Project acronym:	SAPIENT
Project title:	Supporting fundamentAl rights, PrIvacy and Ethics in surveillaNce Technologies
Project number:	261698
Programme:	Seventh Framework Programme for research and technological development
Objective:	SEC-2010.6.5-2: Use of smart surveillance systems, data protection, integrity and sharing information within privacy rules
Contract type:	Collaborative project
Start date of project:	1 February 2011
Duration:	36 months

Deliverable 6.6:

Cross-border law enforcement access to data on the Internet and rule of law challenges in the EU

Rapporteurs:	Gertjan Boulet (VUB) and Nicholas Hernanz (CEPS)
Dissemination level:	Public
Deliverable type:	Report
Version:	1.0
Due date:	31 September 2012
Submission date:	15 August 2013

Abstract

This policy brief examines the cross-border gathering of data on the Internet by law enforcement authorities in the EU, and the cooperation with private companies. The authors examine the extent to which this cooperation is already taking place in the EU and show that the nature of the current EU legal frameworks in place are of incomplete and scattered nature. This leads to a number of rule of law challenges for the actors involved (law enforcement and the private sector), including for the fundamental right of data protection of the individual subject to these practices. The policy brief argues that these challenges cannot be addressed without a clear multi-actor policy strategy at EU level, which should be rooted in strong rule of law foundations.

Document history

Version	Date	Changes
1.0	15 January 2013	Draft restricted version of the deliverable (D6.5)
2.0	15 August 2013	Final public version of the deliverable

Text

1. Introduction – what is the issue?

On 6 June 2013, the Guardian and Washington Post newspapers published articles revealing that an electronic surveillance system called "PRISM" had been used by intelligence services in the United States since 2007.[1] This clandestine operation allegedly allowed the US National Security Agency to collect data on US and non-US citizens residing outside the US territory, through the servers of participating Internet companies.

The widespread coverage on PRISM by European media triggered various reactions at EU level. The European Parliament organised a debate during its plenary session on 11 June 2013 which saw several Members of the European Parliament outraged by the surveillance system. It was announced that the European Commission would bring up this issue during future bilateral EU-US ministerial meetings and that a Transatlantic Group of Experts would be set up to further discuss the programme.[2]

The PRISM "affair" is emblematic of a wider trend in recent years which has seen a rise in the gathering of data by law enforcement authorities on the Internet, for the announced purpose of fighting terrorism and organised crime. Individuals also have a keen interest in knowing how public authorities are dealing with private data on the Internet, and how the industry responds to their requests for data.

This example of law enforcement authorities gathering data on individuals from private Internet companies shows that without a clear legal framework, massive data gathering is bound to happen. It is therefore interesting to look at how, when and under which conditions law enforcement authorities in the EU can request or have access to private data of Internet companies.

In the EU, protection of an individual's private data is one of the fundamental rights enshrined in the European Convention on Human Rights (ECHR) as well as in the legally-binding EU Charter of Fundamental Rights. EU data protection rules expressly recognise the individual as the first owner of his/her data. The fact that the data belongs to the individual is a key paradigm of the EU's data protection culture as it results in the core principle that personal data must not be processed without the consent or permission of the individual.[3]

Law enforcement authorities gathering private data held by Internet companies in the EU therefore challenge the individual's fundamental right to data ownership in two ways:

First, it creates a grey zone of legal uncertainty for the data subject as regards which data protection rules to use in cross-border cases. This is clearly reflected in the current gaps and unfinished components of the EU's legal framework regarding these data requests.

---

[1] See the Guardian article on http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data and the Washington post article on http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

[2] For a more detailed description of PRISM and its implications on the EU, refer to Bigo, D., Boulet, G., Bowden, C. et al (2013) Open Season for Data Fishing on the Web: The Challenges of the US PRISM Programme for the EU, CEPS Policy Brief, June 2013.

[3] See the data protection principles presented in Brouwer, E. (2008) Digital Borders and Real Rights, Martinus Nijhoff Publishers, Leiden, pp. 204-205.

Second, it ignores the principle of individual consent as the collection becomes a matter of "bargaining" between law enforcement authorities and private companies as regards what type of data (metadata and/or personal data?) should be made available, and what data protection standards apply in the fights against cybercrime or organised crime. It is therefore central to understand the relations between law enforcement authorities and private companies at times of assessing how the collection of personal data is made possible in the fight against crime.

In both cases, the asymmetrical use of data collection by law enforcement authorities for security purposes positions the individual in a rather unbalanced context. Against the security of a whole country, the data of one individual – and his rights – might seem irrelevant. The cooperation between law enforcement and private sector transforms the individual from a data subject to a data object with virtually no power to challenge or influence what is done with his/her personal data.

It is therefore key to explore the rules – or lack of rules – at EU level as regards the requests for private data of law enforcement authorities to Internet companies in another member state. One would assume that for an issue which has so many repercussions on the everyday lives of citizens, some legal standards would exist; but it is all the more surprising to see the current gaps and unfinished components in the EU's legal and policy frameworks regarding these data requests.

