Open Season for Data Fishing on the Web: The Challenges of the US PRISM Programme for the EU

Bigo, D.; Boulet, G.; Bowden, C.; Carrera, S.; Guild, E.; Hernanz, N.; de Hert, P.; Jeandesboz, J.; Scherrer, A.

Publication date
2013
Document Version
Final published version

CEPS POLICY BRIEF
30 years CEPS

Open Season for Data Fishing on the Web
The Challenges of the US PRISM Programme for the EU

Didier Bigo, Gertjan Boulet, Caspar Bowden, Sergio Carrera, Elspeth Guild, Nicholas Hernanz, Paul de Hert, Julien Jeandesboz and Amandine Scherrer

No. 293, 18 June 2013

The revelation of the top-secret US intelligence-led PRISM programme has triggered wide-ranging debates across Europe. Press reports featured in the Guardian and Washington Post have shed new light on the electronic surveillance 'fishing expeditions' (dragnet) of the US National Security Agency (NSA) and the FBI into the world's largest electronic communications companies. Sensitive data of citizens and residents of the European Union appear to have been monitored by US intelligence services since 2007. The purposes of this monitoring include the so-called 'fight against terrorism', but also, news reports allege, electronic espionage for political reasons, including the monitoring of civil society organisations in foreign countries.[1]

This Policy Brief addresses the main controversies raised by the PRISM affair and the most relevant policy challenges that it poses for the EU. A set of concrete policy recommendations is also addressed to the EU for implementing a robust data protection strategy in response to the affair. **Our argument is two-fold:**

[1] See title 50 of the US Code, Chapter 36, subchapter 1 'Electronic Surveillance', section 1801. Refer also to the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008, dealing with 'Foreign Intelligence Surveillance', in particular section 702 which deals with procedures for targeting certain persons outside the US other than US persons.

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. Gertjan Boulet is a Doctoral Researcher at the Research Group on Law, Science, Technology and Society (LSTS) at the Vrije Universiteit Brussel. Caspar Bowden is an independent advocate for information self-determination rights. Sergio Carrera is Senior Research Fellow and Head of the Justice and Home Affairs Section at the Centre for European Policy Studies (CEPS). Elspeth Guild is Associate Senior Research Fellow in the same section at CEPS and Jean Monnet Professor ad personam at Queen Mary, University of London as well as at the Radboud University Nijmegen, Netherlands. Nicholas Hernanz is Research Assistant at CEPS. Paul de Hert is Professor at the Vrije Universiteit Brussel and the Tilburg University. Julien Jeandesboz is an Assistant Professor at the University of Amsterdam and Associate Researcher at CCLS. Amandine Scherrer is European Studies Coordinator and Associate Researcher at CCLS.

First, the leaks over the PRISM programme have profoundly undermined **the trust and confidence** that EU citizens have in their governments and the European institutions to safeguard and protect the most fundamental freedoms related to their private and family lives. It has also shown the limits and loopholes of current EU data protection legislation with respect to data processing with third countries and cooperation among law enforcement/IT service providers both inside and outside Europe.

Second, the PRISM affair raises questions regarding **the capacity of EU institutions to draw lessons from the past**. This is hardly the first time that issues related to blanket retention and mass surveillance have surfaced in the European public debate. Although different in scope and outlook, tensions over PRISM are strongly reminiscent of the ECHELON and Carnivore controversies of the late 1990s and early 2000s. More recently, the Passenger Name Record (PNR) and Terrorist Finance Tracking Programme (TFTP) demonstrated the acute sensitivity of discussions on **the EU's capacity to protect the data of its citizens and residents in the context of transatlantic relations**. And last year, some co-authors of this Policy Brief also insisted on the dangers to the privacy of European citizens posed by the concurrence between the growing reliance on and embrace of cloud computing technologies as a central policy option for the EU's 'digital agenda' and legislation passed in the US concerning the data of non-US citizens, particularly under Section 702 of the 2008 Foreign Intelligence Surveillance Amendment Act (FISAA).[2]

1. What is PRISM about?

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.[3] The top-secret document leaked to journalists was reportedly used to train intelligence operatives on the functions and scope of the PRISM programme. The programme was introduced during the George W. Bush administration, following the disclosure of the NSA's 'warrantless wiretapping' activities by the New York Times in 2005.[4] The NSA had installed a computer on the premises of the AT&T switching centre in San Francisco, allowing the agency to plug and tap directly into the fiber optic cables through which Internet data traffic enters and leaves the United States.

