EUROPEAN PARLIAMENT 2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs

12.12.2013

WORKING DOCUMENT 3

on the relation between the surveillance practices in the EU and the US and the EU data protection provisions

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Claude Moraes

Jan Philipp Albrecht (Co-author)

1. Mass surveillance practices in the EU and the US

Several Member States and third countries have programmes of mass surveillance of electronic communications by their communications intelligence agencies, as has been established in the context of the revelations unveiled by former NSA contractor Edward Snowden and further elaborated and supported by a large number of journalistic investigations and reports since then.[1] Some of the revelations have been confirmed by the intelligence agencies, but for most part, the respective agencies have declined to comment or have stated that the documents have been misinterpreted. The United States, the UK, Sweden, France and Germany have the means to tap into the internet backbone cables and collect all of the traffic for a certain period of time ("full take", NSA and GCHQ) or part of it (FRA, DGSE, BND), and at least the Netherlands are reportedly working on such a programme. Access to the backbones is either done by lawful interception facilities and standardised interfaces[2] or by tapping into the fibre-optic cables directly and bending or splicing them[3].

According to media reports, at least the US and the UK also have means of gaining access to confidential computer and telecommunications systems by obtaining unauthorised access, including possible access to the communications provider of the EU institutions. It is also alleged that the NSA also has a programme of actively inserting backdoors in widely-used cryptographic tools in order to be able to read most of the intercepted traffic and data.[4]

Access to data stored and processed on computer facilities, including remote computing facilities (cloud computing), is carried out by various intelligence programmes, the most prominent one being the NSA PRISM programme and the underlying legal provisions in the FISA Act and the USA PATRIOT Act. Furthermore, at least US and UK embassies, consulates and military establishments in third countries, including in other Member States, host electromagnetic interception facilities directed at GSM interception, including on heads of state and government.[5]

Raw personal data collected through these programmes is shared in bulk between the intelligence communities of the US, the UK, Canada, Australia and New Zealand under the "Five Eyes" agreement.[6] Other intelligence sharing agreements exist to varying degrees

---

[1] See the two studies commissioned by DG INPOL, Policy Department C, in the context of the LIBE special inquiry: "The US surveillance programmes and their impact on EU citizens' fundamental rights", PE 474.405, September 2013, and "National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law", PE 493.032, October 2013.

[2] C.f. the secret room 641A at the AT&T switching facility in San Francisco, see Whistle-Blower's Evidence, Uncut, Wired, 22.5.2006, http://www.wired.com/science/discoveries/news/2006/05/70944; the GCHQ Tempora programme, see GCHQ taps fibre-optic cables for secret access to world's communications, The Guardian, 21.6.2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa; the German Telecommunications Surveillance Regulation of 2005. The European Telecommunications Standards Institute (ETSI) has a "Lawful Interception Seminar" responsible for defining such standards.

[3] The US Navy has a specialised submarine for doing this on submarine cables, the USS Jimmy Carter.

[4] NSA Cryptanalysis and Exploitation Services: Project Bullrun – classification guide to the NSA's decryption program, published at http://www.theguardian.com/world/interactive/2013/sep/05/nsa-project-bullrun-classification-guide.

[5] James Ball: NSA monitored calls of 35 world leaders after US official handed over contacts, The Guardian, 25.10.2013, http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls

[6] The existence of the Five Eyes agreement, also known as UKUSA Agreement, was already confirmed by the European Parliament special report on the on the existence of a global system for the interception of private and

between these countries and other Member States.

While in most cases, such mass surveillance is, in a strict reading of the respective laws, only permissible on the communications of foreigners, there are practices to circumvent this limitation including by setting a very low threshold for establishing the probability of the communications subject being foreign (e.g. by an expansive interpretation of the "relevant" threshold in the US FISA act), by declaring the internet as "foreign" by nature (as was recently revealed about the German BND[1]), or by swapping the data collected on each other's citizens.[2] This highlights the intrinsically transnational nature of surveillance activities and the limits to solely national scrutiny bodies.

All these revelations have raised serious concerns on the legality of such measures under EU primary and secondary data protection law, law on cyber-security and cybercrime, obligations under the Council of Europe, and broader provisions in Union law that also address the borders of EU and Member States' competence. The following sections will point out the challenges that mass surveillance practices by the US and several EU Member States pose to EU law and EU data protection in particular.