It is also central to understand the relations between law enforcement authorities and private companies at times of assessing how the collection of personal data is made possible in the fight against crime. This question is all the more interesting when looking at the issue of jurisdiction. What rules should apply to private data belonging to EU citizens but processed by companies that are based in the United States? How can data protection standards be exported to other countries? By definition, the Internet is cross-border and ignores nationality. The growth in cloud computing in recent years, which allows for real-time processing of data on servers in remote locations, multiplies the legal challenges especially as regards the lack of standards and the inexistence of legal certainty in the cloud. It also clearly redefines the territorialisation of legal standards.

In this policy brief, which is part of the SAPIENT project,[4] the authors argue that without a clear legal framework, massive data gathering is bound to happen inside the EU. Therefore, a strong policy framework offering a solid legal framework and minimum standards as well as a multi-actor strategy are essential to address the main challenges encountered by law enforcement authorities and private Internet companies.

Our main argument is that those legal and policy arrangements need to be closely tied to strong rule of law principles, in particular those of legal, judicial and democratic accountability, and take into account the individual fundamental right to

[4] SAPIENT (Supporting fundamentAl rights, PrIvacy and Ethics in surveillaNce Technologies) is a 36-month collaborative research project that started in 2011. This project is co-funded by the European Commission under the 7th Framework Programme (FP7). SAPIENT has organised a policy meeting in October 2012 in which the role of Internet monitoring and cyber-surveillance for law enforcement authorities, especially through preventive data collection and processing on the Internet in the fight against crime, was debated. This policy brief echoes the debates that took place during this policy meeting, while complementing the arguments presented with a clear presentation of the existing legal framework at EU level and of the general context behind law enforcement access to privately-held data in cross-border cases.

data protection and privacy enshrined in the Charter of Fundamental Rights of the EU.[5]

Properly addressing all these issues would require a longer and more in-depth study. The authors' objective is to present the main challenges of law enforcement gathering Internet data through private companies in a short policy brief and to think ahead for possible future policy options. First, this policy brief will look at how – and how much – law enforcement authorities access private data in the EU (Section 2). The authors will then present the existing legal frameworks at EU level as regards law enforcement and data protection, in particular in the scope of the so-called Area of Freedom, Security and Justice (AFSJ) (Section 4). Next, the policy brief will address the challenges stemming out from the multi-actor context (Section 5). Section 6 will then discuss the impacts on the rights to privacy and data protection. Finally, the policy brief will put forward a set of policy recommendations for EU decision-makers at times of debating new data protection rules at EU level.

2. Statistics and scenarios on cross-border law enforcement requests

Cross-border data requests by law enforcement authorities to private companies are not a new trend and have been going on for quite some time. Recent debates on the establishment of an EU TFTS to gain access to financial data from the Swift company[6] as well as current negotiations on the setting-up of a European PNR to access airlines' passenger data[7] are strongly reminiscent of the controversies surrounding the ECHELON system in the early 2000s, on which a special committee of the European Parliament issued a report.[8] It is therefore key to explore the publicly available knowledge as regards how many requests are currently sent to private firms by law enforcement authorities.

Statistics from Google, Microsoft and Twitter

One of the key developments in recent years has been the increasing demand by law enforcement authorities to gain access to private data held by private Internet

[5] The Charter became legally binding after the Lisbon Treaty entered into force in 2009. The principle of the rule of law is inherent to any modern democratic society and is a central notion at times of understanding the challenges of law enforcement requests to private Internet companies. In the EU context, rule of law is a term used frequently in preambles to the EU treaties and the Charter but no definition exists in EU official documents. Understanding rule of law in the EU requires a step back to the national conceptions of rule of law, which greatly differ in their exact definition. One of the most consensual definitions of what rule of law is in Europe has been provided by the work of the Venice Commission, which highlights the importance of checks and balances, legal certainty, proportionality and fundamental rights. See Venice Commission (2011) Report on the Rule of Law, Strasbourg, 4 April 2011, retrievable from www.venice.coe.int/webforms/documents/CDL-AD(2011)003rev-e.aspx

[6] Refer to the communication: European Commission (2011) A European terrorist finance tracking system: available options, COM(2011) 429 final, Brussels, 13 July 2011.