The warrantless wiretapping programme was shut down in 2007 and 'legalised' the same year by the Protect America Act. The Act provided retroactive immunity to the telecommunications companies involved and allowed wiretapping to continue without individual warrants, conditional upon the approval of NSA procedures by the secret Foreign Intelligence Surveillance Court (FISC). A subsequent test case at the Foreign Intelligence Surveillance Court of Review (tasked with reviewing FISC decisions to deny applications for electronic surveillance warrants) confirmed that the Fourth Amendment of the US Constitution,[5] which requires any warrant for surveillance operations to be judicially sanctioned and supported by probable cause, only applied to surveillance directed at US persons.[6] The decision opened the way for the US Congress to enact FISAA §1881a authorising the mass surveillance of non-US foreigners outside

---

[2] D. Bigo, G. Boulet, C. Bowden, S. Carrera, J. Jeandesboz and A. Scherrer (2012), "Fighting Cybercrime and Protecting Privacy in the Cloud", study commissioned by the European Parliament, Brussels (http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050).

[3] See articles in the Guardian (www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data) and the Washington Post (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).

[4] This and the following points draw from C. Bowden (2013), "How to wiretap the Cloud without almost anyone noticing: FISAA, Data Protection and PRISM", speech delivered at 3rd Annual ORGcon, Open Rights Group, London, 8 June (https://orgcon.openrightsgroup.org/2013/videos). See also S. Braun, A. Flaherty, J. Gillum and M. Apuzzo (2013), "Secret to PRISM Program: Even Bigger Data Seizure', Associated Press, 15 June (http://tinyurl.com/lb5b4wc).

5 The Fourth Amendment to the United States Constitution is the part of the Bill of Rights that guards against unreasonable searches and seizures.

[6] Bigo et al., op. cit., pp. 33-34. (http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050).

US territory but whose data are in the range of US jurisdiction.

The programme allows the NSA to have access to communications and stored data in the servers of nine IT companies (designated as 'special source operations'): Google, Microsoft, Facebook, Yahoo, Skype, Apple, Paltalk, Youtube and AOL. The collected data on 'targeted foreign users' include, among others, email, chat, videos, photos, file transfers, social networking data and 'other special requests'. No further details have been reported regarding the exact nature and scope of this data. Media sources state that the NSA does not appear to have direct (so-called 'root') access to user data, and suggest the handling of requests differs from company to company. Possibilities for handling Section 702 requests vary from dealing manually with each query to installing an onsite box enabling NSA access to traffic, to uploading information through an NSA web terminal.[7] These uncertainties notwithstanding, one point is quite clear: PRISM has been enabled by reliance on cloud computing. In this sense, the PRISM affair is less about telecommunication interception, which was the main issue with the ECHELON affair for instance, than about accessing data thought to be processed 'in the cloud', but *de facto* circulating through the data centres of U.S. based companies.

We should learn more about the exact functioning of PRISM over the next few weeks, provided also that the findings of the Transatlantic Group of Experts, whose creation was announced on 14 June 2013 by Commissioner for Home Affairs Cecilia Malmström, build on a thorough assessment and are made fully public.[8] Discussion over the specifics of the programme's functioning, however, **should not obfuscate the central issue** that has stirred so much controversy following the disclosure of the PRISM affair: namely that **non-US citizens using the services of companies falling under the jurisdiction of the US government have consistently been the target of mass data collection for the purpose of foreign intelligence surveillance**.