2. EU and European data protection law

Primary law: Member States' legal systems need to comply with the fundamental rights and fundamental legal principles enshrined in Article 6 of the Treaty on the European Union and the Charter of Fundamental Rights of the European Union. Data protection is a binding fundamental right under Article 8 of the Charter of Fundamental Rights, which reflects Article 8 of the European Convention on Human Rights and has a specific legal basis in Article 16 TFEU: "Everyone has the right to the protection of personal data concerning them". Fundamental rights enjoy special protection and higher safeguards than other rights under law.

There is a significant body of jurisprudence from the ECtHr providing the standards for determining the legality and legitimacy of secret surveillance activities by executives and intelligence communities. In particular, ECtHR case law on the right to privacy and data protection in respect to surveillance by secret services has stressed the danger of these measures of undermining or even destroying democracy on the ground of defending it, and affirmed that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate3. The ECtHR case law provides that the offences and activities in relation to which national security surveillance may be ordered in a clear and precise manner, the law should clearly indicate which

---

commercial communications (ECHELON interception system), A5-0264/2001, 11.7. 2001. See also: NSA Press release, 24.6.2010: Declassified UKUSA Signals Intelligence Agreement Documents Available, http://www.nsa.gov/public_info/press_room/2010/ukusa.shtml.

[1] Fakt, ARD German TV, 12.11.2013, http://www.mdr.de/fakt/video160094.html, manuscript at http://www.mdr.de/fakt/bnd114-download.pdf.

[2] James Ball: US and UK struck secret deal to allow NSA to 'unmask' Britons' personal data, The Guardian, 20.11.2013, http://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data

[3] Klass and others v Federal Republic of Germany, European Court of Human Rights, 6 September 1978 (Series A, NO 28).

categories of people may be subjected to surveillance and that there must be strict limits on the duration of any surveillance and effective remedies in cases of alleged unlawful interferences with ECHR rights.

Member States have claimed that there is no EU competence as regards intelligence surveillance practices since maintaining law and order and safeguarding national security fall within the remit of their exclusive field of intervention. However, as there are national security exemptions in EU data protection law (see in detail below), it needs to be clarified also from the side of the Parliament what "national security" means and to which extent measures taken with a reference to national security are outside the scope of EU primary and secondary law on data protection.

Data protection law: Directive 1995/46/EC[1] lays down the general rules for data protection in the private and public sector. Framework Decision 2008/977/JHA[2] provides the data protection rules for the law enforcement sector when exchanging data across the internal borders in the Union. Current EU data protection law is based on the principles of purpose limitation, data minimisation, and rights of the data subject, including the right to be informed about and to object to the processing, to get access to one's personal data, and to not be subject to automated decisions that significantly affect the data subject.

Data protection limits for mass surveillance by Member States: According to Article 13 of Directive 1995/46/EC, Member States may adopt legislative measures to restrict these rights only "when such a restriction constitutes a necessary measure to safeguard: (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (g) the protection of the data subject or of the rights and freedoms of others."

"National security" here relates to the EU Member States, not to a third country. It also is, in practical terms, hard to distinguish from "public security", which does not fall outside of EU competence. There is significant case-law that limits the notion of "national security", and any measure taken by government agencies in this regard must also be proportionate according to general principles of the rule of law. In instances where private enterprises provide personal data to national intelligence agencies for the purposes of national security, this disclosure and the further processing by the national intelligence services could be considered under the "national exemption" of Article 4 TEU. However, such a request made by the national intelligence services must respect Article 2 TEU and be in full compliance with the ECHR and the rule of law.