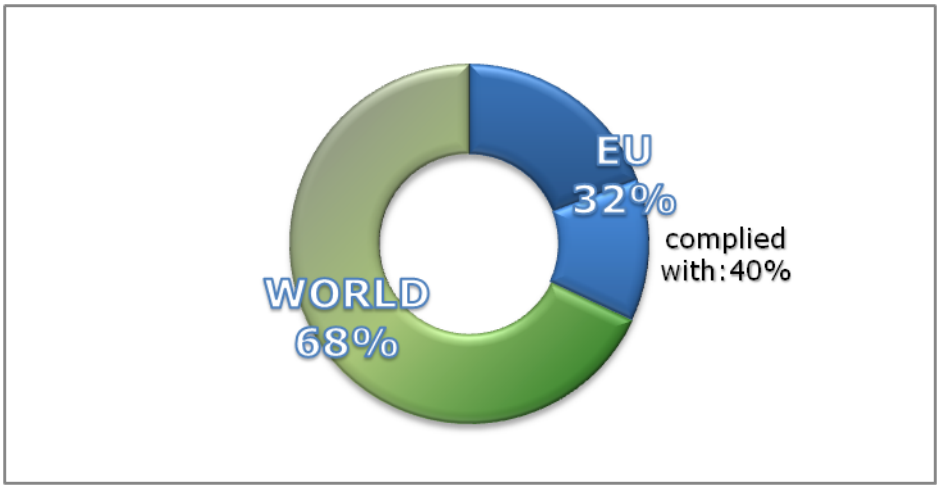
[7] See European Commission (2011) Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final, Brussels, 2 February 2011.

[8] 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)), 11 July 2001.

firms. While it is impossible to assess precisely how many times police authorities in the EU have requested access to individual data held by Internet firms in the past years, some statistics provided by the biggest online data processing firms can hint at the extent of this trend.

In April 2013, the Internet corporation **Google** published its annual transparency reports.[9] Through these reports, Google wanted to show how authorities in the world interacted with the company by requesting content removal or user data. Google also specified how many of these requests it complied with. Between July and December 2012, authorities in the EU alone accounted for more than a third of all requests made in the world. On average, Google complied with 40% of all requests (from 0% for Hungary to 70% in the United Kingdom).[10] Requests came mainly from the United States and India and from the United Kingdom, France and Germany in the EU.

Figure 1: Requests received by Google from law enforcement authorities in the EU, July-December 2012



Source: Authors' own elaboration, based on Google's Transparency Report 2012

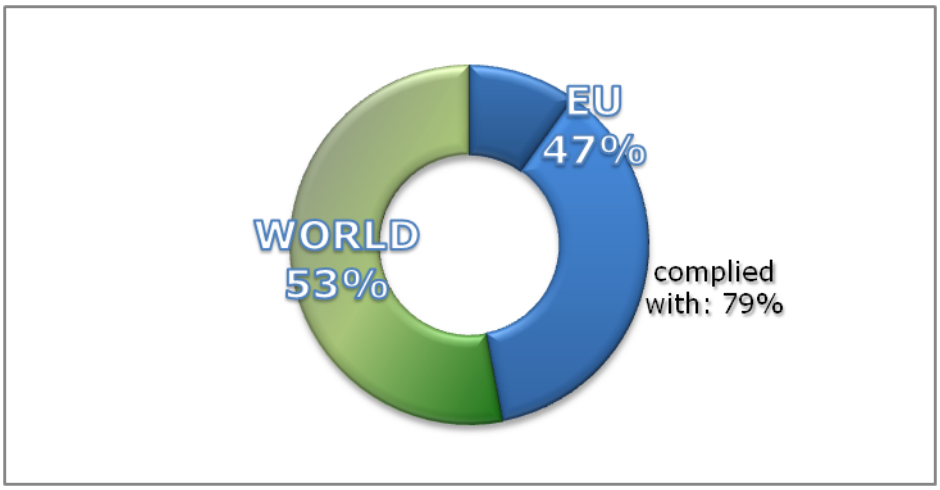
Microsoft also released its Law Enforcement Requests Report which shows that, in 2012, requests from EU member states represented 47% of the total requests. 79% of these requests resulted in the disclosure of data to authorities in EU member states.[11] Requests came mainly from Turkey and the United States and, similarly to Google, from the United Kingdom, France and Germany in the EU.

[9] See www.google.com/transparencyreport/removals/government/

[10] Source: authors' own calculations, based on the User Data Requests by Countries in Google's Transparency Report, available here: www.google.com/transparencyreport/userdatarequests/countries/?t=table

[11] Source: authors' own calculations, based on Microsoft 2012 Law Enforcement Requests Report. Requests for Skype data are included in the statistics. The full report is available at this link: www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/

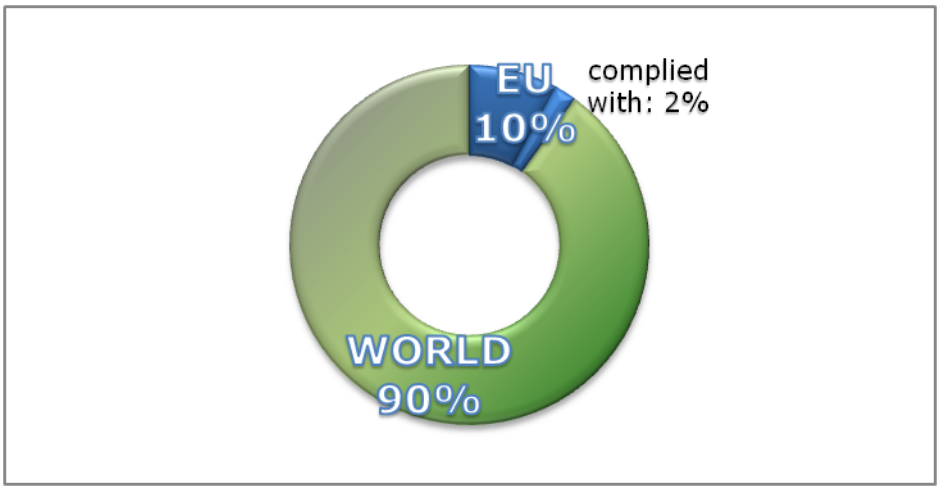
Figure 2: Requests received by Microsoft (including Skype) from law enforcement authorities in the EU in 2012



