. et al. (2012), "The results of inquiries into the CIA's programme of extraordinary rendition and secret prisons in European states in light of the new legal framework following the Lisbon Treaty", Study for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), June.

Dulles, A. (1963), *The Craft of Intelligence*, New York: Harper&Row.

Gandy Jr, O.H (2002), "Data Mining and Surveillance in the Post-9.11 Environment", IAMCR Data Mining, International Association for Media and Communication Research, 7 November.

Geyer, F. (2007), "Fruit of the Poisonous Tree Member States' Indirect Use of Extraordinary Rendition and the EU Counter-Terrorism Strategy", CEPS Working Document No. 263, CEPS, Brussels, April.

Gill, P. (2012), "Intelligence, Threat, Risk and the Challenge of Oversight', *Intelligence and National Security*, 27:2, pp. 206-222.

Guild, E. and S. Carrera (2011), "Towards an Internal (In)security Strategy for the EU?", CEPS Paper in Liberty and Security in Europe, January.

Haggerty, K. and R. Ericson, (2000), "The Surveillant Assemblage", *British Journal of Sociology*, 51(4), pp. 605-622.

Heumann, S. and B. Scott (2013), "Law and Policy in Internet Surveillance Programs: United States, Great Britain and Germany", Stiftung Neue Verantwortung, Berlin and Open Technology Institute of the New America Foundation, Washington, D.C., September.

Hudson, B. and S. Ugelvik (2012), "Justice and Security in the 21st Century: Risks, Rights and the Rule of Law", New York, NY: Routledge.

Jones, C. (2013), "Secrecy reigns at the EU's Intelligence Analysis Centre", Statewatch Analysis, London.

Klamberg, M. (2010), "FRA and the European Convention on Human Rights", *Nordic Yearbook of Law and Information Technology*, Bergen, pp. 96-134.

Lyon, D. (2003), *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*, London: Routledge.

Marx, G.T. (1989), *Undercover: Police Surveillance In America*, Berkeley, CA: University of California Press.

Obar, J. and A. Clement (2013), "Internet surveillance and boomerang routine", Working Paper, July 2013, University of Toronto.

O'Donnell, G. (2004), "The Quality of Democracy: Why the Rule of Law Matters*?"*, *Journal of Democracy*, Vol. 15, No. 4, October.

Omand, D. (2008), "Can we have the Pleasure of the Grin without Seeing the Cat? Must the Effectiveness of Secret Agencies Inevitably Fade on Exposure to the Light?", *Intelligence and National Security*, Vol. 23, No. 5, pp. 593-607.

Parkin, J. (2012), "EU Home Affairs Agencies and the Construction of EU Internal Security", CEPS Paper in Liberty and Security in Europe, CEPS, Brussels, December.

Wills, A., M. Vermeulen, H. Born, M. Scheinin, M. Wiebusch and A. Thornton (2011), "Parliamentary Oversight of Security and Intelligence Agencies in the EU", Note for the European Parliament, PE 453.207, 15 June.

Weller, D. and B. Woodcock (2013), "Internet Traffic Exchange: Market Developments and Policy Challenges", *OECD Digital Economy Papers*, 207, OECD, Paris.

ANNEX
The EU Member States' Practices in the context of the Revelations of Large-Scale Surveillance Operations by the NSA

This Annex draws together the available evidence to shed light on potential programmes of large-scale surveillance being conducted by the intelligence services of EU member states. It seeks to establish whether PRISM-like surveillance programmes exist in the EU. Do surveillance programmes run by EU member states share commonalities with those executed by the NSA? How do they compare in terms of scale, technical features and the degree of accountability and oversight characterising their implementation?

The Annex does not attempt to make a new, comprehensive assessment of the surveillance practices of every EU member state but rather selects for in-depth assessment five countries where the available evidence (via investigative journalism, academic analysis or official documentation) indicates the use of electronic surveillance practices that go beyond traditional, targeted surveillance for intelligence purposes. These five countries are the UK, Sweden, France, Germany and the Netherlands. Each member state is examined with the following criteria in mind: the basic technical features of large-scale surveillance programmes; stated purpose of programmes, targets and types of data collected; actors involved in collection and use, including evidence of cooperation with the private sector; cooperation or exchange of data with foreign intelligence services, including the NSA; and the legal framework and oversight governing the execution of the programme(s).

1. The United Kingdom[1]

Of the five member states examined, the evidence suggests that the UK government is engaged by far in the most extensive large-scale surveillance activities in the EU.

Internet surveillance in the UK is primarily carried out by the agency known as the Government Communications Headquarters (GCHQ), which produces signals intelligence (SIGINT) for the UK government. GCHQ is mandated to work "in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's government; in the interests of the economic wellbeing of the United Kingdom; and in support of the prevention and the detection of serious crime".[2] In budgetary terms GCHQ receives the greatest investment of all the UK's intelligence services (approximately £1 billion annually) and its human resources are twice the size of the workforce of MI5 and MI6 combined (6,000 staff).[3]

The disclosures by former NSA contractor Edward Snowden and revelations in the US and European press, particularly The Guardian newspaper, have provided a much broader understanding of the depth and range of GCHQ's activities than experts previously had access to. These reports describe a range of programmes and projects linked to the large-scale access, processing and storage of data that fall within the overarching framework of a GCHQ project named by the agency 'Mastering the Internet' (MTI).[4] Reports indicate a budget of over £1 billion devoted to the MTI project over a three-year period,[5] creating capacities for the interception, storage and processing of data on a par with, and potentially even exceeding that of, the NSA with whom it works in close cooperation.

---

[1] The information presented here is primarily based on revelations published in press reports, testimony to the European Parliament Inquiry on electronic surveillance of EU citizens and the expert witness statement of Dr. Ian Brown, Associate Director of Oxford University's Cyber Security Centre, for Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK Application No: 58170/13 to the European Court of Human Rights.

[2] Intelligence Services Act (ISA) 1994.

[3] N. Hopkins, J. Borger and L. Harding, "GCHQ: inside the top secret world of Britain's biggest spy agency", *The Guardian*, 2 August 2013(www.theguardian.com/world/2013/aug/02/gchq-spy-agency-nsa-snowden).

[4] E. MacAskill et al., "Mastering the internet: how GCHQ set out to spy on the world wide web", *The Guardian*, 21 June 2013 (www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet).

[5] C. Williams, "Jacqui's secret plan to master the internet", *The Register*, 3 May 2009 (www.theregister.co.uk/2009/05/03/gchq_mti/).

1.1 Programme(s) for large-scale surveillance

Potentially the most far-reaching of the programmes run by GCHQ within the MTI project is the so-called 'Tempora programme'. According to disclosures by The Guardian newspaper, the UK is engaged in the routine interception of undersea cables for the purpose of capturing internet content. Reports allege that GCHQ has placed data interceptors on approximately 200 of the UK-based fibre-optic cables that transmit Internet data into and out of the British Isles carrying data to Western Europe from telephone exchanges and Internet servers in North America.[6] The Tempora programme is estimated to be around five years old, having first been developed and piloted in 2009 and operational since at least early 2012.[7]

The technique of directly tapping the fibre-optic cables entering and exiting the UK (known as Special Source Exploitation) appears to have given GCHQ access to unprecedented quantities of information. In terms of scale, leaked official documents claim that by 2012, GCHQ was able to process data from at least 46 fibre-optic cables at any one time, giving the agency the possibility to intercept, in principal, more than 21 petabytes of data a day.[8] This is estimated to have contributed to a 7,000% increase in the amount of personal data available to GCHQ from internet and mobile traffic in the past five years and given the UK the biggest Internet access in 'Five Eyes'.[9] Data are understood to be stored at underground storage centres at GCHQ headquarters in Cheltenham, and potentially other agency sites (GCHQ's sister base in Bude, Cornwall as well as another unnamed base outside of the UK).[10]

The data intercepted and processed consist both of 'content' – referring to recordings of phone calls, content of email messages, entries on Facebook, histories of an Internet user's access to websites, etc. – as well as 'metacontent' – data recording the means of creation of transmitted data, the time and date of its creation, its creator and location where it was created.[11] Content intercepted by Tempora is kept for up to three days, while metacontent is stored for up to 30 days. Around 300 GCHQ and 250 NSA operatives are charged with analysing the data intercepted by Tempora.[12]

Both content and metacontent are filtered using a technique called Massive Volume Reduction (MVR). Approximately 30% of the data is removed early in the process, classified as 'high-volume, low-value' traffic (consisting for instance of peer-to-peer music, film and computer programme downloads). The remaining data are searched using so-called 'selectors', which can include keywords, email addresses and phone numbers of targeted individuals. There are approximately 40,000 such selectors identified by GCHQ.[13]

The objectives underpinning this mass collection of data and the individuals targeted are ambiguous, and as yet they are not clearly delineated in the documents and reported disclosures. According to an intelligence source quoted by The Guardian, the criteria governing the use of selectors to search and filter the data relate to security, terrorism, organised crime and economic well-being.[14] An internal GCHQ memo dated October 2011 stated: "[Our] targets boil down to diplomatic/military/commercial targets/terrorists/ organised criminals and e-crime/cyber actors."[15]

---

[6] E. MacAskill et al., "GCHQ taps fibre-optic cables for secret access to world's communications", *The Guardian*, 21 June 2013 (www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa).

[7] Ibid.

[8] A petabyte is approximately 1,000 terabytes, which in turn is 1,000 gigabytes. The comparison made by The Guardian was that this is equivalent to sending all the books in the British Library 192 times every 24 hours.

[9] P. Beaumont, "NSA leaks: US and Britain team up on mass surveillance", *The Observer*, 22 June 2013; N. Hopkins, J. Borger and L. Harding, "GCHQ: inside the top secret world of Britain's biggest spy agency", *The Guardian*, 2 August 2013 (www.theguardian.com/world/2013/aug/02/gchq-spy-agency-nsa-snowden).

[10] Statement by Duncan Campbell at the European Parliament's LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, 1st Hearing, 5 September 2013; N. Hopkins, J. Borger and L. Harding (2013), "GCHQ: inside the top secret world of Britain's biggest spy agency", *The Guardian*, 2 August (www.theguardian.com/world/2013/aug/02/gchq-spy-agency-nsa-snowden).

[11] MacAskill et al. (2013), op. cit.

[12] Ibid.

[13] The NSA has reportedly identified 31,000 selectors. Ibid.

[14] Ibid.

[15] Op. cit.