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[2] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

Data protection limits for mass surveillance by third countries: Third countries' national security does not provide a basis for exemptions under the existing data protection law. Therefore, European personal data is in principle protected against such exemptions when transferred to third countries, such as the Safe Harbour decision of 2000 on transfers of personal data to the United States[1] specifying that any limitations to data subject rights are allowed only "to the extent necessary" to meet national security, public interest, or law enforcement requirements. In case a third country does not provide an adequate level of protection of personal data, there are two ways in Union law to prevent or interrupt the transfer of data from the Union to such countries: a) The Commission can unilaterally lift an existing adequacy rating; b) the national data protection authorities can stop the transfer of personal data. This is also spelt out in the Safe Harbour Agreement in Article 3(1), based on Article 25(3) of Directive 1995/46.[2] The Commission has recently announced 13 recommendations to improve the Safe Harbour Agreement with, among others, the aim of ensuring that the national security exemption in the Safe Harbour decision is used only to an extent that it is strictly necessary and proportionate. [3]

In general, the EU system on transfers of personal data to third countries is based on the principle of the continuity of protection, so as to avoid that the protection granted in the EU is lost, eroded or denied just because the data are transferred to a third country. The rules and mechanism established aim at ensuring this requirement. This was already established in Directive 95/46/EC, and the current proposals for a Regulation and a Directive will make this principle clearer. The Directive will also improve the situation with regard to law enforcement activities as it will achieve a greater convergence of the data protection legal framework applicable to this sector. Transfers to third countries always require respect of the purpose limitation, and personal data shall be only processed in the third country for the specific, specified and legitimate purpose and not further processed in an incompatible manner. This is a prerequisite that applies to any transfer, whether it is based on an adequacy decision of the Commission or on contractual arrangements put in place by the EU controller and the importer. Further processing of data transferred to a third country for intelligence purposes is an incompatible purpose and would necessarily be an exception to the obligations imposed. It therefore should be in line with the system of exceptions of Article 13 of Directive 1995/46/EC.[4] Regarding mass surveillance and activities of intelligence conducted on the basis of processing of bulk categories of personal data, countries where the powers of state authorities to access information go beyond those permitted by internationally accepted standards of human rights protection will not be safe destinations for transfers.

The data protection reform package: The above-mentioned two laws are currently being revised, with a General Data Protection Regulation replacing the 1995 Directive, and a Data

[1] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441.

[2] C.f. Franz C. Mayer: Mit Europarecht gegen die amerikanischen und britischen Abhöraktionen? Teil 1: NSA, www.verfassungsblog.de/de/mit-europarecht-gegen-die-amerikanischen-und-britischen-abhoeraktionen-teil-1-nsa.

[3] Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013)847, 27.11.2013.

[4] The EDPS in his presentation to the LIBE Committee hearing of 7 October 2013 took this view.

Protection Directive replacing the 2008 Framework Decision. This Committee has on 21 October 2013 voted almost unanimously for the negotiation mandates for the rapporteurs, Jan Philipp Albrecht and Dimitrios Droutsas, with the aim of achieving a first reading agreement with Council before the end of this legislative term.

The LIBE reports build on the rights established in the existing EU laws, specify them to a certain extent, and aim at a better and more coherent enforcement across the Union. The explicit reference to the "national security" exemption in Article 2 on the scope of the regulation has been deleted by LIBE, based on the argument that the scope of the national security exemption is contested. The LIBE report also has introduced a new Article 43a into the data protection regulation to ensure that access requests by public authorities or courts in third countries to personal data stored and processed in the EU can only be granted if they also have a legal basis in EU law and are authorised by the competent European data protection authority.

The e-Privacy Directive, confidentiality of communications, and data retention: Electronic communications privacy is also specifically regulated in Directive 2002/58.[1] Under Article 5, Member States shall "ensure the confidentiality of communications through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1),"Such a restriction of the confidentiality of communications can only be adopted by Member States according to Article 15 (1), when it "constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system". Again, such a national security exemption cannot be used as a carte blanche, but has to meet certain tests. Article 15, however, as a general opening clause, has led several Member States to adopt laws for data retention that go further than the Data Retention Directive of 2006[2]. The data retention directive is currently subject to a proceeding of the Court of Justice after constitutional complaints in Ireland and Austria.[3] The e-Privacy Directive also establishes positive obligations on Member States to prevent mass surveillance of communications data by private operators. In its ruling in the case Scarlet v Sabam, the CJEU ruled that a system of general surveillance by an internet service provider of its customers to track their activities on the internet was not in line with the e-Privacy Directive and the EU Charter of Fundamental Rights.[4]

Data protection by Union institutions: Regulation 2001/45[5] concerns the processing of