Source: Authors' own elaboration, based on Microsoft's Law Enforcement Requests Report 2012

Another big Internet company which published the number of requests received was **Twitter**: in the second half of 2012, approx. 10% of all requests came from EU member states and only 2% of these requests were complied with.[12] The requests came mainly from the United States, Japan and Brazil and from the United Kingdom and France in the EU.

Figure 3: Requests received by Twitter from law enforcement authorities in the EU, July-December 2012



Source: Authors' own elaboration, based on Twitter's Transparency Report 2012

The main challenge related to these transparency reports is that they only show statistics on the reported cases of data requested. It is clear from the recent events

[12] Source: authors' own calculations, based on Twitter's Transparency Report, available here: https://transparency.twitter.com/information-requests-ttr2

that a big majority of data gathered by law enforcement authorities takes place outside the knowledge and consent of the private companies.

Recent articles have shown that France allegedly operates a massive surveillance programme, similar to PRISM, which gets automatic access to data from all major Internet companies.[13] The same seems to happen in the United Kingdom where the UK Government Communications Headquarters (GCHQ) has supposedly gained access to massive amounts of personal data through its operation "Tempora".[14] Similarly, article 88ter of the Belgian Code of Criminal Procedure allows an investigating judge,[15] when performing a search on a computer system, to extend this search to another computer system even outside of the Belgian borders. The judge would need to respect the conditions of necessity, proportionality and a risk of evidence loss.[16] This is why the authors will now look at the possible ways in which law enforcement authorities can access data from private companies in another state.

Four scenarios

The current situation reveals four possible scenarios for law enforcement agencies in the EU when requesting private data on the Internet to companies hosting or processing the requested data:

1. **Voluntary cooperation:** Law enforcement authorities get the needed data by simply contacting bilaterally a private party wherever located and requesting the data. This approach requires the private company to voluntarily cooperate with the law enforcement authority requesting the data. As recent examples have shown, this voluntary cooperation cannot be taken for granted as it creates a burden for private companies.[17] If the requested data is stored on a server located in another country, most law enforcement authorities (depending on national law) need to notify the country concerned.
2. **Direct access:** Law enforcement authorities get access to private databases without the knowledge or the consent of the private company. Some law enforcement agencies can also obtain remote access to data through special software or technical means ("key loggers", "sniffers") in very exceptional circumstances. Moreover, another scenario is the observation by police authorities on social networks such as Facebook.
3. **Mutual legal cooperation:** Law enforcement authorities use mutual legal cooperation as an old fashioned way of obtaining requested data when the private party is located outside the territory. Police are often complaining about the technical difficulties and length of this procedure.

---

[13] See www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html

[14] See www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

[15] An investigative judge is a magistrate charged with the task of gathering evidence in a case. Investigative judges only exist in the inquisitorial system used throughout continental Europe.

[16] See Council of Europe (2012) Discussion paper: Transborder access and jurisdiction: What are the options? Report of the Transborder Group, adopted by the T-CY on 6 December 2012, p. 33.

[17] For instance, the recent British proposal to create a new retention order requiring Internet companies in third-countries to store the personal data of all their British-based users for up to one year was met with strong criticism from five major Internet firms. See: www.guardian.co.uk/politics/2013/may/30/snoopers-charter-web-five-letter

4. **Europol:** A fourth possible scenario could be, in the future, for police agencies to turn to a centralised EU law enforcement authority (for instance Europol) which would adopt a streamlined approach and directly request private data from Internet companies in the EU to then share the data with the requesting national police authority. This scenario would require upgrading the mandate of EU agencies to include such responsibility.

Most of these scenarios suppose that the requesting law enforcement authority knows in which country the data is stored. As we have shown above, the increasing use of cloud computing services makes it more difficult to assess where the data is located. It is likely that companies using cloud services do not themselves know in which country the data is stored. Thus, access to an individual's data is based more on informal and bilateral haggling between police and firms and less on jurisdictional rules.

This section has shown the different scenarios used by law enforcement when requesting data to private Internet companies, and the extent to which these companies cooperate and accommodate law enforcement requests in the EU. It is now central to examine what is the legal framework at EU level, which will be addressed in the next section.