In principal, the UK legal framework allows Tempora only to target 'external' communications, in other words communications between non-UK residents, or between a UK resident and a non-UK resident. However, in practice, given that a substantial proportion of internal UK communications is routed offshore, all internet users are potential targets of the Tempora programme, both British citizens (and UK residents) as well as non-British citizens and residents. As the UK is an important landing point for the vast majority of transatlantic fibre-optic cables, the monitoring of these cables means that a large proportion of communications from around the world would be intercepted.[16]

Details concerning the logistical operation of the Tempora programme imply some cooperation with private-sector telecommunications companies. On 2 August 2013, the Süddeutsche newspaper published the names of the commercial companies cooperating with GCHQ and providing access to their customer's data within the Tempora programme.[17] The newspaper cited seven companies (BT, Vodafone Cable, Verizon Business, Global Crossing, Level 3, Viatel and Interroute), referred to as 'intercept partners', which together operate a large proportion of the undersea fibre-optic internet cables.[18] Allegations claim that companies are paid for logistical and technical assistance and are obliged to cooperate under the 1984 Telecommunications Act. Spokespersons of the companies concerned have stated that they are legally obliged to cooperate, and all cooperation is in accordance with European and national laws.[19] Allegations have also been made that GCHQ has accessed cables without the consent or knowledge of the companies that own or operate them.[20]

The Guardian's reports on the Tempora programme have been verified and deemed credible by external experts, such as Ian Brown, member of the UK Information Commissioner's Technology Reference Panel. According to Dr. Brown's statement in the application to the European Court of Human Rights Big Brother Watch and others vs. the United Kingdom:

> The Guardian reports appear to me to be credible. Some of the details have been confirmed by the US government, and by previous leaks (including by statements by former senior NSA officials such as William Binney). Much of the technology used (such as optical splitter equipment) is commercially available. The budgetary resources required fit within the publicly known budgets of the UK and US intelligence agencies.[21]

Another key dimension of GCHQ's large-scale surveillance activity that has emerged from The Guardian's disclosures is the UK's participation in the PRISM programme. Following press revelations concerning the US surveillance activities and programmes operated by the NSA (see section 1 of this study), The Guardian reported that the US shares information it obtains via the PRISM programme with the UK authorities. According to reports, GCHQ has had access to the data gathered under the PRISM programme since June 2010 and generated 197 intelligence reports from this data in 2012. It has been subsequently presumed that GCHQ also has access to wider information obtained by NSA surveillance activities under section 1881a, including material that is directly intercepted from so-called 'upstream collection' – the direct interception of communications as they pass through fibre-optic cables and electronic infrastructures of telecommunication companies or online service providers in the US (and potentially around the world).[22]

Privacy advocacy groups and experts have claimed that through its access to US programmes such as PRISM, the UK is able to obtain information about UK citizens' or residents' internal communications that would otherwise be out of bounds to UK intelligence agencies without first obtaining a warrant under the

---

[16] Expert Witness Statement of Ian Brown for Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK Application No: 58170/13 to the European Court of Human Rights.

[17] J. Goetz and F. Obermaier (2013), "Snowden enthüllt Namen der spähenden Telekomfirmen", *Süddeutsche Zeitung*, 2 August. The paper's exposé was based on information it had seen on an internal GCHQ powerpoint slide from 2009.

[18] Goetz and Obermaier (2013), op. cit.

[19] J. Ball, L. Harding and J. Garside (2013), "BT and Vodafone among telecoms companies passing details to GCHQ", *The Guardian*, 2 August.

[20] Ibid. See also Statement by Duncan Campbell at the European Parliament's LIBE Committee Inquiry on Inquiry on Electronic Mass Surveillance of EU Citizens, 1st Hearing, 5 September 2013.

[21] Expert Witness Statement of Ian Brown for Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK Application No: 58170/13 to the European Court of Human Rights.

[22] Privacy International submission to the Investigatory Powers Tribunal, "Statement of Grounds", 8 July 2013 (www.privacyinternational.org).

Regulation of Investigatory Powers Act 2000 (RIPA). The allegations that this cooperation has effectively allowed the UK authorities to circumvent the UK legal regime have been investigated by the ISC and are further discussed in section 1.3 of this Annex.

Leaked documents have also cited a decryption programme named 'Edgehill'. On 6 September 2013, The Guardian published a report alleging that GCHQ has been cooperating with a 10-year programme by the NSA against encryption technologies.[23] According to documents seen by The Guardian, a GCHQ pilot programme attempted to establish a system that could identify encrypted traffic from its internet cable-tapping programmes (e.g. Tempora). Reports indicate that the decryption programme, named 'Edgehill', was seen as critical in maintaining the strategic advantage that GCHQ has gained with its Tempora programme, as large internet providers began increasingly to encrypt their communications traffic.

GCHQ documents show that Edgehill's initial aim was to decode the encrypted traffic certified by three major (unnamed) internet companies and 30 types of Virtual Private Network (VPN), used by businesses to provide secure remote access to their systems. It is reported that by 2015, GCHQ hoped to have cracked the codes used by 15 major internet companies and 300 VPNs. The Guardian also claims that analysts on the Edgehill project were working on ways into the networks of major webmail providers as part of the decryption project.

Documents leaked by Edward Snowden have also indicated that the UK has engaged in GCHQ-coordinated offensive operations aimed at diplomatic or economic espionage. Internal GCHQ powerpoint slides published by The Guardian in June 2013 indicated that GCHQ intercepted the phones and monitored internet use of foreign politicians and diplomats taking part in two G20 summit meetings in London in 2009.

In September 2013, Der Spiegel published revelations that GCHQ coordinated a project code-named 'Operation Socialist' which saw a cyber-attack against the Belgian telecoms company Belgacom.[24] During the European Parliament hearing of 3 October 2013, Belgacom Vice-President Geert Standaert stated that the 'spyware', discovered in June 2013, had penetrated 124 of its 26,000 IT systems.[25] Belgacom executives indicated that the scale and sophistication of the attack implied a state actor, but neither confirmed nor denied allegations alluding to GCHQ's involvement.[26]

In addition to the main disclosures relating to GCHQ large-scale surveillance activities discussed above, other programmes about which less is known have come to light. These include the so-called 'Global Telecoms Exploitation' programme which is understood to also be conducted through tapping fibre-optic cables and which allows GCHQ to handle 600 million 'telephone events' each day.[27]

Further, documents leaked to The Guardian reveal a 'mobile' project designed to exploit mobile devices, collecting voice, sms and geo-locations as well as the additional functionalities that come with smartphones, such as emails, internet searches and social media posts. Internal GCHQ documents underscore the importance of this project in order to keep pace with the increased use of smart phones. It is estimated that 90% of all internet traffic will come from mobile phones by 2015.

According to The Guardian, it had seen documents which make it clear that "GCHQ was now capable of 'attacking' hundreds of apps, and a 'mobile capability map' from June last year stated the agency had found ways of looking at the search patterns, emails and conversations on many commonly used phone services."[28]

---

[23] J. Ball, J. Borger and G. Greenwald (2013), "Revealed: how US and UK spy agencies defeat internet privacy and security", *The Guardian*, 6 September.

[24] Spiegel online (2013), "Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm", *Der Spiegel*, 20 September.

[25] European Parliament's LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, 3 October 2013.

[26] Ibid.

[27] MacAskill et al. (2013), op. cit. Also Expert Witness Statement of Ian Brown for Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK Application No. 58170/13 to the European Court of Human Rights.

[28]. MacAskill et al. (2013), op. cit.

1.2 Cooperation with foreign intelligence services

Evidence that has come to public attention over the past four months indicates a close working relationship between the NSA and GCHQ on mass cyber-surveillance activities.[29] This concerns both data and intelligence-sharing but also in the collaborative development of pilot programmes and technologies. For example, early internal GCHQ documents describing Tempora initially referred to this programme as "a joint GCHQ/NSA research initiative".[30] Reports also allege close cooperation between GCHQ and NSA in the development of decryption technologies.[31]

In terms of data and intelligence-sharing, the UK appears to conduct a substantial and routine reciprocal relationship of data exchange with the US authorities. Reflecting the details of the UK's access to PRISM data outlined in section 2.1.2 in the main report, a UK government paper that set out the views of GCHQ in the wake of the 2010 strategic defence and security review admitted that 60% of the UK's high-value intelligence "is based on either NSA end-product or derived from NSA collection" (end product referring to official reports that are distillations of raw intelligence.)[32]

Similarly, the UK is reported to provide access to the data collected through the Tempora and other programmes, available to the NSA, with Guardian reports implying that while the UK had the means to collect huge amounts of data through Tempora and its access to undersea internet cables, the NSA could provide the resources (850,000 operatives) and technologies to process and analyse that data. An internal report explained that "GCHQ and NSA avoid processing the same data twice and proactively seek to converge technical solutions and processing architectures."[33]

The degree of cooperation between the two agencies is reflected in revelations exposing the details of the NSA payments to GCHQ in the last years. The Guardian reports that the payments, which are set out in GCHQ's annual 'investment portfolios' seen by the newspaper, show that the US government has paid at least £100 million to the UK spy agency GCHQ over the last three years. The papers show that NSA gave GCHQ £22.9 million in 2009. The following year the NSA's contribution increased to £39.9 million, of which £17.2 million was allocated for the agency's Mastering the Internet project. The NSA also paid £15.5 million towards redevelopments at GCHQ's sister site in Bude, Cornwall, which intercepts communications from the transatlantic cables that carry internet traffic. In 2011-12, the NSA paid another £34.7 million to GCHQ.[34]

1.3 Legal framework and oversight

1.3.1 Legal framework

Surveillance of communications in the UK are carried out within the legal framework established by the UK's 2000 Regulation of Investigatory Powers Act (RIPA). The warranting process under RIPA falls under two separate regimes, depending on the types of data accessed. Interception of content is authorised by a warrant signed by the Secretary of State specifying an individual or premises and is valid for 3-6 months.[35] Access to 'communications data' is regulated under a separate Chapter of RIPA and permits some agencies to self-authorise access to some of this data.[36] 'Communications data' are here defined in relatively vague

---

[29] N. Hopkins and J. Borger (2013), "Exclusive: NSA pays £100m in secret funding for GCHQ", *The Guardian*, 1 August (http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden).

[30]. MacAskill et al. (2013), op. cit.

[31] Ball, Borger and Greenwald (2013), op. cit.

[32] Hopkins and Borger (2013), op. cit.

[33] MacAskill et al. (2013), op. cit.

[34] Hopkins and Borger (2013), op. cit.

[35] Part 1, Chapter 1 of RIPA, 2000.

