Submission

by

the European Digital Rights Initiative (EDRi) &
Fundamental Rights Experts Group (FREE)

to

the United States Congress,

the European Parliament, the European Commission & the Council
of the European Union,

& the Secretary-General & the Parliamentary Assembly
of the Council of Europe

on

the surveillance activities of the United States and certain European States' national security and "intelligence" agencies

August 2013

EDRi/FREE submission

To the United States Congress, the European Parliament and Commission & the Council of the European Union, and the Secretary General & the Parliamentary Assembly of the Council of Europe ***on the surveillance activities of US and certain European national security/"intelligence" agencies***

Note on the choice of addressees:

EDRi and FREE submitting it to the addressees mentioned on the cover page for the following reasons:

- **US Congress** is ultimately responsible for providing democratic oversight over the activities of the US Executive. It has established a *Privacy and Civil Liberties Oversight Board* (PCLOB) consultation on FISA and the PATRIOT Act. However, while we are sending a copy of this submission to that consultation, this document is addressed to the Speaker of the **House of Representatives** and the President *pro tempore* of the **Senate** because we argue that the issues raised can only be addressed properly by the establishment of a special investigation committee of Congress, with appropriate support and powers. We also wish to stress that, whatever the defects in the scope of protection afforded to non-US citizens under the US Constitution, the USA, as parties to the UN International Covenant on Civil and Political Rights and the Council of Europe Cybercrime Convention, are bound under international law to extend privacy protection to non-US citizens and to observe the principles of legality, necessity and proportionality also in their surveillance activities.

- The **European Parliament** is responsible for providing democratic oversight over the activities of the European Union, and has taken a keen interest in the issues raised, as has the **European Commission**, which forms the executive branch of the EU. However, the **European Council** (representing the governments of the EU Member States) has been less demanding. We are calling for all of them to seek to establish the full truth about the relevant laws and practices, in both Europe and the USA. We are aware of the "national security" exemptions in the main EU treaties, but these are not and should not be absolute, or seen as granting Member States total exemption from scrutiny in this regard. The EU Charter on Fundamental Rights, which has fundamental status in the EU (even in relation to UN Security Council decisions) and explicitly demands full protection of personal data, cannot be simply ignored in this context. Ultimately, it is for the European Court of Justice to determine the scope of the exemption, but we already note that the US' NSA's activities are manifestly not limited to national security as defined in international law. We are therefore urging the EU bodies to address the issues to the fullest extent possible within their legal competences.

- The **Council of Europe (CoE)**, as the oldest, broadest European institution, has the main responsibility for upholding human rights and the rule of law throughout the territory of its 47 Member States. Its mandate, in particular in relation to human rights and the upholding of the European Convention on Human Rights, does *not* exclude matters relating to national security. On the contrary, the standards that we cite in our submission have been mainly developed by the **European Court of Human Rights** in its case-law under the Convention. All European States are legally obliged to "secure" full protection of these rights and freedoms. Within the Council of Europe, responsibility for the upholding of these standards is shared between the **Secretary-General** and the **Committee of Ministers** (representing the CoE Member States), the **Parliamentary Assembly of the Council of Europe** (PACE), and the Court.

Effective action on the issues addressed in this submission will require the involvement of all of the above. For that reason, we address this submission to all of them.

EDRi/FREE submission

To the United States Congress, the European Parliament and Commission & the Council of the European Union, and the Secretary General & the Parliamentary Assembly of the Council of Europe ***on the surveillance activities of US and certain European national security/"intelligence" agencies***

I. General:

1. The activities of national security agencies in Europe and the USA, and the arrangements under which they cooperate, have been outside the scope of effective democratic oversight and outside clear legal frameworks for too long; they must be brought under the Rule of Law.

2. For Europe, that means those activities must be made to comply, in law and in practice, with the relevant minimum European human rights standards developed by the European Court of Human Rights under the European Convention on Human Rights (ECHR) summarised below, at II, and in Attachment 1. At present, it appears that several European States are not complying with these standards.

3. These European constitutional standards are in line with the global (UN) standards enunciated by the Human Rights Committee acting under the UN International Covenant on Civil and Political Rights (ICCPR) and others, briefly noted in Attachment 2. All European States and the USA are parties to the ICCPR in particular.

4. For the USA, this means that it, too, should bring its activities in line with these standards. As a first step, US surveillance law and practice (in relation to surveillance of both US citizens and non-US/European citizens) must be made totally clear, and any divergence from those standards must be made public. Only that will allow for sensible discussions on how to bring those activities into line with international standards. Current US law as far as currently known is summarised below, at IV, and in Attachment 3.

II. European requirements: (For more detail, see Attachment 1)

5. If an agency of any European State is given powers under the laws of that State to gather information on (the communications- or other data of) anyone, be that within Europe or not, then that activity must be regarded as being done "within the jurisdiction" of the State concerned.[1] This means that, in relation to any surveillance activity by any European State, on anyone, wherever they are, the State in question must comply with the minimum European standards, set out in Attachment 1, which are directly derived from the ECHR case-law.

6. Moreover, from a European perspective, any spying on Europeans and non-Europeans living in Europe, by any non-European State, anywhere in the world, should meet the same minimum European-constitutional and the similar UN standards, set out in Attachment 2.

[1] Note that this is the case, even if the exercise of that jurisdiction would violate the sovereignty of another State, e.g., because it concerned data in another country (cf. the *Lotus* case, referred to in para. 7): the fact that the act was contrary to international law of course does not mean that the State perpetrating the act is not bound by its human rights obligations; that would be perverse. The point we make here is that in the circumstances described, the State is bound to comply with the European Convention on Human Rights, because the acts concerned are "within its jurisdiction". While generally territorial in nature, this concept also covers acts carried out by State bodies within their home country (or territories of the State overseas) under domestic legislation that affects individuals in other countries.