3. EU agenda, policy instruments and legal framework

Law enforcement cooperation at EU level is a particularly complex area which is not only fragmented but also subject to a lot of controversies. Historically, the setting up of the EU's Area of Freedom, Security and Justice (AFSJ) since 1999 and specifically police and criminal justice cooperation between EU member states has always been torn between the need for more cooperation and the will to preserve security policies as a purely national matter reserved to member states' sovereignty. The abolition of the former pillar structure after the entry into force of the Treaty of Lisbon in 2009 has not meant a convergence in the ways of working of the former third pillar on police and judicial cooperation in criminal matters. In a majority of fields, the ordinary legislative procedure has been expanded (with certain exceptions), but the old third-pillar spirit is still present in this area.[18] This brings about deficiencies which include democratic deficit, lack of accountability and weak judicial control together with secrecy and lack of transparency, therefore weakening rule of law standards.

At EU-level, the legal frameworks governing the access of law enforcement authorities to private data in other EU member states are fragmented and present huge gaps. The EU has adopted legal instruments on police cooperation but there is no parallel framework on what the actors involved shall do in the case of information sharing on the Internet. This section will present the main policy and legal instruments at EU level that are currently in place, as well as the ones being negotiated and likely adopted in the future.

[18] See Guild, E. and Carrera, S. (2011) Towards an Internal (In)security Strategy for the EU? CEPS Liberty and Security Papers, Brussels, January 2011.

The EU agenda and policy instruments for cooperation

Cooperation between law enforcement authorities in the EU on the fight against crime, more specifically on the gathering of evidence on the Internet, has been called for repeatedly by decision-makers in the EU's policy agenda.

In the **Stockholm Programme** (2010), which aims at setting out the main EU policy priorities on AFSJ cooperation for the years 2009 – 2014, the European Council invited the European Commission to "*take measures for enhancing public-private partnerships*" and to "*explore if and how authorities of one Member State could obtain information rapidly from private or public entities of another Member State without use of coercive measures or by using judicial authorities of the other Member State*".[19] In the **Internal Security Strategy** (2010), which envisages the challenges, principles and guidelines for dealing with security threats in the EU, the European Commission noted that the cooperation between the public and private sector must be strengthened.[20] More recently, in its **Cybersecurity Strategy** (2013), the European Commission added that "*[l]egal obligations should neither substitute, nor prevent, developing informal and voluntary cooperation, including between public and private sectors, to boost security levels and exchange information and best practices.*"[21]

In the Communication "**An area of freedom, security and justice serving the citizen**" (2009), the European Commission already noted that "*a legal framework must be established that will allow cooperation agreements between law enforcement authorities and operators*", and simultaneously identified at least two of the building blocks for such a framework, that is rules on electronic evidence and rules on jurisdiction applicable to cybercrime.[22]

As regards rules on jurisdiction, in the **Digital Agenda for Europe** (2010), the European Commission announced "legislative initiatives, to combat cyber attacks against information systems by 2010, and related rules on jurisdiction in cyberspace at European and international levels by 2013".[23]

As regards the rules on electronic evidence, the **Proposal for a European Investigation Order Directive** (2010) allows the monitoring of banking transactions; and the **Child Abuse Directive** (2011) allows the interception of communications, covert surveillance including electronic surveillance, monitoring of bank accounts or other financial investigations.[24] The importance of electronic

[19] European Council (2010) The Stockholm Programme: An open and secure Europe serving and protecting citizens, C 115/1, 4.5.2010.

[20] European Commission (2010) Communication from the Commission to the European Parliament and the Council, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, Brussels, 22.11.2010 (COM(2010) 673 final), p. 10. For a critical assessment of the ISS, refer to Carrera, S. and Guild, E. (2011) Towards an Internal (In)security Strategy for the EU? *op. cit.*

[21] European Commission (2013) Joint Communication, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels (JOIN(2013) 1 final), p. 6.

[22] European Commission (2009) Communication from the Commission to the European Parliament and the Council, An area of freedom, security and justice serving the citizen, Brussels, 10.6.2009 (COM (2009) 262 final).

[23] European Commission (2010) Communication on A Digital Agenda for Europe, Brussels, 26.8.2010 (COM(2010) 245 final).

[24] Council of the EU (2010), Initiative (…) for a Directive regarding the European Investigation Order in criminal matters, Council doc 9288/10, 21 May 2010, articles 24 and 25. See also European Parliament and Council of the EU (2011) Directive 2011/92/EU on combating the sexual abuse and

evidence is also highlighted in the recently **adopted resolution of the European Parliament on the proposal for a directive on attacks against information systems** (2013).The European Parliament added a §23 to the preamble, which provides that

'Cooperation between public authorities on the one hand, and the private sector and civil society on the other, is of great importance in preventing and combating attacks against information systems. It is necessary to foster and improve cooperation between service providers, producers, law enforcement bodies and judicial authorities, while fully respecting the rule of law. Such cooperation could include support by service providers in helping to preserve potential evidence, [...] Member States should also consider setting up cooperation and partnership networks with service providers and producers for the exchange of information in relation to the offences within the scope of this Directive."[25]

Yet, apart from pending rules on jurisdiction in cyberspace and rules on electronic evidence, the EU agenda is silent as regards the relevant rules on data protection for the area of cooperation between the private sector and law enforcement agencies.