[36] Ibid., Chapter 2. See also Expert Witness Statement of Ian Brown for Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK Application No: 58170/13 to the European Court of Human Rights. According to RIPA, communications data can be accessed by a range of government agencies on a broad set of grounds, including in the interests of national security, preventing or detecting crime or disorder, economic well-being and so on, and includes any purpose specified in an order made by the Secretary of State. See S.22(2) RIPA.

terms and refers to 'traffic data' that includes identities of individuals and equipment as well as location details, routing information and signalling information.[37]

An interception warrant specifying an individual or premises is not needed where UK authorities intercept communications external to the UK. In this scenario, an authorising certificate from the Secretary of State is required which describes the nature/classification of material to be examined.[38] It is under the latter legal mechanism by which data exchange with the US, including that implicated in the PRISM programme, as well as Tempora Programme activities are understood to have been authorised.[39]

In addition, under the Telecommunications Act 1984, the Secretary of State may give providers of public electronic networks "directions of a general character… in the interests of national security or relations with the government of a country or territory outside the United Kingdom".[40]

Although RIPA is stated to be compatible with the ECHR and includes explicit tests of proportionality and necessity before communications content and metadata may be accessed, experts have noted that "the standards according to which these tests of proportionality are carried out are mainly secret, and applied by the government's legal advisers and the Secretary of State, with limited oversight."[41]

1.3.2 Oversight

The UK's intelligence oversight regime is composed of the Intelligence and Security Committee, an Interception of Communications Commissioner (IoCC) and the Investigatory Powers Tribunal.

On 7 June 2013, the Intelligence and Security Committee (ISC)[42] issued a statement indicating that it had launched an investigation into allegations that the agency circumvented UK law by using the NSA's PRISM programme to access the content of private communications within the UK without proper authorisation. On 17 July 2013, the Chairman of the Intelligence and Security Committee of Parliament, the Rt Hon Sir Malcolm Rifkind MP, issued a follow-up statement regarding the outcome of those investigations.[43] The statement concluded that, after taking detailed evidence from GCHQ, any suggested allegations are "unfounded" and complied with the legal safeguards set out in RIPA. The ISC maintained that "in each case" that it examined, GCHQ had a warrant for interception in accordance with RIPA, although the terms of those warrants have not been published. Experts have concluded from the ISC's public statements that it was not previously aware of the PRISM Programme. While the ISC concluded that GCHQ has not circumvented the law, it nevertheless acknowledged the need "to consider further whether the current statutory framework governing access to private communications remains adequate".

An Investigatory Powers Tribunal, appointed from current or former senior members of the judiciary, also exists to explore complaints covering the eligibility of GCHQ activities under RIPA. Both the UK charity Privacy International and the civil rights group Liberty have submitted claims to the IPT following the

[37] S. 21 (4) RIPA.

[38] S.8(4) RIPA.

[39] Expert Witness Statement of Ian Brown for Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK Application No: 58170/13 to the European Court of Human Rights.

[40] S.94 Telecommunications Act.

[41] Expert Witness Statement of Ian Brown for Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK Application No: 58170/13 to the European Court of Human Rights.

[42] The Intelligence and Security Committee of Parliament (ISC) is a statutory committee of Parliament that has responsibility for oversight of the UK intelligence community. The Committee was originally established by the Intelligence Services Act 1994. The Committee oversees the intelligence and security activities of the UK, including the policies, expenditure, administration and operations of the Security Service (MI5), the Secret Intelligence Service (MI6) and the Government Communications Headquarters (GCHQ). The Committee consists of nine Members drawn from both Houses of Parliament.

[43] Intelligence and Security Committee of Parliament, Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme, 17 July 2013 (http://isc.independent.gov.uk/news-archive/17july2013).

revelations of GCHQ's activities in PRISM and Tempora.[44] However, this body has not in the past demonstrated a strong oversight function of GCHQ.[45]

2. Sweden[46]

According to revelations by investigative journalists and experts consulted for the purpose of this study, Sweden is becoming an increasingly important partner of the global intelligence network. Signals intelligence operations in Sweden are the responsibility of the National Defence Radio Establishment (FRA). In recent years, reports have emerged alleging that FRA has engaged in operations and programmes for the mass collection of data, with features that resemble in part those pursued by the US NSA and the UK's GCHQ.

2.1 Programme(s) for large-scale surveillance

Swedish intelligence services have a longstanding history of intercepting signals intelligence,[47] however the past five years have seen allegations emerge stating that the FRA has been engaged in accessing data traffic crossing its borders from fibre-optic internet cables.[48] In 2008 the TV broadcaster SVT reported that FRA was collecting/receiving data from Russia and the Baltic states and forwarding them in bulk to the US.[49] These allegations were recently re-stated during Duncan Campbell's testimony to the European Parliament Inquiry on Electronic Mass Surveillance of EU Citizens of 5 September 2013, where he alleged that while the Försvarets radioanstalt has been running satellite interception facilities for many years, Sweden's new internet laws passed in 2009 (FRA law) authorised the agency to monitor all cable-bound communications traffic into and out of Sweden, including emails, text messages and telephone calls. FRA is now alleged to engage in intercepting and storing communications data from fibre-optic cables crossing Swedish borders from the Baltic sea.[50]

The evidence indicates that FRA has been running operations for the 'upstream' collection of private data – collecting both the content of messages as well as metadata of communications crossing Swedish borders. The metadata are retained in bulk and stored in a database known as 'Titan' for a period of 18 months.[51]

It is understood that interception of these fibre-optic cables involves a legal obligation on communications service providers to transfer all cable communications crossing Swedish borders to specific 'interaction points', where the communications service providers surrender the data to the state.[52]

---

[44] Privacy International submission to the Investigatory Powers Tribunal, "Statement of Grounds", 8 July 2013 (www.privacyinternational.org).

[45] In 2004 the IPT received 115 cases in which it found no breach of RIPA or the Human Rights Act 1998. In leaked documents there are implications that GCHQ did not take this oversight mechanism particularly seriously, stating in internal documents leaked to The Guardian newspaper that "so far they have always found in our favour". (Guardian – "GCHQ taps fibre optic cables").

[46] The information gathered on the large-scale surveillance practices of Sweden is based primarily on the expert input of Dr. Mark Klamberg, Uppsala University, as well as press articles, and official documentation.

[47] Swedish Government Official Reports record that Swedish law enforcement agencies began with signals intelligence as early as 1939. See SOU (2009), 'Signalspaning för polisiära behov,' Stockholm, p.55.

[48] N. Nielsen (2013), "EU asks for answers on UK snooping programme", *EU Observer*, 26 June.

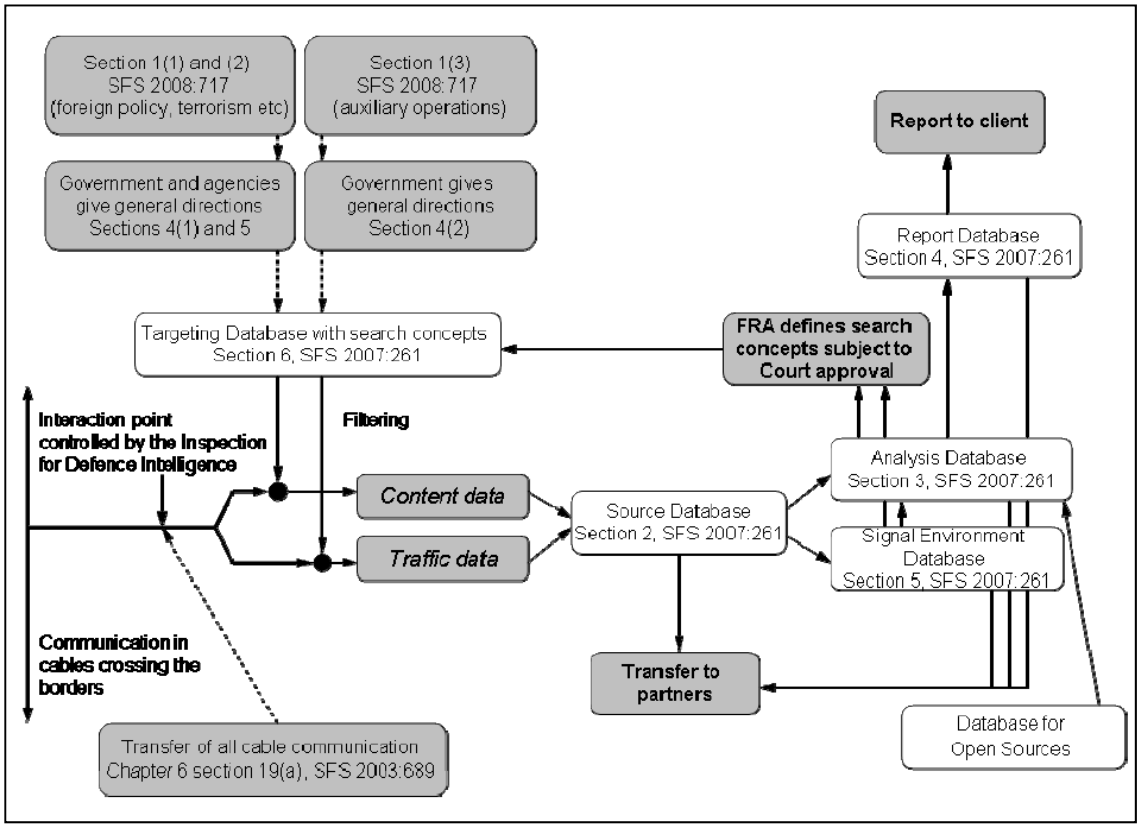
[49] SVT "FRA-lagen ska användas mot Ryssland", 9 July 2008.

[50] Statement by Duncan Campbell at the European Parliament's LIBE Committee Inquiry on Inquiry on Electronic Mass Surveillance of EU Citizens, 1st Hearing, 5 September 2013; A. Tomkvist (2013), "Bildt: surveillance in Sweden "not like Prism'", *The Local*, 13 June.

[51] M. Klamberg, (2010), 'FRA and the European Convention on Human Rights', *Nordic Yearbook of Law and Information Technology*, Bergen 2010, pp. 96-134.

[52] Klamberg (2010), Ibid.

Figure A1. How the FRA processes communications and information



Source: M. Nilsson, M. Klamberg and A. Petersson in M. Klamberg (2010), "FRA and the European Convention on Human Rights", Nordic Yearbook of Law and Information Technology, Bergen.