Controversies over the exact scope of PRISM and its implications demonstrate that the current situation is one of **high legal uncertainty that poses a critical challenge to the fundamental rights of EU citizens.** The PRISM affair conjured a significant amount of indignation in the U.S. over the fact that its functioning could violate the safeguards afforded to US citizens under the 4th Amendment, and the so-called '51% test'.[9] Under FISAA section 702, however, non-US citizens are excluded from the scope of the 4th Amendment. Existing European instruments such as the data protection Directive, the Council of Europe's Convention 108 on the Protection of Individuals with regard to Automatic Processing of Personal Data or the Convention on Cybercrime, and the European Convention on Human Rights, do not apply. The PRISM affair further casts doubt over the sincerity and effectiveness of existing data protection and privacy measures regulating transatlantic flows of data, particularly the Safe Harbor principle. Finally, should news reports be confirmed that the United Kingdom's GCHQ (the British equivalent of the NSA) has been using data collected through PRISM for similar purposes, it is clear that this is not a problem that the US authorities alone can be easily and conveniently blamed for.

2. What are the main controversies around PRISM? Sovereignty, ownership and data protection

The first outstanding issue in the PRISM affair is the **loss of sovereignty over the information** held by the IT companies. The PRISM programme has reportedly allowed US intelligence authorities to spy on and have access to data stored about citizens and residents in the EU without the knowledge and express consent of its European counterparts, including the EU institutions and agencies, as well as member states' national governments. By doing so, American authorities have directly circumvented the 'rules of the game' in international relations, which require faithful cooperation by partner sovereign powers. A foreign state seems to have unlimited access to

[7] See e.g. A. Soltani (2013), "PRISM: Solving for X", 14 June (http://tinyurl.com/m5sau2v).

[8] C. Malmström (2013), "EU and US will set a transatlantic group of experts to discuss the U.S. programmes more in details", Dublin, EU-US Justice and Home Affairs Ministerial Conference, Dublin, 14 June, SPEECH/13/537.

[9] According to which data collection measures should affect 51% or more of non-US persons.

the lives of millions of EU citizens and persons legally residing in the Union's territory.

Mistrust transpires from the first reactions in the EU after the revelation of the affair. The German Justice Minister Sabine Leutheusser-Schnarrenberger called the programme "*alarming*" and pointed out that the "*fight against enemies of the state does not legitimate any means available*".[10] These reactions constitute only one example of the sovereignty dilemmas raised by PRISM. Similar concerns have been raised by the Vice-President of the European Commission and Commissioner for Justice, Fundamental Rights and Citizenship, Viviane Reding. In a letter sent to the US Attorney General on 10 June 2013, Reding asked for clarification on the PRISM programme and underlined that "*trust that the rule of law will be respected is also essential to the stability and growth of the digital economy, including transatlantic business*".[11] She also emphasised that programmes like PRISM can undermine the trust of citizens and companies and formal channels of legal assistance cooperation should be instead used, except in "*clearly defined, exceptional and judicially reviewed situations*".

PRISM has shown **a clear 'loss of control' in the EU and its member states over the sovereignty of this data and revealed a great deal of mistrust** on the part of European institutions and member states' national governments towards the US. This is particularly worrying in a policy domain ('the fight against terrorism') that has been highly political and controversial during the last 15 years of cooperation with Europe because of the challenges posed by the US policy to well-established European data protection and privacy standards and legislation. **The EU institutions and the US had already experienced substantial tension over the US acquisition, retention and use of data about EU citizens before PRISM**.

The first case involved Passenger Name Records (PNR) where, using the same *modus operandi,* the US authorities obliged private-sector actors, in this case airlines, to allow wide access to personal data of people flying to the US. In the end, after substantial negotiations, the EU institutions (including the European Parliament) ceded to most of the demands of the US and signed an agreement making the data collection and use lawful.[12] The second occasion was the SWIFT/TFTP affair, where the US authorities required another private-sector actor, SWIFT, to allow them wide access to information on electronic transactions of individuals and businesses around the world managed by the company for banks and other financial institutions. Once again, after negotiations and substantial pressure from the US authorities, all the EU institutions ceded to the majority of the US demands and settled an agreement legalising the information practices. The question might be raised as to whether the EU institutions will simply enter into an agreement making such personal data collection, storage and use lawful or whether they will take a more robust approach this time?