The EU data protection legal framework

It is interesting to note here that from the very early stages of policy-making in this are, EU decision-makers chose to separate rules on, first, data protection in the field of the internal market and, second, in the field of law enforcement cooperation. This relates to the old third pillar way of working on Justice and Home Affairs mentioned earlier, and has now changed, at least formally, since the Treaty of Lisbon entered into force. The abolition of the former pillar structure has brought about the revision of the data protection framework, leading to the current negotiations on the General Data Protection Regulation and Directive.

The first directive on data protection, adopted in 1995, excluded law enforcement access to data from its scope.[26] No similar standard-setting text was adopted until the 2008 Framework Decision.[27] In the meantime, specific measures on data protection were adopted for various sectors such as the Schengen Information System, Europol or the Prüm Decision. This effectively meant that data protection rules in the field of law enforcement cooperation were progressively adopted in a fragmented way. *"Data protection regulations for security-related processing were thus not introduced in the anticipated order: rather than first introducing a standards-setting instrument to be followed by sector-specific regulations, quite the opposite took place."*[28]

---

sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, L 335/1, 17.12.2011, preamble §27.

[25] European Parliament (2013) Legislative resolution of 4 July 2013 on the proposal for a directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (COM(2010)0517 – C7-0293/2010 – 2010/0273(COD)).

[26] European Parliament and Council of the EU (1995) Directive 95/46/EC of the European Parliament and 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, OJ L 281, 23.11.1995.

[27] Council of the EU (2008) 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, OJ L 350, 30.12.2008.

[28] De Hert, P. and Papakonstantinou, V. (2012) The Police and Criminal Justice Data Protection Directive: Comment and Analysis, in: Computers & Law Magazine of SCL (vol. 22, no. 6), p. 2.

The 2008 **Framework Decision** is designed to govern processing of data by public law enforcement bodies but does not apply to the private sector nor to EU Home Affairs Agencies such as Europol (Recital 39). The 1995 **Data Protection Directive**, as mentioned above, does not cover law enforcement cooperation but only data processing by private firms and public bodies for commercial or administrative purposes. In two cases, the Court of Justice of the EU held that the 1995 **Data Protection Directive** governs the storage of data by private companies, but not the subsequent use and access for law enforcement purposes.[29]

It should be noted that in the cases **Scarlet v. SABAM** and **SABAM v. Netlog**,[30] the Court clarified that the injunction imposed on respectively an Internet service provider and a hosting service provider to install the contested filtering system would require those providers to carry out general monitoring, prohibited by the **e-commerce Directive.**[31]

As the authors argue, this fragmentation and complexity of the legal framework leads to legal uncertainty. This legal uncertainty is not solved however by the currently negotiated Data Protection Reform Package, which consists of a **Proposal for a General Data Protection Regulation**[32] and a **Proposal for a Police and Criminal Justice Data Protection Directive**.[33] These two proposals aim at replacing the 1995 Data Protection Directive and the 2008 Framework Decision. While the two areas of commercial data processing and law enforcement data processing are still kept apart, the first in the Regulation, the second in the Directive, the two European Parliament rapporteurs (Jan Albrecht and Dimitrios Droutsas) in charge of these files have both called for the proposals to be considered as a single package requiring coordinated legislative approaches. Moreover, it can be noted that the current draft report of the European Parliament amends the proposal to bring private entities in the context of law enforcement activities within the scope of the proposed General Data Protection Regulation.[34]

This section has shown that the current EU legal framework presents huge gaps and that future policy initiatives are very unlikely to address those gaps. In fact, the

---

[29] Court of Justice of the EU, Joined cases C-317/04 and C-318/04, Parliament v. Council of 30 May 2006, §57; Case C-301/06, Ireland v. Parliament and Council, judgment of 10 February 2009, §80.

[30] Court of Justice of the EU, Case C-70/10, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), 24 November 2011; as well as Case C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV, 16 February 2012.

[31] European Parliament & Council of the EU (2000) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), L 178/1, 17.7.2000, Article 15(1)

[32] European Commission (2012) Proposal for a Regulation of the European Parliament and of the Council 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), Brussels, 25.01.2012 (COM(2012) 11 final).

[33] European Commission (2012) Proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (General Data Protection Directive), Brussels, 25.01.2012 (COM(2012) 11 final).