Concerning the profile of individuals targeted by the FRA's mass data interception programme, the initial targets again appear to be indiscriminate. As in the UK, the bulk retention of data is, under the Swedish legal regime, only meant to cover communications entering or exiting Swedish borders and not internal communications. However, internal communications that have been routed through nodes based outside Swedish territory are likely to also be classified as 'foreign' communications and retained for analysis. The Swedish legislative framework regulating the collection of signals intelligence provides that if there is uncertainty whether data are foreign or domestic, the data may be collected and retained.[53]

Final (processed) intelligence, described as 'reports to clients' is discriminate and does not include citizens in general. The legislation differentiates between 'defence intelligence operations' and 'auxiliary operations'. Defence intelligence operations concern a relatively small fraction of the communications that are deemed to directly relate to external military threats, international terrorism and similar phenomena. The content of such communications associated with such threats is selected and reserved for detailed analysis. By contrast, the 'auxiliary operations', which make up the lion's share of communications intercepted, is analysed as metadata, not content, and are not intended for generating intelligence reports to FRA's clients.[54]

However, academic experts argue that the division between these modes of processing these two kinds of data is not clear-cut. Dr. Klamberg states that this division:

> …creates the impression that a wall has been erected where the large amounts of traffic data [metadata] collected through the auxiliary operations is used purely for some abstract technical matters and not for intelligence purposes. This is a misconception.[55]

[53] Section 2(a) of the Act 2008:717 on signals intelligence.

[54] Prop. (Government Bill) 2006/07:63, En anpassad försvarsunderrättelseverksamhet (Adapted Defence Intelligence Operations) (www.regeringen.se/content/1/c6/07/83/67/2ee1ba0a.pdf).

[55] Expert input by Dr. Mark Klamberg, Uppsala University. See also Klamberg (2010), op. cit.

This misconception is due to the fact that the preparatory works for the Swedish law on signals intelligence state that since the auxiliary operations "aim to facilitate the defence intelligence operations it would not be incompatible with the purpose for which the data is collected that the data is also used to some extent in the defence intelligence operations."[56]

Second, the preparatory works explain that reports to clients may involve extensive descriptions of meta-data patterns and therefore, despite being intended for auxiliary operations, may also be used for defence intelligence purposes.[57]

While there is no explicit statement as to which national entities receive the data or resulting intelligence drawn from this programme, according to the Swedish legislative framework, data collected by the FRA may be shared with the following 'customers':[58]

1. Government offices (Regeringskansliet)
2. National Police Board (Rikspolisstyrelsen - RPS) which includes the National Bureau of Investigation and the Secret Service
3. Swedish Agency for Non-Proliferation and Export Controls (Inspektionen för strategiska produkter - ISP)
4. Defence forces (Försvarsmakten)
5. Swedish Defence Materiel Administration (Försvarets materielverk - FMV)
6. Swedish Defence Research Agency (Totalförsvarets forskningsinstitut - FOI)
7. Swedish Civil Contingencies Agency (Myndigheten för samhällsskydd och beredskap - MSB)
8. Swedish Customs (Tullverket)

2.2 Cooperation with foreign intelligence services

There is evidence that FRA may be sharing substantial quantities of the data it collects with foreign intelligence services, including NSA. Swedish legislation allows for the bulk transfer of data to other states if authorised by the Government.[59] Reports from media, experts as well as government statements indicate that Swedish authorities have made use of this possibility through exchanges of large amounts of raw data with the US as well as the Baltic states.[60]

Duncan Campbell, during his testimony to the European Parliament hearing on 5 September 2013, stated that Sweden's FRA has become a new and important partner of 'Five Eyes', by providing major satellite and undersea-cable interception arrangements, stating that FRA "is deemed, according to the documents, to be the biggest collaborating partner of GCHQ outside the English-speaking countries". Code-named 'Sardine', he highlighted that Sweden makes an important contribution to the Five Eyes organisation, having access to cables that were hitherto inaccessible (those from the Baltic states and Russia).

In a statement following the revelations by Campbell, Defence Minister Karin Enstrom said Sweden's intelligence exchange with other countries is "critical for our security" and that "intelligence operations occur within a framework with clear legislation, strict controls and under parliamentary oversight."[61] Likewise a FRA spokesperson has acknowledged that FRA shares data with other countries, but declined to specify which countries or to provide further details of the types of data shared.[62] Similarly, there is no

---

[56] Prop. (Government Bill) 2006/07:46, Personuppgiftsbehandling hos Försvarsmakten och Försvarets radioanstalt (Processing of Personal Data by the Armed Forces and the National Defence Radio Establishment) (www.regeringen.se/content/1/c6/07/73/05/7ac2933f.pdf).

[57] SOU (Swedish Government Official Reports) 2009:66, Signalspaning för polisiära behov (Signal Intelligence for Law Enforcement Purposes) (http://www.regeringen.se/content/1/c6/12/99/11/e20e1ef6.pdf).

[58] Section 9 Förordning (2007:261) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet (Decree 2007:261 on processing of personal data by the FRA).

[59] Section 9 Act 2008:717 on signals intelligence.

[60] NyTeknik, FRA:s metoder granskas efter ny avlyssningsskandal, 27 August 2008, cited in Klamberg, (2010), op. cit.

[61] Quoted in D. Landes (2013), "Sweden's Spy Links 'deeply troubling", *The Local*, 6 September.

[62] N. Nielsen (2013), "EU asks for answers on UK snooping programme", *EU Observer*, 26 June.

indication of whether Sweden has been the recipient of data from other states, including data from the NSA's PRISM and other mass-surveillance programmes.

2.3 Legal framework and oversight

2.3.1 Legal framework

The legal authorisation for Sweden signals intelligence-gathering operations are issued by an intelligence court (Underrättelsedomstolen - UNDOM). However, according to the legislative framework governing the issuing of warrants – namely Act 2008:717 on signals intelligence within defence intelligence operations, Act 2009:966 on the Intelligence Court, and Decree 2009:968 with instructions for the Intelligence court – warrants can be sweeping and are not limited to a specific individual.[63]

2.3.2 Oversight

The surveillance activities of the FRA are monitored by a national oversight body, the Inspection for Defence Intelligence Operations (Statens inspektion för försvarsunderrättelseverksamheten – SIUN) which is composed of representatives from the Government and Opposition parties.[64]

However, academic experts have critiqued the weak system of checks and balances when it comes to Swedish collection of signals intelligence. With regard to the UNDOM and the SIUN, Dr. Mark Klamberg contends:

> All of these institutions are under very tight control of the Government, an entity that can issue requests for signals intelligence operations. The intelligence court has one chief judge, one or two deputy chief judges. The judges are appointed by the Government. One of the three nominees for the next chief judge is currently the chief legal advisor at the Ministry of Defence. The current head of the signals intelligence agency was previously the chief legal advisor at the Ministry of Defence when the legislation was drafted. The members of SIUN do represent different political parties but are appointed by the Government and report to the Government. Most of the members of SIUN are former parliamentarians, which weakens the parliamentary oversight in comparison to a system where the responsibility for oversight is conducted by a committee of parliament, i.e. parliamentarians in office. All in all, the Swedish system of checks and balances is weak when it comes to signals intelligence.[65]

3. France[66]

Since 2008, France has been constantly improving its architecture for the large-scale collection of data, with the main intelligence agency in France, the DGSE (Direction générale de la sécurité extérieure) increasing its foreign intelligence capabilities in recent years.[67] A report of 30 April 2013 by the French National Assembly highlighted the fact that:

---

[63] Expert input by Dr. Mark Klamberg, Uppsala University. See Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet (Act 2008:717 on signals intelligence within defence intelligence operations), section 4(a); Lag (2009:966) om Försvarsunderrättelsedomstol (Act 2009:966 on Intelligence court); Förordning (2009:968) med instruktion för Försvarsunderrättelsedomstolen (Decree 2009:968) with instructions for the Intelligence court). For further information on the Swedish legal framework covering communications surveillance, see Klamberg, (2010), op. cit.

[64] Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet (Act 2008:717 on signals intelligence within defence intelligence operations), Sections 10 and (10(a); Förordning (2009:969) med instruktion för Statens inspektion för försvarsunderrättelseverksamheten (Decree 2009:969 with instructions for the Inspection for Defence Intelligence Operations).

[65] M. Klamberg (2013), Blogpost on EU Metadata Collection, Lawfare, 29 September (www.lawfareblog.com/2013/09/mark-klamberg-on-eu-metadata-collection).

[66] The data presented here were gathered on the basis of news articles and official documents and complemented by an interview with an expert academic source who wishes to remain anonymous.

[67] Assemblée Nationale (2013), Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2012, Rapport No. 1012 par Mme Patricia ADAM, Députée, Délégation parlementaire au renseignement, 30 April (www.assemblee-nationale.fr/14/rap-off/i1012.asp).

> Since 2008, progress has been made in terms of pooling of capabilities, in particular concerning electro-magnetic intelligence activities operated by the DGSE to benefit the entire intelligence community.[68]

In this report, the French MPs also suggested strengthening the data-collection structure of the DGSE and the links between all levels of intelligence.[69]

Experts consulted for this study claim that France now ranks fifth in the world of metadata collection after the US, the UK, Israel and China and runs the second-most important intelligence data collection and processing centre in Europe after the UK. Claims of this nature have been made publicly by Bernard Barbier, a Technical Director at the DGSE, in 2010.[70]

3.1 Programme(s) for large-scale surveillance

Reportedly, France's communications surveillance and collection architecture rest primarily on a supercomputer operated by the DGSE in Paris.[71] This super-computer intelligence centre, allegedly installed on three levels in the basement of the DGSE headquarters, is reported to be capable of collecting, processing and storing dozens of petabytes of data. Data are intercepted and collected by approximately 20 interception sites located on both national and overseas territory, comprised of both satellite stations and interception of fibre-optic submarine cables.[72]

In February and March 2013, the French National Assembly's Committee on National Defence and Armed Forces conducted hearings during which the heads of the main French intelligence services all confirmed the existence of a metadata intelligence centre located at the DGSE capable of intercepting and processing internet flows, social network and phone communications.[73] For instance, on 20 February 2013, the then Head of the DGSE, Érard Corbin de Mangoux, alluded to France's communications surveillance capabilities when he stated before the Committee:

> Regarding the technical means, we have at our disposal the entire capabilities for electro-magnetic intelligence. Following the recommendations of the 2008 White Paper, we have developed an important apparatus for intercepting Internet flows.[74]

Data storage appears to relate primarily to metadata from phone and internet use. Concerning the use of this information, evidence indicates that the metadata centre operated by DGSE forms an 'intelligence platform' that feeds a range of intelligence, defence and law enforcement bodies within France. The following six agencies have been cited as 'customers' of the DGSE metadata bank (named 'mutualisation infrastructure' by French officials):[75]

---

[68] Ibid. (The original text states "depuis 2008, des progrès ont été réalisés en matière de mutualisation des capacités, notamment en ce qui concerne le renseignement d'origine électromagnétique, opéré par la DGSE au profit de l'ensemble de la communauté du renseignement.")