The second outstanding issue is related to **the ownership of the data and the protection of EU citizens' and residents' privacy**. Who owns the information and personal data stored by these IT companies? The existing European legal standards on data protection provide a fairly clear answer to this question. The EU Charter of Fundamental Rights and the European Convention of Human Rights expressly recognise the individual as the first owner of her/his personal data. Consent is therefore deemed to be a fundamental component in EU law with respect to lawful uses and processing of personal information, including law enforcement purposes. A majority of Europeans surveyed in a Special Eurobarometer Report on "Attitudes on Data Protection and Electronic Identity"[13] were concerned about the recording of their behaviour via payment cards (54% vs. 38%), mobile phones (49% vs. 43%) or mobile Internet (40% vs. 35%). 70% of them were concerned that their personal data held by companies could be used for

[10] See http://www.dw.de/pressure-on-merkel-to-talk-prism-with-obama/a-16876477

[11] Viviane Reding, Vice-President of the European Commission, Brussels, 10 June 2013, Ref. Ares(2013)1935546 - 10/06/2013.

[12] E. Brouwer (2011), "Ignoring Dissent and Legality: The EU's Proposal to Share the Personal Information of all Passengers", CEPS Paper in Liberty and Security in Europe, CEPS, Brussels.

[13] Eurobarometer (2011), "Attitudes on Data Protection and Electronic Identity in the European Union", Special Eurobarometer Report No 359, June (http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf).

purposes different from those for which it was collected. Moreover, more than six respondents out of ten (63%) declared that the disclosure of personal information constitutes a big issue for them. PRISM defies data protection and takes away the ownership of that data from the hands of European citizens and residents as data subjects towards distant territories and foreign authorities. A particular issue of concern however is the challenges inherent in data protection in the scope of social networks such as Facebook. How to ensure a meaningful ownership of people's personal data in the cloud, especially in what concerns social networks?

PRISM challenges the status of citizenship of the Union. As President Obama has indeed stated in his response to the leaking of the NSA secret document, the PRISM programme "*does not apply to US citizens and it does not apply to people in the United States*".[14] Only non-US persons outside the US are targeted by the programme. This tracking of 'suspected foreign terrorists' has, in Obama's view, respected a 'fair balance' between security and freedom. EU citizens and residents have been therefore amongst those targeted by these fishing expeditions and subject to a generalised suspicion which stands in tension with the presumption of innocence. One of the main differences between in the US and the EU is that the US legal system does not protect 'non-American citizens or residents' (including EU citizens) as data subjects. In contrast, in the EU data protection legal regime, *any* third-country national (including US citizens) should have access to data protection rights and effective remedies in cases of alleged violations by the authorities. In this way, the PRISM programme sends a clear message that all EU citizens and residents are at the mercy of US intelligence services. EU member states and institutions have therefore failed in protecting their citizens and residents against unlawful interference and mass surveillance by foreign authorities. Programmes like PRISM make the rights of citizens and residents in Europe ever more insecure and unsafe.

3. What are the policy challenges for the EU? Loopholes and shortcomings

A first policy challenge arises from **the legal gaps** revealed by the affair. The existing EU legislative framework does not cover transatlantic cooperation on data protection in the domain of police and criminal justice cooperation, or in what concerns European governments' collaboration with IT companies in these same law enforcement areas. This leads to a situation of severe legal uncertainty. There is currently no general legislative framework for the protection of personal data across the Atlantic in the area of police and judicial cooperation in criminal matters. The Agreement on mutual legal assistance between the EU and the US,[15] signed in 2003, includes in its scope the sharing of information already held by public authorities in both parties. The current data protection Directive (95/46/EC) governs the storage of data by private companies, but not the subsequent use and access for law enforcement purposes.[16] **The PRISM affair is thus unfolding in a legal grey area that current and forthcoming legislation does not seem equipped to address.**