[34] See the proposed Amendment 80 in European Parliament (2012) Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Committee on Civil Liberties, Justice and Home Affairs, rapporteur: Jan Philipp Albrecht, (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).

cooperation between private sector and law enforcement authorities is "*likely to be occurring independently of the actual existence of any applicable or common legal framework setting the necessary data standards and regulations framing this relationship and safeguarding the capacity of the individual to control her/his data as a fundamental right. The potential for misuses and abuses by law enforcement actors and agencies becomes henceforth an issue of serious concern*."[35] The "safe harbour" principle applicable to international data transfers, allowing data transfers to third-country organisations that demonstrate an adequate standard of protection, is challenged by cloud computing: it places data subjects in a complex matrix of blurred legal responsibilities, standards and potential liabilities. While cloud computing might increasingly attract the attention of law enforcement agencies, "*data protection laws are not up to the task*".[36] This leaves uncertainty for the individual, and all the actors involved, about the applicable data protection standards governing those cross-border data exchanges, and brings about challenges as regards the core principle of rule of law in democratic societies, and therefore related, the individual's fundamental right to data ownership.

The question of the legal framework governing law enforcement cooperation with private companies is important for the challenge of legal certainty, but, as said, the more important question is how this legal framework is put into practice. The extent to which private Internet companies cooperate with and accommodate requests by government and law enforcement, the different scenarios used by governments and law enforcement for gathering data from these companies, and the gaps in the EU legal framework create several challenges for all the involved actors, which are presented in the next section

4. Multi-actor challenges

The multi-level actor context brings about different views and different concerns from key stakeholders, and insecurity in their respective tasks and services. The lack of understanding of these issues, as well as the gaps in the legal framework mentioned above, leads potentially to mistrust in and among all the actors involved. In addition, the current bilateral informalities taking place between law enforcement and private firms are counter-productive for the other actors and for the individual.

In the course of criminal investigations, **law enforcement authorities** are often facing the challenge of getting access to private data of suspects to be used as 'evidence'. The arguments advanced by law enforcement authorities is that having access to data stored on the Internet can enable them to trace back to offenders or take down servers with illegal content. Using the above-mentioned traditional method of mutual legal cooperation (Scenario 3) for getting access to data held by a private company located in another state is a very slow process, which law enforcement authorities are often tempted to circumvent, thus undermining the essence of the rule of law. Since the terrorist attacks of the 2000es, law enforcement authorities worldwide are trying to gain access to as much data as

[35] Bigo, D., Boulet, G., Bowden, C. et al (2012) Fighting cyber crime and protecting privacy in the cloud, European Parliament, PE 462.509, pp. 18, 37 & 46.

[36] Porcedda, M. G. (2012) Law enforcement in the Clouds: Is the EU Data Protection Legal Framework up to the Task?, in: Gutwirth, S., Leenes, R., De Hert, P. and Poullet, Y. (eds.), European Data Protection: In Good Health, Springer, 203, 206-207.

possible in order to fight terrorism and organised crime. This trend can directly challenge the fundamental rights of the suspects and the core principle of presumption of innocence.

For **private companies**, the three main concerns are liability, defamation and costs. If providers get assurances on these three levels, it is highly likely that they should be more willing to collaborate with law enforcement. The concept of legal certainty is key in the context of cross-border access to data stored on their servers, as private companies expect to be able to perform their activities under the rules of the country in which they have their headquarters. However, big companies offering services in several countries are already struggling to comply with disparate and/or conflicting rules on this issue. The search for legal certainty could partially explain why major Internet companies such as Facebook use guidelines for law enforcement agencies seeking records.[37]

The role of **data protection authorities** in this debate is key. A complex system of cross-border exchanges of data from private companies to law enforcement authorities creates a blurring of the responsibilities regarding the supervision of the lawful use of personal data. The multi-actor process complicates the allocation of this responsibility. The European Data Protection Supervisor and the Article 29 Working Party (WP29) do not have the legal competence to perform a supervisory duty of all data requests of law enforcement authorities across the EU.

And finally, where does this cooperation between different actors leave **the individual**? As said, law enforcement authorities gathering private data held by Internet companies in the EU therefore challenge the rule of law, and in that respect, the individual's fundamental right to data ownership in two ways: first, it creates a grey zone of legal uncertainty for the data subject as regards which data protection rules to use in cross-border cases. Secondly, it ignores the principle of individual consent as the collection becomes a matter of "bargaining" between law enforcement authorities and private companies as regards what type of data should be made available. The next section therefore addresses the challenges of the individual's data protection and privacy in the broader context of the notion of rule of law.

5. Challenges to the rights to privacy and data protection

Any law enforcement activity which risks impacting on individual fundamental rights even in the slightest way needs to be backed by the necessary safeguards. All modern democracies under the rule of law have set in place a system of checks and balances to ensure that any policy restricting civil liberties or fundamental rights is necessary and proportionate. Article 8 of the ECHR on the right to private and family life states that the only possible interference by a public authority with the exercise of this right must be in accordance with the law and necessary in a democratic society. The case-law of the ECtHR has, throughout the years, established a necessity and a proportionality test for each measure that could threaten the rights of individuals. The questions that need to be asked when

[37] For instance, Facebook's "Information for Law Enforcement Agencies": https://www.facebook.com/safety/groups/law/

assessing the massive gathering of data by law enforcement authorities are the following:

- Is this system the most optimal solution to achieve the goal of fighting terrorism and organised crime?
- Could less intrusive means accomplish the same objective?