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), last amended 2009.
[2] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
[3] The statement of the attorney-general is expected for 12 December 2013.
[4] Judgement of the Court (Third Chamber) in Case C-70/10, 24 November 2011.
[5] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

personal data by Union institutions and bodies. For agencies such as Europol or Eurojust, the data protection regime is set out in their specific legal acts. Moreover due to the specific and sensitive nature of the information processed by these agencies they have a higher responsibility, because of the serious adverse effects on individuals' fundamental rights raised from disclosure to third countries. Where the EU or its agencies transfer personal data to third countries, they should take the necessary measures to ensure that data transferred is not further processed for incompatible purposes such as intelligence. Should they become aware that data is or may be used for intelligence purposes or mass surveillance, they should adopt the necessary measures to prevent it, inform the EDPS and if needed suspend the transfer.

Concerns have been raised that the sharing of information with Europol by national law enforcement authorities and potentially by intelligence services, and other international partners, renders indistinguishable the boundaries of what is police cooperation covered by Title V, Chapter 5 TFEU) and what is intelligence at EU level. This leaves little room for properly reviewing the legality and adequacy of the kind of information exchanged and their exact sources against data protection principles, because it is not clear which law is applicable and consequently which principles apply. The allegations of surveillance programmes operating by some EU Member States indicate a progressive merging of police, military and intelligence actors and practices which create legal insecurity and uncertainty in the actions and credibility of EU agencies themselves and reveal an accountability gap which needs to be effectively addressed at European level.

EU-US data protection framework agreement: In May 2010, the European Commission adopted the mandate for negotiations between the EU and the US on a framework agreement on data protection in the field of police and judicial cooperation ("umbrella agreement"), authorised by the Council on 2rd December 2010.[1] From the beginning the negotiations have been challenging and over a year ago reached a stalemate. The main importance of a framework agreement would be the resolution of the issue of judicial redress for EU citizens when their personal data is transferred to the US. At the moment EU citizens do not enjoy full and reciprocal judicial redress rights as access to US courts are guaranteed only to US persons (citizens and permanent residents). On top of this actual and urgent issue, completing the negotiations would restore trust in transatlantic data transfers. It would be crucial that the Commission objective of a meaningful and comprehensive agreement that ensures legal redress for EU citizens be reached before summer 2014.

Council of Europe Convention 108: The EU is currently acceding the European Convention on Human Rights of the Council of Europe, and all Member States are already party to it. Article 8 ECHR states "Everyone has the right to respect for his private and family life, his home and his correspondence." This is more clearly spelled out in Convention 108 of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data from 28 January 1981, which provides in Article 5 that personal data shall be "obtained and processed fairly and lawfully" and stored "for legitimate purposes and not used in a way incompatible with those purposes". Article 9 of Convention 108 allows derogations only if they constitute "a necessary measure in a democratic society" or for "protecting the data subject or the rights and freedoms of others". There is a significant body

[1] http://europa.eu/rapid/press-release_IP-10-1661_en.htm

of case law spelling out what falls under these limits.[1]

3. Data Security and Cyberattacks Provisions

Data security provisions: All of the Union's data protection laws have provisions that mandate the data controller to ensure the security of the personal data processed. This includes securing the data against cyber-attacks from the outside and notifications to the supervisory authorities and the data subject in case of data breaches. By logical conclusion, Member States' authorities should be banned from pursuing such attacks and rather obtain lawful access in individual cases based on lawful interception. It is as yet unclear if the reported attacks on Belgacom and other telecommunications providers such as SWIFT have included a breach of personal data, however, given that Belgacom have subsequently admitted that there is a possibility that customers personal data have been accessed[2], precautionary measures should be put in place to notify the customers, which includes the EU institutions, about the reported cyberattacks.

Cyberattacks directive and Budapest Convention: The new Directive on attacks against information systems[3] has entered into force this summer and has replaced the existing Framework Decision. Both are based on the Council of Europe Convention on Cybercrime from 2001, also known as the Budapest Convention.[4] The Budapest Convention mandates its parties to establish as criminal offences, if done without right, the access to a computer system, the interception of non-public data transmissions, as well as interference with computer data and computer systems. While the Budapest Convention has provisions that allow the parties to establish legal provisions for the interception of content data by competent authorities (e.g. in the case of law enforcement measures), these apply only to the territory of the respective country. The (mass) surveillance of communications and the attacks on information systems in the territory of another party to the Convention are not covered and are therefore illegal under the national transpositions of the Budapest Convention and the EU Framework Decision and the new Directive. This is even more relevant, as the United States is a party to the Budapest Convention.