The so-called **data protection reform legislative package** presented by the European Commission in 2012 is indeed composed of the general data protection Regulation (COM(2012)11) and the Directive (COM(2012)10) dealing with data protection in the fields of police and judicial cooperation in criminal matters.[17] The package is now in the hands of the European Parliament, which is acting as co-legislator in both legislative files. In general, the negotiation process is proving to be highly controversial and difficult because of the reticence shown by a majority of member states' governments and the concerns expressed by the private sector as regards the implications of a stronger European regulatory framework on data protection for their businesses.[18] On the other hand, the negotiations

[14] See the complete statement at www.whitehouse.gov/the-press-office/2013/06/07/statement-president

[15] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:181:0034:0042:EN:PDF

[16] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:PDF

[17] http://www.ceps.be/book/towards-new-eu-legal-framework-data-protection-and-privacy-challenges-principles-and-role-europ

[18] The original proposal by the European Commission did contain an express provision (Article 42) that would have

as regards the proposal for the Directive are being particularly contested, as this is a field where EU national governments remain hesitant to lose discretion in favour of European institutions. To this we may add the proposal for **an EU-US general agreement on the protection of personal data** when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism. No progress has been so far achieved because of fundamental disagreements between the parties involved regarding 'common standards'.

The Data Protection package does not seem to address the **fundamental lacuna in EU law and policy regarding private sector and law enforcement cooperation**. The scope of this cooperation should not be underestimated. According to statistics recently published by Reuters, the UK, France and Germany were in 2012 the top three countries behind the United States to request user data from Google, Microsoft, Skype and Twitter.[19] These figures are piecemeal, but they do suggest, alongside controversies over the involvement of the GHCQ in the UK, that the issues raised by the PRISM affair are not limited to the actions of the US government.

The EU does not have common standards applying to the cooperation between IT companies and law enforcement in the EU, which comes as a surprise when taking into account the fast pace at which European cooperation in policing has evolved since 1992. This creates legal uncertainty between the actors involved, which is not beneficial to any of them. The lack of clearly defined rules and standards of cooperation and relations in the EU leads to mistrust and a lack of clarity as regards the possibility for companies to allow access by national governments requesting information. It also safeguards their interest not to face liability for the potential violation of EU data protection rights and principles. Governments are not under a clear legal obligation to inform companies when they have informal access to this data.

An additional challenge relates to **the necessity and proportionality tests** of the PRISM programme. Is the programme necessary in a democratic society? Obama's reaction to the leaks of secret documents was to defend the US government's collection of data on the phone records of millions of Americans, declaring that in his view this was a "modest encroachment on the privacy" and one he thinks is both lawful and justified in order to identify terrorists plotting to attack the United States. Obama also called for an open discussion about "the balance between the need to keep the American people safe and our concerns about privacy". In determining the proportionality and the necessity in a democratic society of these mass surveillance measures directed at EU citizens and residents, the following questions can be raised: Can we really talk about a 'balance' in light of the rather disproportionate and mass-surveillance nature of the 'fishing practices' and the mass surveillance inherent in the PRISM programme? Is there oversight of the 'fishing expeditions' operated by the US intelligence services? Are these activities within the scope of the conferred powers and do they respect the fundamental principle of purpose limitation? Finally, is massive electronic surveillance the most efficient and least-restrictive policy option for law enforcement?

These questions should be familiar to EU and member State authorities, and are a matter of concern for EU citizens and residents. **Blanket collection and retention of personal data are hardly specific to US policy orientations and have been repeatedly called into question by European courts**. In March 2010, the German Constitutional Court abrogated the German national law implementing the so-called data retention Directive on grounds that it did not meet the criteria of proportionality for data security, purpose limitation, transparency, judicial control and effective legal remedies.[20] Meanwhile, notions such as intelligence-led policing, **'data-sharing by default' or the principle of availability** endorsed in various EU

made the processing of information to third countries conditional on the use of a mutual legal assistance agreement and the authorisation by a competent data protection authority. After strong lobbying by the US government, however, the article disappeared and only a recital in the Preamble has so far remained covering transfers of data to third countries.