[69] Ibid., pt. II.

[70] Speech by Bernard Barbier on 30 September 2010 at the French Association of Reservists for Ciphering and Information Security. His remarks were reported in a specialised blog article (http://bugbrother.blog.lemonde.fr/2010/10/02/frenchelon-la-dgse-est-en-1ere-division).

[71] J. Follorou and F. Johannes (2013), "Révélations sur le Big Brother français", *Le Monde*, 4 July.

[72] Follorou and Johannes (2013), Ibid.

[73] See Assemblée Nationale (2013), Commission de la défense nationale et des forces armées, Comptes-rendus n° 52, 54, 55, 56, 59 et 62 des réunions du 12 février, 13 février, 19 février, 20 février, 26 février et 13 mars 2013 respectivement (www.assemblee-nationale.fr/14/cr-cdef/12-13/index.asp).

[74] Hearing of Érard Corbin de Mangoux, Director-General of the DGSE, 20 February 2013, before the French National Assembly's Committee on National Defence and Armed Forces. See Assemblée Nationale (2013), Commission de la défense nationale et des forces armées, Compte-rendu No. 56 (www.assemblee-nationale.fr/14/cr-cdef/12-13/c1213056.asp). The original text states: "S'agissant des moyens techniques, nous disposons de l'ensemble des capacités de renseignement d'origine électromagnétique (ROEM). À la suite des préconisations du Livre blanc de 2008, nous avons pu développer un important dispositif d'interception des flux Internet."

[75] J. Follorou and F. Johannes (2013), " Révélations sur le Big Brother français", *Le Monde*, 4 July.

- National Directorate of Customs Intelligence and Investigations (DNRED), responsible for carrying out investigations on smuggling, counterfeit money and customs fraud;
- Directorate for Defence Protection and Security (DPSD), responsible for military counter-espionage;
- Directorate of Military Intelligence (DRM), tasked with centralising all military intelligence information;
- Central Directorate of Interior Intelligence (DCRI), soon to be replaced by the General Direction of Interior Security (DGSI), responsible for counter-espionage and counter-terrorism;
- TRACFIN service (Intelligence Analysis and Action against Clandestine Financial Circuits), responsible for the fight against illegal financial operations, money laundering and terrorism financing; and
- The intelligence arm of the Police Prefecture of Paris.

According to reports from Le Monde newspaper, these services send a request to the DGSE and the DGSE searches the database on a hit/no-hit basis. It then forwards intelligence reports on the basis of the data analysed to the client agencies.[76] This is allegedly carried out routinely, discreetly and without any form of parliamentary control.[77] According to a French Senat report, this logic of 'mutualisation' is long-standing:

> ...the logic of pooling of resources between services has been continued for several years. Therefore, the DGSE is specialised in communication interception and cryptography to the benefit of the entire intelligence community. The Directorate of Military Intelligence (DRM) is in charge of the observation satellites and radar signal surveillance. Approximately 80% of the annual budget of the DGSE is invested in projects linked to the other intelligence agencies.[78]

There are currently no confirmed reports or evidence that agreements exist between the French intelligence services and French telecommunications operators such as SFR, Bouygues, Orange etc. exist giving access to data traffic.[79]

3.2 Cooperation with foreign intelligence services

The French intelligence services engage in wide cooperation with foreign intelligence services. During the above-mentioned hearing, Head of DGSE Érard Corbin de Mangoux declared before the French Parliament that the Agency was working with more than 200 foreign services, among which 50 formed part of the 'second circle' engaged in 'frequent' collaboration, while 10 were considered part of a 'first circle' engaged in intense cooperation. The states with which the DGSE engages were not named, nor the nature of the cooperation detailed beyond a reference to joint analysis of information and research.[80] He added that, on the initiative of the US, western intelligence services have set up a database allowing each nation to immediately obtain access to all the information gathered.[81]

These statements supplement revelations from 2005 that, according to disclosures by the Washington Post, France has been hosting a secret intelligence centre in Paris named "Alliance Base" where six countries,

---

[76] Follorou and Johannes (2013), Ibid.

[77] Input by anonymous expert.

[78] See Sénat (2013), Projet de loi de finances pour 2013 - Défense : environnement et prospective de la politique de défense, Avis n° 150 (2012-2013) de MM. Jeanny LORGEOUX et André TRILLARD, 22 November 2012, paragraph III a) 1) d) (www.senat.fr/rap/a12-150-5/a12-150-5.html) (original text: « Cet effort s'effectue dans la logique de mutualisation des moyens entre services retenue depuis plusieurs années. Ainsi, la DGSE est spécialisée sur l'interception des communications et la cryptologie, au bénéfice de l'ensemble de la communauté du renseignement. La direction du renseignement militaire (DRM) met en oeuvre quant à elle les satellites d'observation et les moyens d'écoute des signaux radar. Environ 80 % du budget annuel d'investissement de la direction technique de la DGSE financent des projets intéressant également d'autres organismes. »)

[79] *Source*: Statement by Jacques Follorou at the European Parliament's LIBE Committee Inquiry on Inquiry on Electronic Mass Surveillance of EU Citizens, 1st Hearing, 5 September 2013.

[80] *Source*: Assemblée Nationale (2013), Compte-rendu no. 56, op. cit.

[81] Ibid. The original statement was « Ainsi à l'initiative des Américains, les services occidentaux ont mis en place une base de données permettant à chacun de disposer immédiatement de l'ensemble des informations recueillies »

namely USA, UK, France, Germany, Canada and Australia routinely exchange information.[82] It was reported that Alliance Base is headed by a French general assigned to the DGSE and hosts case officers from Britain, France, Germany, Canada, Australia and the United States. Alliance base is believed to have ended in 2009 due to tensions between the French and the US.[83]

3.3 Legal framework and oversight

3.3.1 Legal framework

Electronic surveillance is regulated by the Code de la Sécurité Intérieure, a legislative code established in 2012 and regrouping various laws and rules related to French internal security.[84] The specific rules on "security intercepts" (interceptions de sécurité) can be found in Book 2, Title IV of this Code. They strictly regulate security intercepts authorised by the Prime Minister on the advice of the National Advisory Commission on security intercepts (CNCIS), an independent administrative authority reviewing surveillance requests. The Code de la Sécurité Intérieure abrogated a 1991 law on secrecy of correspondence[85] which had, until 2012, regulated the conditions for wiretaps (which required permission of an investigative judge). The new Code was strongly criticised by the CNCIS in its activity report[86] for including security intercepts in a broader and vaguer package of rules along with, for instance, "security in public transportation" or "security guards in buildings". The report underlined the fact that any exception to the right to secrecy of correspondence should be provided for in a specific law and not in a code.[87]

In addition, a new Anti-Terror Act enacted on 23 January 2006[88] granted increased powers to the police and intelligence services, allowing them to get telecom data directly from ISPs and extended telecom data retention possibilities.

The law strictly regulates security intercepts authorised by the Prime Minister on the advice of the National Advisory Commission on security intercepts (CNCIS). However, there is a gap in the legal framework regarding the large-scale interception and storage of data, leaving a degree of legal uncertainty which intelligence services appear to have exploited. Hence a senior member of the intelligence services interviewed by Le Monde journalists is reported to have claimed that collection of meta-data by DGSE is not illegal but 'alegal' – conducted 'outside the law'.[89] This was however contrasted by the CNIL, the independent body which stated that:

> Le régime juridique des interceptions de sécurité interdit la mise en œuvre par les services de renseignement, d'une procédure telle que Prism. Chaque demande de réquisition de données ou d'interception est ciblée et ne peut pas être réalisée de manière massive, aussi quantitativement que temporellement. De telles pratiques ne seraient donc pas fondées légalement.[90]

---

[82] *Source*: D. Priest (2013), "Help From France Key In Covert Operations", Washington Post, 3 July 2005.

[83] Source: D. Servenay (2010), «Terrorisme: pourquoi Alliance Base a fermé à Paris », Rue89, 24 May 2010 (http://www.rue89.com/2010/05/24/terrorisme-fermeture-dalliance-base-a-paris-152349).

[84] Available (in French) (http://bit.ly/1dimLYp).

[85] Loi no 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques.

[86] See Commission nationale de contrôle des interceptions de sécurité (2012), 20e rapport d'activité 2011-2012, Paris.

[87] Ibid., p. 38: "S'agissant de dispositions portant sur la protection des libertés publiques, il résulte des travaux parlementaires ayant conduit à l'adoption, tant de la loi n° 91-646 du 10 juillet 1991 que de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme, que la consecration législative du secret des correspondances électroniques privées, ainsi que les exceptions à ce principe, doivent être prévues par une loi spéciale, comme pour toute liberté publique. Or ces dispositions se retrouvent désormais fondues dans un vaste ensemble normatif couvrant des domaines multiples et variés."

[88] Loi No. 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

[89] *Source*: J. Follorou and F. Johannes (2013), 'Révélations sur le Big Brother français,' *Le Monde*, 4 July 2013; See also testimony of Jacques Follorou, EP Hearing 5 September 2013.

[90] *Source*: J. Follorou and F. Johannes (2013), 'Révélations sur le Big Brother français,' *Le Monde*, 4 July 2013.

3.3.2 Oversight

Parliamentary oversight over communications surveillance in France is deemed to be relatively weak.[91] First, because all requests for classified documents from parliamentary committees to intelligence services are rejected since all data transmitted by a foreign service remain property of the service to which the data have been directed. A senator or representative has no right to hear or question a member of a defined intelligence service. The directors of intelligence agencies can only be subjected to official hearings.[92]

The main body responsible for the oversight of interception surveillance in France is the CNCIS (Commission nationale pour les interceptions de securité).[93] The CNCIS is mandated to exert an a priori control on security interceptions (wiretapping) and to assess whether the purpose of the interception meets principles of proportionality etc. However, its reach is judged to be substantially constrained by its limited personnel (only five members),[94] budget and administrative capacity.[95] Moreover it is doubtful that it has been routinely consulted (if at all) during the DGSE's metadata collection activities.[96]

It is relevant here to note that two French human rights NGOs are attempting to launch an official judicial investigation into the surveillance scandals in France. The Paris prosecutor's office has opened a preliminary inquiry following the submission of a joint complaint by the NGOs Fédération internationale des droits de l'homme (FIDH) and Ligue des droits de l'homme (LDH) on 11 July 2013.[97] Both NGOs claim that infringements of personal liberties have taken place through automated data processing. On the basis of the French Criminal Code, they challenge the fraudulent access to an automated data processing system, collection of personal data by fraudulent means, wilful violation of the intimacy of the private life and the use and conservation of recordings and documents obtained through such means.