The LIBE Committee has recently expressed its concern about the work carried out within the Council of Europe's Cybercrime Convention Committee with a view to developing an additional protocol on trans-border access to stored computer data, and expressed that it is "alarmed by the fact that should such an additional protocol be endorsed, its implementation could result in unfettered remote access by law enforcement authorities on servers and computer systems located in other jurisdictions, without recourse to MLA agreements and other instruments of judicial cooperation put in place to guarantee the fundamental rights of

[1] Two prominent examples are S and Marper v United Kingdom (2009), which curtailed the retention period in the UK National DNA Database, especially for non-suspects, and Gillan and Quinton v United Kingdom (2010), which ruled that powers granted to the police under the Terrorism Act of 2000 were neither sufficiently circumscribed nor subject to adequate legal safeguards and therefore not 'in accordance with the law'.

[2] http://www.lesoir.be/343247/article/economie/2013-10-18/belgacom-pirate-donnees-privees-ses-clients-sont-concernees

[3] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

[4] Council of Europe, Convention 185 on Cybercrime, Budapest, 23.11.2001

the individual, including data protection and due process."[1]

4. Conclusions and recommendations

1. Member States' legal systems need to comply with the fundamental rights and fundamental legal principles as enshrined in Article 6 of the Treaty on the European Union and the Charter of Fundamental Rights of the European Union.

2. Data protection is a binding fundamental right under Article 8 of the Charter of Fundamental Rights, which reflects Article 8 of the European Convention on Human Rights and has a specific legal basis in Article 16 TFEU.

3. Member States are bound by several EU data protection and cyber-security laws. It should be further investigated if any of the mass surveillance activities are in breach of EU primary or secondary law in this regard. It should also be investigated if Member States' activities are in breach of obligations in the context of Council of Europe conventions and the European Convention on Human Rights.

4. As there are national security exemptions in EU data protection law, it should be clarified also from the side of the Parliament what "national security" means and to which extent measures taken with a reference to national security are outside the scope of EU primary and secondary law on data protection.

5. Third countries' national security does not provide a basis for exemptions under the existing data protection laws. European personal data is in principle protected against such exemptions when transferred to third countries, such as the Safe Harbour decision of 2000 on transfers of personal data to the United States. The revision of the Safe Harbour Agreement should clearly limit the scope of possible exemptions and should exclude mass surveillance activities.

6. The EU data protection reform should be concluded with priority. After the adoption of the LIBE reports and negotiation mandates on 21 October 2013, Council should now adopt its negotiation position as soon as possible, so an agreement can still be reached before the end of this legislative term. It will be of utmost importance to maintain the new Article 43a on protection against data access by third countries.

7. The negotiations between the EU and the US on a framework agreement on data protection in the field of police and judicial cooperation should be concluded swiftly, while solidly resolving the current lack of judicial redress for EU citizens in the US.

8. The proposed Council of Europe's Cybercrime Convention additional protocol on trans-border access to stored computer data could result in unfettered remote access by law enforcement authorities on servers and computer systems located in other jurisdictions, which is unacceptable. Any such protocol should instead refer to MLA agreements and other

[1] Opinion under Rule 50 of the Committee on Civil Liberties, Justice and Home Affairs for the Committee on Industry, Research and Energy on unleashing the potential of cloud computing in Europe (2013/2063(INI)), 19.9.2013, PE504.203v02-00.

instruments of judicial cooperation to guarantee data protection and due process.

9. The future Europol regulation should include an article stating that data obtained in violation of fundamental rights in accordance with article 6 TEU and the Charter of Fundamental Rights of the European Union shall not be processed.

10. The allegations of surveillance programmes operated by some EU Member States indicate a progressive merging of police, military and intelligence actors and practices, which create legal insecurity and uncertainty in the actions and credibility of EU agencies themselves and reveal an accountability gap which needs to be effectively addressed at European level.