[19] http://reuters.tumblr.com/post/52817521108

[20] K. De Vries et al., *Proportionality overrides unlimited surveillance: The German Constitutional Court judgment on data retention*, CEPS, Brussels, May 2010.

strategy and policy documents foresaw mass collection and retention of personal data in the developing European model of law-enforcement cooperation. The challenge, here, lies in the possibility to reconsider these policy orientations in the light of new developments and to assess the actual need for and proportionality for such schemes.

A final, yet still central policy challenge is that of **'cloud computing'.** Two points in particular warrant consideration, as discussed below.

On the one hand, cloud computing involves the **processing of information and data in remotely located computers and/or data centres** accessed through the Internet. In itself, this notion defies traditional European privacy guarantees and safeguards in the framework of international transfer of data and cooperation between law enforcement authorities and private sectors. As argued in the previously cited study conducted for the European Parliament (Bigo et al., op. cit.), cloud computing challenges the 40-year old model applicable to international data transfers, i.e. *the safe harbour principle*. This principle allows data transfers to US organisations that demonstrate an adequate standard of protection. In the case of cloud computing, however, data subjects who are clients of IT companies are caught in a complex matrix of contracts where the determination of legal responsibilities, application of adequate standards and potential liabilities in cases of data protection violations are difficult if not impossible to ascertain in practice.[21]

The second point, on which the PRISM affair has shed a particularly bright light, is that cloud computing is not only an issue of remote data *storage*, but also of **remote *computing***. Cloud providers spent a considerable amount of resources in money, energy and CPU cycles on formatting, indexing and otherwise organising the data of their customers. In the case of PRISM, these resources have been harnessed to provide the NSA with the information it required. What seems to be happening, in this regard, is a variant of Platform-as-a-Service (PaaS), where a governmental agency delegates the task of scalable mass surveillance to cloud providers themselves.

4. What should the EU do? Policy Recommendations

1. **Strengthen the legal framework for data protection in the EU.** All the relevant European institutions should work harder in the smooth development of a more comprehensive and stronger EU legal framework and common standards applying to first, international transfers and processing of data and second, cooperation between private sector (especially IT companies and online service providers) and law enforcement authorities in Europe. The PRISM affair might well provide the necessary political momentum and boost for speeding up the ongoing negotiations on the Commission's data protection legislative package, including not only the Regulation but also the Directive. Both legislative instruments should incorporate express provisions covering international transfers and private-sector law enforcement cooperation and aim at the strongest data protection standards.

   The general data protection Regulation should include a provision stipulating the legal requirements applicable where a judgment of a court or tribunal (or any decision by an administrative authority) from a third country requires a data controller/processor to transfer personal data of EU citizens and residents. These should be only recognised and enforceable if there exist a mutual assistance treaty or international agreement in force between the requesting country and the EU, and after the verification by relevant EU data protection authorities.[22]

   Special attention should be particularly paid to better ensuring proper guarantees and

[21] For a study of the political and legal challenges of cloud computing in the fight against crime refer to D. Bigo, G. Boulet, C. Bowden, S. Carrera, J. Jeandesboz and A. Scherrer (2012), Fighting Cybercrime and Protecting Privacy in the Cloud, European Parliament, Brussels http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050

[22] As stipulated in Amendment 259, Article 43a of http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-501.927+04+DOC+PDF+V0//EN&language=EN

effective remedies in hands of individuals (effective and enforceable rights) whose data protection and privacy might have been violated in these contexts. Social networks constitute a particularly challenging case in point from the perspective of privacy and data protection. Users of 'social networks' should be offered a 'right to be informed' when their data are transferred to third countries. This could consist for instance of including standardised logos or pop-up icons/box (presenting multi-layered formats) informing the user that her/his data have been transferred/processed to a third country by using a clear, plain and adapted language, allowing them the possibility to object or consent. The general data protection Regulation proposal should reincorporate this obligation as originally proposed by the Draft Report of the European Parliament.[23] Moreover, the situation of third-country nationals residing in the EU, who are also subject to increasing processing of personal data in the EU, should constitute also a central focus point. A key issue here is the ways in which this EU framework of protection is being implemented (or not) in practice.