4. Germany[98]

Evidence gathered on the surveillance activities of the German intelligence services also indicate that Germany has been engaging in large-scale surveillance of communications data, and that these activities are linked to a network of exchange and transfer of data with both domestic intelligence and law enforcement agencies as well as with international partners, despite the existence of a strong constitutional and legal framework for the protection of privacy.

4.1 Programme(s) for large-scale surveillance

At the centre of the allegations concerning German large-scale surveillance activities is the Bundesnachrichtendienst (BND) or Federal Intelligence Service which is responsible for conducting foreign intelligence analysis and electronic surveillance of 'threats to German interests' from abroad. It employs approximately 6,500 persons and had a budget of €504.8 million for the year 2012.[99] However, also

---

[91] A. Wills et al. (2011), *Parliamentary oversight of security and intelligence agencies in the European Union*, Study for LIBE Committee of the European Parliament.

[92] *Source*: input of anonymous expert.

[93] CNCIS was established by the law of 10 July 1991 on secrecy of correspondence via electronic communication.

[94] Composed of both Parlementarians and judges.

[95] A. Wills et al. (2011), *Parliamentary oversight of security and intelligence agencies in the European Union*, Study for LIBE Committee of the European Parliament; Statement by Jacques Follorou at the European Parliament's LIBE Committee Inquiry on Inquiry on Electronic Mass Surveillance of EU Citizens, 1st Hearing, 5 September 2013; CNCIS (2012), *CNCIS: 20e rapport d'activité 2011 – 2012* (http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/134000156/0000.pdf).

[96] *Source*: input of anonymous expert.

[97] See C. Labbe and N. Vinocur (2013), "French prosecutor investigates U.S. Prism spying scheme", Reuters, 28 August 2013 (www.reuters.com/article/2013/08/28/us-usa-security-france-idUSBRE97R0WE20130828). See also the official complaint on the website of the FIDH (www.fidh.org/en/europe/France,568/fidh-and-ldh-file-a-complaint-for-infringement-of-personal-data-13648).

[98] Data presented in this section have been gathered primarily on the basis of press reports and official documentation (e.g. Parliamentary questions, reference to official legal texts and case law).

[99] The number of employees for the BND is mentioned on the BND's website (www.bnd.bund.de/DE/Karriere/Allgemeine%20Informationen/Allgemeine%20Informationen_node.html), the budget of the BND can be

implicated are the Militärischen Abschirmdienst (MAD) the Military Counterintelligence Service[100] and the Bundesamt für Verfassungsschutz (BfV) the Federal Office for the Protection of the Constitution which is tasked with "intelligence-gathering on threats concerning the democratic order, the existence and security of the federation or one of its states, and the peaceful coexistence of peoples; with counter-intelligence; and with protective security and counter-sabotage". The latter is under the responsibility of the Ministry of Interior and specific regional offices exist in all 16 Länder. The BfV employed 2,757 persons and had a budget of €210 million in 2012.[101]

According to the information available to the public, the BND operates a service capable of **directly connecting to digital traffic nodes** through which most of the foreign communications flow.[102] This is legally authorised by the G-10 Law (see below) which allows the three intelligence agencies mentioned above (the BND, the MAD and the BfV) to search up to 20% of communications having a foreign element according to certain keywords for specific purposes such as the fight against terrorism or the protection of the Constitution.[103]

In terms of data flows, the biggest node in Germany – and, according to certain figures, in the world – is the DE-CIX (German Commercial Internet Exchange) in Frankfurt.[104] According to the Spiegel newspaper, the BND has set up special offices at this location to divert incoming traffic, copy the data and analyse it later in the BND headquarters in Pullach, Bavaria.[105] This was confirmed by a reply to a parliamentary question by the government,[106] as well as by Germany's Justice Minister Sabine Leutheusser-Schnarrenberger and by the head of the G-10 Committee Hans De With.[107] The gathered data is then analysed through the use of keywords and selectors on terrorism.[108]

According to the Spiegel,

> Via this hub, the largest in Europe, e-mails, phone calls, Skype conversations and text messages flow from *regions that interest the BND like Russia and Eastern Europe*, along with crisis areas like *Somalia*, countries in the *Middle East*, and states like *Pakistan* and *Afghanistan*.[109] (Emphasis added)

---

found in the Official federal budget for 2012, Section 04 (www.bundesfinanzministerium.de/bundeshaushalt2012/pdf/epl04.pdf), p.21.

[100] German Ministry of Interior (2013) Verfassungsschutzbericht 2012, BMI 13006, p. 13, (www.verfassungsschutz.de/embed/vsbericht-2012.pdf).

[101] Ibid.

[102] *Source*: P. Beuth (2013), 'Wie der BND das Netz überwacht', Zeit Online, 18 June 2013 (www.zeit.de/digital/datenschutz/2013-06/internet-ueberwachung-bnd).

[103] The G-10 Law, in its § 10(4), states "In den Fällen der §§ 5 und 8 sind die Suchbegriffe in der Anordnung zu benennen. Ferner sind das Gebiet, über das Informationen gesammelt werden sollen, und die Übertragungswege, die der Beschränkung unterliegen, zu bezeichnen. Weiterhin ist festzulegen, welcher Anteil der auf diesen Übertragungswegen zur Verfügung stehenden Übertragungskapazität überwacht werden darf. In den Fällen des § 5 darf dieser Anteil höchstens 20 vom Hundert betragen." (www.gesetze-im-internet.de/g10_2001/BJNR125410001.html)

[104] D. Weller and Woodcock, B. (2013), 'Internet Traffic Exchange: Market Developments and Policy Challenges'. *OECD Digital Economy Papers*, 207, p. 41.

[105] *Source*: Spiegel Online (2013) '100-Millionen-Programm: BND will Internet-Überwachung massiv ausweiten', 16 June 2013 (www.spiegel.de/politik/deutschland/internet-ueberwachung-bnd-will-100-millionen-investieren-a-905938.html).

[106] German Parliament (2012) Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan Korte, Jan van Aken, weiterer Abgeordneter und der Fraktion DIE LINKE - „Strategische Fernmeldeaufklärung" durch Geheimdienste des Bundes, Drucksache 17/9640 (http://dip21.bundestag.de/dip21/btd/17/096/1709640.pdf).

[107] See M. Ermert (2013), "PRISM scandal: internet exchange points as targets for surveillance", H-Online, 2 July 2013 (www.h-online.com/security/news/item/PRISM-scandal-internet-exchange-points-as-targets-for-surveillance-1909989.html).

[108] *Source*: Spiegel Online (2013) 'The German Prism: Berlin Wants to Spy Too', 17 June 2013 (www.spiegel.de/international/germany/berlin-profits-from-us-spying-program-and-is-planning-its-own-a-906129-2.html).

[109] Ibid.

The same article mentions that the head of the BND, Gerhard Schindler, recently requested an increase in the BND's budget of €100 million for the next five years in order to hire new agents and improve the technological surveillance capabilities. This modernisation project has been given the name of "Technikaufwuchsprogramm" (which can be translated into "Technological Coming-of-age Programme").[110] Several sources of information hint at a possible German system collecting data through private companies, similar to the US PRISM programme. Private companies such as Internet service providers allegedly copy the data requested by the BND on its special servers. The hardware and software architecture used in that case could be the so-called 'SINA-box' which is a means of transferring sensitive data in unsecure environments.[111]

It is also worth mentioning that the Federal Police has set up a computerised architecture called 'INPOL-neu' which contains millions of data extracted from police and judicial investigations and from the SIS database. Intelligence services have complete access to the INPOL database, which is also linked to the Europol Information System (EIS).

As seen in the French case, there is considerable pooling of resources/data exchange between the various German intelligence and law enforcement bodies. Since 2001 the three intelligence services have been authorised to extend their domain of investigation in terms of information collection, analysis and dissemination and may exchange information between themselves as well as with police agencies, something which was once regulated and restricted by federal laws.

In particular, the **MAD** has been allowed to collect information on the national borders and exchange information with the two other intelligence services, which has broken the long established German tradition of complete separation between a military intelligence service and its civilian counterparts.

Concerning police-intelligence cooperation, it is interesting to note that the **BfV** has implemented a common database on Islamic terrorism with the Federal Criminal Police Office (Bundeskriminalamt, BKA), a first tool bridging the historical gap between federal police and secret service. A recent bill also extended the powers of the BKA to secretly gather data on private computers through the use of highly specialised software (so called "Bundestrojaner" or Federal Trojan Horses) for the purposes of criminal investigations.[112] It is also worth noting the existence of integrated police services that have been set up at federal level to boost data exchange and analysis at all levels, such as the GTAZ (Gemeinsames Terrorismusabwehrzentrum). The GTAZ, located in Berlin, is aiming at strengthening national cooperation between Länder and State, i.e. between regional and federal police forces, the military, the customs, intelligence services, financial services, and at fostering international cooperation against Islamic terrorism.

4.2 Cooperation with foreign intelligence services

Reports publishing the Snowden revelations concerning German surveillance programmes such as the Spiegel, also highlighted evidence regarding cooperation between the German intelligence services and their US counterparts.

Allegedly, millions of metadata collected by the BND were transferred to the NSA via data collection sites on German territory:

> The Snowden documents mention two data collection sites known as signals intelligence activity designators (SIGADs), through which the controversial US intelligence agency gathered about 500 million pieces of metadata in December 2012 *alone*. The code names cited in the documents are "US-987LA" and "US-987LB." The BND now believes that the first code name stands for Bad Aibling. Day after day and month after month, the BND passes on to the NSA massive amounts of connection data relating to the communications it had placed under surveillance. The so-called

[110] Ibid.

[111] *Source*: P. Beuth (2013), "Wie der BND das Netz überwacht", op. cit.

[112] See Federal Office of Crime Prevention Act (Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten, BKA-Gesetz) (www.gesetze-im-internet.de/bkag_1997/).