The fact that data protection rules exist but are not applicable to the data collected because the data are considered as non-personal data ("metadata") is a clear example of how the informalities linked to the "bargaining" between law enforcement authorities and private companies profoundly endanger the core data protection principle of individual ownership of his/her data. Law enforcement authorities usually make the distinction between two types of data: the content and the "metadata". The term metadata refers to "data about the data" – which can be defined as the information on one or more aspects of the data, but not on the content of the data itself. In the case of a digital image, for instance, metadata include the size of the picture, the colour depth, the date of creation, etc. As data protection rules do not apply to metadata, law enforcement authorities have a preference for gathering metadata rather than personal data. A similar distinction is being used in the EU between personal data and "operational" data, to which data protection rules do not apply.[38]

The distinction between personal data and metadata becomes irrelevant when several sources of data about one individual are cross-referenced. A law enforcement authority can learn as much from metadata as from the private content of e-mail exchanges, Internet phone conversations (VoIP) or social networks' activities. Thus, a huge risk for the fundamental right to data protection is that operational data gathered and shared by law enforcement authorities in the EU without any safeguards for the individual might reveal personal information about him or her. Moreover, metadata might be more revealing than content.[39]

As a corollary to this observation, the informalities linked to the "bargaining" between law enforcement authorities and private companies as regards what data should be made available profoundly endanger the core data protection principle of individual ownership of his/her data. The question then becomes: who is the owner of the data requested? And how can individuals consent to their data being gathered?

6. Conclusions and policy recommendations

The key horizontal issue in this policy brief is the respect of the rule of law and of fundamental rights as enshrined in the EU Charter of Fundamental Rights. Rule of law normally defines how states operate and how the necessary checks and balances are implemented at the institutional level. The question of the public-private divide in the context of law enforcement cooperation with private companies

[38] See European Commission (2010), Overview of information management in the area of freedom, security and justice, COM(2011) 385 final, Brussels, 20.7.2010.

[39] Chavoukian, A. (2013) "A Primer on Medatata: Separating Fact From Fiction", Information and Privacy Commissioner Ontario, Canada, July 2013, http://www.privacybydesign.ca/index.php/paper/a-primer-on-metadata-separating-fact-from-fiction/

can thus be raised: are companies bound by rule of law or are states obliged to control companies in accordance with the principles of rule of law? More specifically, what does this mean for the individual and the required "informed consent" to collection of data when state authorities are siphoning information off from the private sector?

The massive gathering of data by law enforcement authorities needs to be limited and safeguards for the individual need to be put in place. A coherent legal framework is needed to ensure legal certainty for all actors involved, but the laws in place as regards data collection and data protection need to be implemented and monitored accordingly by a system of constant checks and balances. This is key for all the actors involved: law enforcement authorities need to know under what rules they can request data to private companies, private companies must be certain that the policies in place in the country where they have their headquarters will not challenge their commercial activities, and most importantly the right of the individual to own his data must not be forgotten. This is the only way the potential mistrust between all actors involved can be addressed.

This policy brief makes the following policy recommendations to EU policy-makers:

1) **More cooperation between law enforcement and private sector** is key, especially at EU level. A research project on the extent to which cooperation between law enforcement authorities and private companies takes place would be welcome. Different platforms for cooperation could also be explored at other levels, for instance at the level of the Council of Europe or even the United Nations in order to address the trans-continental cases of data gathering (such as PRISM).

2) **A clear rule of law approach** must be taken in the EU as regards policies in the field of police and judicial cooperation. The fact that data protection rules exist but are not applicable to the data collected because it is considered as non-personal data ("metadata") is a clear example of how a gap can threaten fundamental rights.

3) A **strong multi-actor strategy** is needed at EU-level, which takes into account the needs of all the different actors involved. EU policy-makers should seek the development of a common EU-level set of standards and guidelines applicable to practical cooperation between companies, law enforcement agencies and the judiciary. The role of EU Home Affairs agencies such as Europol, Eurojust, the EDPS, the WP29 and the FRA needs to be clarified. Moreover, a bottom-up approach should be developed, which would consist in providing an EU platform for sharing experiences and practical challenges experienced by law enforcement authorities, companies and judicial authorities in the IT sector.

4) **Strengthen the legal framework for jurisdiction, electronic evidence and data protection in the EU.** More work is needed to adopt a more comprehensive and robust EU legal framework applying to cooperation between private sector (especially IT companies and online service providers) and law enforcement authorities in Europe. The current General Data Protection package under negotiations should remain a package in order to ensure a coordinated legislative approach for both commercial and law enforcement aspects.

Co-ordinator:
Dr. Michael Friedewald
Fraunhofer Institute for Systems and Innovation Research ISI
Breslauer Straße 48 | 76139 Karlsruhe | Germany
Phone: +49 721 6809-146 | Fax +49 721 6809-315
michael.friedewald@isi.fraunhofer.de