The nationality or country of residency should not be a constitutive factor here for the individual to have access, rectify or challenge her/his data. Non US-citizens or residents should be allowed effective judicial remedies. The Commission should make sure that EU data protection standards, and the negotiations in the current EU data protection package, are not undermined as result of the Transatlantic Trade and Investment Partnership (TTIP) agreement with the US.[24]

2. **Safeguard the rights of users of cloud computing.** An accountability approach (vesting of obligations and potential liabilities to every actor with power or knowledge about the access, use, transfer/processing of data) should be applied here. This should be accompanied by a concrete tool to ensure that individual users of cloud services are properly informed of the risk that their private data might be used by US authorities without their consent. One approach could be to design a pop-up on Internet websites that would warn the user that her/his data might be subject to surveillance or when that information leaves the EU. Also, the safe harbour principle should apply to telecommunications companies and carriers. The Commission should review its recent Communication "Unleashing the Potential of Cloud Computing in Europe" (Brussels, 27.9.2012 COM(2012) 529 final) in view of the recent revelations and consider, together with European stakeholders, alternatives such as the establishment of a 'European Cloud' and 'European Facebook'. Social media and the Internet are today's' critical infrastructure and should receive proper protection accordingly.

3. **Introduce a solid legal framework regulating third-country data transfer/processing.** Strong rules applying to third-country data transfers/processing should constitute another central component deserving immediate policy and legislative attention. The use of existing legal channels should be favoured, such as the one applicable to mutual legal assistance. This should be accompanied by an injection of increased momentum in the negotiations on the EU-US agreement on data protection and privacy, which are currently frozen. Here, the EU should not compromise its own European privacy standards and data protection principles in favour of those currently prevailing in the US.

[23] See Amendment 118 of Article 11 of the proposal, which has now surprisingly disappeared during the negotiations (http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-501.927+04+DOC+PDF+V0//EN&language=EN). See also the Opinion of Article 29 Data Protection Working Party, 15/2011, on the definition of consent, 13 July 2011, which also includes this idea to be offered to the user of social networks to select the use of data to which s/he agrees, including transfer to third parties, p. 18 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf).

[24] See http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B7-2013-0187&language=EN

4. **Implement standard-setting and sharing of experiences: A multi-actor approach**. Legislation alone, however, would not provide an all-encompassing solution to the current controversy and the challenges pointed out in this Policy Brief. Legislation must be supplemented by the development of a common EU-level set of standards and guidelines applicable to practical cooperation between companies, law enforcement agencies and the judiciary. A multi-actor approach should be the one preferred and developed as should also a bottom-up approach. This would consist of providing an EU framework for sharing experiences and practical challenges experienced by law enforcement authorities, companies and judicial authorities in the IT sector.
5. **Put in place a policy infrastructure at EU level capable of dealing with these kinds of revelations.** There is a need for the European Parliament to reflect critically about its capacity to deal with these controversies. What lessons have been learned from the Echelon event: political upheaval, a Parliamentary inquiry and then very little follow-up and impact. A more systematic policy follow-up is needed, including a protection scheme for whistleblowers. The European Parliament should open an enquiry into the whereabouts, implications and follow-up of the PRISM affair. This could be accompanied by an inter-parliamentary delegation to the US in connection with the Transatlantic Legislators Dialogue (TLD). In this context, consideration should be given to setting up an inter-parliamentary commission between the European Parliament and the US Congress to debate ways forward to address the challenges raised by PRISM.