> *metadata* -- telephone numbers, email addresses, IP connections -- then flow into the Americans' giant databases.[113]

The same article underlines the fact that copies of two pieces of software developed by the German BND have also been given to NSA agents: "Mira4" and "Veras".[114] These two programmes are allegedly similar in nature to the US XKeyscore system, but there is a clear lack of information on the functions and scope of such software. According to the Spiegel information, the NSA and the BND jointly presented the XKeyscore programme to the civilian Bundesamt für Verfassungsschutz in 2011. Also, according to disclosures by the Washington Post, Germany participates in meetings in the framework of the secret intelligence "Alliance Base" in France, mentioned above, along with US, UK, French, Canadian and Australian representatives which routinely exchange information.[115]

Many articles mention the long history of data exchanges between Germany and its Western allies, mostly during the Cold War in the 1960s but also after the 9/11 attacks.[116] Bilateral data transfer agreements with the former powers that occupied West Germany – United States, UK and France – have recently been cancelled following the PRISM scandal. These agreements included a task foreseen for the German intelligence agencies to spy on post and radio communications for the purpose of protecting Western troops stationed in Germany.[117]

4.3 Legal framework and oversight

4.3.1 Legal framework

Article 10 of the German Constitution on the privacy of correspondence, posts and telecommunications states:

> 1) The privacy of correspondence, posts and telecommunications shall be inviolable.
>
> 2) Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a Land, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature.[118]

The main federal law in Germany regulating communications surveillance is the G-10 Law, which allows for certain limitations to the secrecy of communications as provided in the Article 10 of the Constitution.[119] Under the G-10 Law, intelligence services may operate warrantless automated wiretaps of domestic and international communications for specific purposes such as the fight against terrorism or the protection of the Constitution. The G-10 Law was amended in 1994 and 2001 to add electronic and voice communications to the list of communications that intelligence agencies may monitor. Also, the law in its paragraph 10 allows the BND to search up to 20% of foreign communications according to certain keywords – these communications include telephone conversations, e-mails, chats etc.

Two major decisions of the German Federal Constitutional Court have limited the scope of the G-10 Law in recent years:

---

[113] *Source*: H. Gude, L. Poitras and M. Rosenbach, "Mass Data: Transfers from Germany Aid US Surveillance", Spiegel Online, 5 August 2013 (www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html).

[114] Ibid.

[115] *Source*: Priest (2013), "Help From France Key In Covert Operations", op. cit.

[116] *Source*: M. Eddy, "For Western Allies, a Long History of Swapping Intelligence", *New York Times*, 9 July 2013 (www.nytimes.com/2013/07/10/world/europe/for-western-allies-a-long-history-of-swapping-intelligence.html).

[117] Der Standard, "Deutschland beendet Geheimdienst-Abmachung mit Frankreich", 6 August 2013 (http://derstandard.at/1375625808305/Deutschland-beendet-Geheimdienst-Abmachung-mit-Frankreich).

[118] See the translated version of the German Grundgesetz (http://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html).

[119] The full text of the G-10 Law is available online (in German) (http://www.gesetze-im-internet.de/g10_2001/BJNR125410001.html).

- In March 2004, the Court ruled that the G-10 Law infringed the German Constitution, especially its Article 1 on human dignity and Article 13 on the inviolability of private homes.[120] The court held that certain communications, such as contacts with close family members, doctors, priests or lawyers, are protected by an absolute area of intimacy that no government may infringe.
- In February 2008, in a landmark decision, the Court declared certain provisions of a regional law unconstitutional.[121] The regional law (of North-Rhine Westphalia) allowed the regional Office for the Protection of the Constitution to secretly gather data on private computers. The Court interpreted Articles 1 and 2 of the German Constitution as containing a fundamental right for every citizen to have the integrity and confidentiality of IT systems guaranteed by the state. The possibility of secret online searches on computers is not categorically ruled out – the Court specified that such measures can only be justified under strict conditions and when there is an imminent threat to the life, physical integrity or liberty of persons, or to the foundations of the state or the existence of mankind.

4.3.2 Oversight

Two oversight bodies exist at Parliamentary level for controlling the activities of German intelligence services:

- The G-10 Committee is a committee of the German Parliament (Bundestag) which has the task to decide on the necessity and legitimacy of the measures taken by the three intelligence agencies mentioned above which could infringe upon the fundamental rights enshrined in Article 10 of the German Constitution.[122] It is composed of 4 Members of the German Parliament. The G-10 Committee is triggered when an intelligence service makes an official request for a surveillance measure to the German Ministry of Interior and this request is granted. The G-10 also follows the whole procedure, including the collection of the personal data, its analysis and its use. The G-10 also checks whether fundamental rights of German citizens have been violated following individual complaints. Compared with oversight authorities in the USA and in other member states examined in this briefing paper, the German G-10 is the only oversight body that does not only authorise surveillance requests, but also checks how the collection, storage, and analysis of personal data is carried out, investigate individual complaints and holds responsibility for the implementation of the surveillance programmes.[123]
- The PKGr – Parliamentary Control Committee is the oversight body responsible for controlling the three federal intelligence services mentioned above.[124] The German government is obliged to inform the PKGr and to provide all relevant information on the activities of the intelligence agencies to its members. The PKGr is composed of 11 Members of Parliament. According to a recent report by the PKGr on the 2011 activities of the BND, more than 2,9 million of e-mails and text messages have been the subject of surveillance measures.[125]

In parallel to these two oversight authorities, several other official bodies may have an influence on the ways in which the intelligence services operate in Germany:

---

[120] Federal Constitutional Court (Bundesverfassungsgericht) decision of 3 March 2004, reference number: 1 BvR 2378/98 (http://www.bverfg.de/entscheidungen/rs20040303_1bvr237898.html) (in German).

[121] Federal Constitutional Court (Bundesverfassungsgericht) decision of 27 February 2008, reference number: 1 BvR 370/07 (www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html) (in German);

[122] http://www.bundestag.de/bundestag/gremien/g10/index.html

[123] Refer to S. Heumann and B. Scott (2013), "Law and Policy in Internet Surveillance Programs: United States, Great Britain and Germany", Stiftung Neue Verantwortung, Berlin and Open Technology Institute of the New America Foundation, Washington, D.C., September.

[124] http://www.bundestag.de/bundestag/gremien/pkgr/index.jsp

[125] German Parliament (2013), Unterrichtung durch das Parlamentarische Kontrollgremium (PKGr) - Bericht gemäß § 14 Absatz 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10) über die Durchführung sowie Art und Umfang der Maßnahmen nach den §§ 3, 5, 7a und 8 dieses Gesetzes - (Berichtszeitraum 1. Januar bis 31. Dezember 2011), Drucksache 17/12773, 14 March 2013, available at: http://dip21.bundestag.de/dip21/btd/17/127/1712773.pdf (in German).

- Committee on Budget of the Bundestag (Haushaltsausschuss),[126]
- Courts at national and regional levels,
- Federal Court of Auditors (Bundesrechnungshof)[127] and
- Data Protection Authority (Federal Commissioner for Data Protection and Freedom of Information).[128]

German data protection bodies at the federal and the regional levels have, in a joint statement, called for increasing the control powers of the two German oversight bodies and strengthening the links with data protection authorities.[129]

5. The Netherlands[130]

There are currently no publicly disclosed programmes of mass cyber surveillance in the Netherlands. Current discussions around large-scale surveillance are limited to expert arenas and are linked to the mandate and capabilities of a new Sigint and Cyber agency, the Joint Sigint Cyber Unit (JSCU) to be established in 2014.

5.1 (Potential) programmes for large-scale surveillance

The Joint Sigint Cyber Unit (JSCU), codenamed 'Project Symbolon', will start to function in 2014.[131] The unit was announced as part of the Dutch Ministry of Defence's Cyber Strategy in 2012[132] as a joint effort of the AIVD (General Intelligence and Security Service) and MIVD (Military Intelligence and Security Service). It will replace the current National Signals Intelligence Organisation (NSO), also created with staff from AIVD and MIVD in 2003.

The JSCU is expected to centralise all Signals and Cyber surveillance in the Netherlands[133] and will have a staff of 350.[134] Its headquarters should be located in the offices of the AIVD in Zoetermeer, while other departments will be located in MIVD premises in The Hague. The signals location in Burum and the analysis location in Eibergen, currently operated by the NSO, will stay active.[135]

There is currently little knowledge about the budget that will be dedicated to the JSCU. Project Argo II (establishment of the agency) has a budget of €17 million[136].

Concerning the objectives of the new agency, traditionally, Dutch SIGINT activities have focused on supporting military missions abroad and increasingly on counterterrorism activities,[137] but their official mandate also includes non-security related tasks, such as the collection of economic intelligence. The official objectives of the new agency are both defensive and offensive cyber activity. Offensive activities are being

---

[126] See http://www.bundestag.de/bundestag/ausschuesse17/a08/index.jsp

[127] http://www.bundesrechnungshof.de/en?set_language=en

[128] http://www.bfdi.bund.de/EN/Home/homepage_node.html

[129] See the joint statement at http://bit.ly/17yD7nn

[130] The data presented here was gathered on the basis of news articles, checked and complemented by interviews with the following experts: Ot van Daalen, Bits of Freedom, 9/10/2013; Jelle van Buuren, Leiden University, Center for Terrorism and Counter-terrorism 10/10/2013; Axel Arnbak, cybersecurity and information law researcher at the Institute for Information Law, University of Amsterdam, 14/10/2013.

[131] The renovation operation was codenamed "Argo II". A description of the project can be found on the Dutch Rijks ICT-Dashboard website (http://bit.ly/18Pqw32).

[132] Netherlands Ministry of Defence, *The Defense Cyber Strategy*, The Hague, September 2012 (http(://bit.ly/GIGC4O).

[133] Letter of the Dutch Ministry of Interior to Dutch MP Van Raak, 21/06/2013, available on the website of the NGO Bits of Freedom (http://bit.ly/18PpGn3).

[134] NRC Handelsblad, 24/09/2013 (translation in English available at http://bit.ly/1hwMyK2).

[135] NRC Handelsblad, 24/09/2013 (translation in English available at http://bit.ly/1hwMyK2).

[136] Dutch Rijks ICT-Dashboard (http://bit.ly/18Pqw32).

[137] The need for autonomous Dutch SIGINT was made particularly pressing after the debacle of the 'Dutchbat' (Dutch Battalion under the command of the United Nations Protection Force) in Srebrenica during the war in Bosnia-Herzegovina, which was largely based on misleading intelligence. Source: Interview with Axel Arnbak.

justified by recent cyber-attacks, such as the compromising of the security of government services by the hijacking of electronic signatures issued by certificate authority DigiNotar.[138]

The official objectives of the program, as reported in the 2012 Cyber Strategy prepared by the Ministry of Defence,[139] are the following:

- Infiltration of computers and networks to acquire data: mapping out relevant sections of cyberspace; monitoring vital networks; gaining a profound understanding of the functioning of and technology behind offensive cyber assets.
- The gathered information will be used for: early-warning intelligence products; the composition of a cyber threat picture; enhancing the intelligence; production in general; conducting counterintelligence activities.
- Cyber intelligence capabilities cannot be regarded in isolation from intelligence capabilities such as: signals intelligence (SIGINT); human intelligence (HUMINT) and the MIVD's existing counterintelligence capability.

At the moment, SIGINT activities in the Netherlands are limited to targeting specific individuals, both citizens and non-citizens, domestically and abroad. The MIVD is responsible for overseas SIGINT, while the AIVD is responsible for domestic targeted searches.

As mentioned previously, Dutch intelligence agencies are prohibited from conducting mass cable surveillance. Telecommunication interceptions are focused on individuals, and have to receive ministerial approval. In the meantime, both the AIVD and the MIVD working within the NSO are allowed to collect and store internet communications. This data can be searched through queries and keywords, but these also need to receive prior ministerial approval. It is worth noting however the potential for large-scale surveillance that the Netherlands holds given that the Amsterdam Internet Exchange Point (IXP) is the second largest in Europe after Frankfurt.[140]

The information currently gathered by the NSO and in the future by the JSCU will be available to both AIVD and the MIVD. It is not known yet which other law enforcement agencies will have access to the information produced by the JSCU.

Concerning the involvement of private actors, Dutch MP Ronald Van Raak has asked the Ministry of Interior and Kingdom Relations to comment on the alleged involvement of private sector companies in project Argo II: NICE Systems, an Israeli firm specialising in cyber security, and Accenture, an American consulting firm. It also asked the government about the role of the Amsterdam Internet Exchange (AMS-IX)[141]. In its response to van Raak, the Dutch Ministry of Interior and Kingdom Relations did not confirm the involvement of NICE Systems nor Accenture, invoking national security reasons: "The functional specifications of the platform give insight into the modus operandi of the MIVD and are therefore classified state secret"[142]. It has also implicitly denied that the Amsterdam Internet Exchange (AMS-IX) was involved in the project stating that there was "no involvement of a supplier, either directly or through subsidiaries, in the collection of Sigint"[143].

Ot van Daalen, from the the Dutch Digital Rights organisation Bits of Freedom (BoF) has however recently raised concerns about the vulnerability of the AMS-IX to Dutch and US intelligence services: First, he raised concern over the fact that in a recent parliamentary hearing AMS-IX "did not consider the Dutch secret

---

[138] NRC Handelsblad, 24/09/2013. (translation in English available at http://bit.ly/1hwMyK2).

[139] Netherlands Ministry of Defense, *The Defense Cyber Strategy*, The Hague, September 2012 (http://bit.ly/GIGC4O).

[140] D. Weller and B. Woodcock (2013), "Internet Traffic Exchange: Market Developments and Policy Challenges", *OECD Digital Economy Papers* No.207, OECD, Paris, p. 41.

[141] Questions of Dutch MP Ronald van Raak to the Dutch Ministry of Interior: "Vragen gesteld door de leden der Kamer" - 2013Z11570 - kv-tk-2013Z11570 http://bit.ly/1bVlUsb Accessed 9/10/2013

[142] Translated excerpts from the letter of the Dutch Ministry of Interior to Dutch MP Van Raak. 21/06/2013 Available on the website of the NGO Bits of Freedom http://bit.ly/18PpGn3 Accessed 9/10/2013

[143] Idem

services to be part of its threat model"[144]. Second, he found AMS-IX project to expand to the US a worrying prospective, arguing that "one of the most significant worries brought forward by members is that the NSA by this expansion would be legally authorised to gain access to data handled on the Dutch AMS-IX"[145]. According to AMS-IX, which has confirmed its expansion in the US, the new legal structure of the firm should however separate US-based activities and EU-based activities[146].

5.2 Cooperation with foreign intelligence services

Anonymous sources from the Dutch intelligence agencies have told the Telegraaf newspaper that the AIVD has routine access to information from the NSA "within five minutes".[147] This would allegedly allow Dutch intelligence services to have access to information on Dutch individuals from the US PRISM programme without the need for an express warrant as required by Dutch law. The Dutch Parliament has launched an inquiry into the role of the AIVD in this context to assess whether they have used private data obtained through the NSA's activities.[148] Dutch officials such as Home Affairs Minister Ronald Plasterk have denied that AIVD and MIVD make direct use of the PRISM programme.[149] The Dutch government also released an official statement rebuffing the allegation.[150]

5.3 Legal framework and oversight

5.3.1 Legal framework

The current legislative framework the Dutch Intelligence and Security Act 2002 (Wiv 2002) does not permit the services to wiretap "cable-bound communications" under any circumstances.[151] The establishment of the JSCU will therefore require a modification of the law. A commission, headed by C.W.M. Dessens, has been established to investigate if and under which conditions should the law be modified.[152] The conclusions of the commission, initially expected in September 2013, are likely to be made public before the end of 2013.[153] On the basis of the composition of the commission, two of our respondents suggested that it is likely that the law will be amended to permit the tapping of cable-bound communications.

5.3.2 Oversight

Currently, wiretapping activities require the approval of the minister of interior, who signs off all wiretapping orders. The main institution in charge of the monitoring of the AIVD and MIVD activities is the CTIVD (Review Committee on the Intelligence and Security Services). The CTIVD does not have direct access to all activities of the services, but is allowed to "sample" some of their activities for compliance. A

---

[144] Van Daalen, Ot (2013), "Considerations on the Expansion of AMS-IX to the US" *Bit of Freedom*, http://bit.ly/1b94w1J Accessed 9/10/2013

[145] Idem

[146] "Structuur nieuwe AMS-IX entiteit in de VS gekozen" 23/10/213 http://bit.ly/1b978N3 Accessed 5/11/2013

[147] *Source:* B. Olmer, "Ook AIVD bespiedt internetter", *De Telegraaf*, 11 June 2013 (www.telegraaf.nl/binnenland/21638965/__Ook_AIVD_bespiedt_online__.html See also the official condemnation by the Dutch digital rights organization Bits of Freedom « Persbericht: Bits Of Freedom Eist Einde Gebruik Prism Door Nederlandse Geheime Diensten » http://bit.ly/HeBh6l Accessed 10/10/2013).

[148] *Source:* Amsterdam Herald, "Inquiry into role of Dutch intelligence agencies in Prism data harvesting scandal", *The Amsterdam Herald*, 3 July 2013 (http://amsterdamherald.com/index.php/rss/906-20130703-inquiry-role-dutch-intelligence-agencies-prism-data-harvesting-scandal-united-states-nsa-europe-aivd-mivd-netherlands-dutch-security).

[149] See A. Eigenraam, "Plasterk: Nederland maakt geen gebruik van Prism", 21 June 2013, NRC Handlesblad (www.nrc.nl/nieuws/2013/06/21/plasterk-nederland-maakt-geen-gebruik-van-prism/).

[150] See www.rijksoverheid.nl/nieuws/2013/06/21/geen-onbelemmerde-toegang-tot-internet-en-telefoon-voor-aivd-en-mivd.html

[151] NRC Handelsblad, 24 September 2013 (translation in English available at http://bit.ly/1hwMyK2).

[152] The commission is composed of Luitenant-generaal b.d. M.A. Beuving; prof. dr. mr. E.R. Muller; vice-admiraal b.d. W. Nagtegaal; mr. H.J.I.M. de Rooij; prof. mr. W.M.E. Thomassen; prof. dr. W.J.M. Voermans. See "Regeling instelling Evaluatiecommissie Wiv 2002" (http://bit.ly/18PuM2J).

[153] NRC Handelsblad, 24/09/2013 (translation in English available at http://bit.ly/1hwMyK2).

recent report showed that when the committee looked into the compliance in the context of international SIGINT assistance, "it found that such assessments were not always made properly".[154]

There is currently no information about the structure of checks and balances that will apply to the new JSCU, although it is likely that it will fall under CTIVD mandate.

[154] See CTIVD, "Toezichtsrapportage inzake de inzet van SIGINT door de MIVD", CTIVD nr. 28, 23 August 2011, pp. 59-60. Quoted in Hoboken, Arnbak, van Eijk (2013) "Obscured by Clouds, or How to Address Governmental Access to Cloud Data from Abroad", pPaper presented at the Privacy Law Scholars Conference 2013, 6-7 June, Berkeley, CA. (http://bit.ly/18PxyVK); see also the most recent report of the CTIVD, "TOEZICHTSRAPPORT inzake de inzet van de afluisterbevoegdheid en de bevoegdheid tot de selectie van Sigint door de AIVD", July 2013 (http://bit.ly/H1KA8R).

ABOUT CEPS

Founded in Brussels in 1983, the Centre for European Policy Studies (CEPS) is widely recognised as the most experienced and authoritative think tank operating in the European Union today. CEPS acts as a leading forum for debate on EU affairs, distinguished by its strong in-house research capacity, complemented by an extensive network of partner institutes throughout the world.

Goals

- Carry out state-of-the-art policy research leading to innovative solutions to the challenges facing Europe today,
- Maintain the highest standards of academic excellence and unqualified independence
- Act as a forum for discussion among all stakeholders in the European policy process, and
- Provide a regular flow of authoritative publications offering policy analysis and recommendations,

Assets

- Multidisciplinary, multinational & multicultural research team of knowledgeable analysts,
- Participation in several research networks, comprising other highly reputable research institutes from throughout Europe, to complement and consolidate CEPS' research expertise and to extend its outreach,
- An extensive membership base of some 132 Corporate Members and 118 Institutional Members, which provide expertise and practical experience and act as a sounding board for the feasibility of CEPS policy proposals.

Programme Structure

In-house Research Programmes

Economic and Social Welfare Policies
Financial Institutions and Markets
Energy and Climate Change
EU Foreign, Security and Neighbourhood Policy
Justice and Home Affairs
Politics and Institutions
Regulatory Affairs
Agricultural and Rural Policy

Independent Research Institutes managed by CEPS

European Capital Markets Institute (ECMI)
European Credit Research Institute (ECRI)

Research Networks organised by CEPS

European Climate Platform (ECP)
European Network for Better Regulation (ENBR)
European Network of Economic Policy Research Institutes (ENEPRI)
European Policy Institutes Network (EPIN)