7. Non-European national security agencies should not seek or gain direct access to any personal data held in Europe (e.g., by asking US companies to "pull" data from their Europe-based servers, or to allow US agencies to query the data in Europe, and hand over the results): that infringes the sovereignty of the relevant European States (PCIJ, *Lotus* judgment, pp. 18-19).[2] Instead, they should seek such access through bi- or multilateral assistance treaties, under arrangements similar to Mutual Legal Assistance Treaties (MLATs) for law enforcement agencies; and those treaties should in substance and process conform to the minimum European-constitutional and international standards.

8. Failure of a European State to prevent improper spying by non-European countries constitutes a breach of that country's "positive obligations" under the ECHR. Active support for, complicity in, or even passive condoning of such spying would breach the State's primary obligations under the ECHR.

9. In addition, European States and the European Union should ensure that personal data on Europeans and non-Europeans living in Europe, if held on US-based "cloud" servers, will be accessible to the US national security agencies **only** on the basis of clear and published provisions of treaty arrangements that also meet those European-constitutional and international standards.

III. USA requirements: (For more detail, see Attachment 3)

10. The First and Fourth Amendments to the US Constitution in principle guarantee the right to free speech and freedom from unreasonable searches to US citizens. However, even domestically, this protection is weakened by the "third party" doctrine on personal data and the relaxed "pen/trap" rules on searches. Secret rulings of the FISA Court reportedly further erode these rights, arguably in unconstitutional ways. Those rulings are being challenged in the US courts. Here, we may note that current US law and practice, even with regard to spying on US citizens, falls short of European and international standards.

11. Moreover, it has become clear that non-US citizens outside the USA do not enjoy even the limited protections of the First and Fourth Amendments: they can be spied upon arbitrarily by US agencies, without any meaningful substantive or procedural limitations, in clear breach of international standards on privacy generally, and on privacy and freedom of expression on the Internet in particular. Under international human rights law, those guarantees should be afforded to "everyone" affected by the measures.

IV. How to address the issues: our demands

[2] This is also the view of the vice-president of the European Commission, Viviane Reding, who issued a statement on 25 July 2013, saying: "*The [EU's new General Data Protection Regulation] will also provide legal clarity on data transfers outside the EU:* ***when third country authorities want to access the data of EU citizens outside their territory, they have to use a legal framework that involves judicial control. Asking the companies directly is illegal. This is public international law.***" See: http://techcrunch.com/2013/07/25/ireland-prism/ (emphasis added)

12. The ultimate aim should be for both the US and the European legal systems to offer high-level privacy/data protection to "everyone", in line with the established European minimum standards (set out in Attachment 1), that are also in line with UN standards (set out in Attachment 2); and for those standards to be adhered to in practice by the USA, all European States, and the EU, whether acting independently or jointly.

To this end, we demand urgent action from both the US and the European institutions.

Demands for review and redress from the USA:

i. Clarity about the law, and honesty about practice:

13. We demand complete transparency in relation to the scope and detail of US spying activities, and of the bi- and multilateral arrangements between the USA and other States and international organisations, in particular "5EYES"[3], Atlantic and/or European ones, relating to this activity, under which data on the communications and Internet activities of European citizens are intercepted, held, recorded and/or monitored and analysed.

14. We demand complete clarity about the limitations of the US legal system, and in particular as concerns the apparent fact that it provides insufficient protection to US citizens, and effectively none to non-US citizens. Following such a full clarification, urgent measures should be taken to bring the US surveillance system fully into line with international human rights- and privacy/data protection standards.

ii. The way to achieve this:

15. While we appreciate the establishment of the PCLOB consultation, we do not believe that this is the appropriate forum or process to achieve the required full transparency, or that it will lead to US law and practice being brought fully into line with the requirements of international law.

16. To be more specific: we are joining US civil liberty organisations in calling on the US Congress to establish a properly staffed **special investigatory committee**, on the lines of the 1970s CHURCH Commission, with the power to subpoena witnesses and documents; and to make arrangements to ensure that European institutions, States and NGOs can fully participate in the investigation carried out by this special committee, and indeed in the drawing up of the mandate for this committee.

iii. The changes to be made

17. Senior European politicians have called for the extension of US legal protections afforded under US constitutional and federal law to (communications) data on US citizens, to (communications) data on European citizens held in the USA or accessed from the USA by US agencies, just as data on US citizens, held in Europe, is already protected under European human rights- and data protection law.

[3] The alliance of intelligence operations between the USA, UK, Australia, Canada and New Zealand.

18. Reciprocity is indeed an important element in international relations. However, in the present context, this fails to recognise that while, in respect of their data, Europeans currently enjoy hardly any protection under US laws, the protection accorded to US citizens under those laws is also deficient, and falls below European and wider international minimum requirements. Raising the level of US legal protection for data on Europeans to the level of protection of data on US citizens therefore still leaves European citizens and US citizens subject to a regime that falls short of international standards. That is not enough.

19. We are joining civil liberty organisations in the USA in calling for fundamental changes in US law, to ensure proper protection under the law against non-transparent and undemocratic surveillance. New laws must be introduced at federal level to provide much stricter rules, open judicial warrants and rulings, and full democratic control, in accordance with international human rights and privacy/data protection standards. Specifically, we demand that when such laws are in place, they should afford equal protection to US and non-US citizens.

20. Until this is achieved, the USA cannot be said to offer "adequate" protection to data, in relation to any of the areas for which the European Commission has (wrongly) held it to offer such protection: the "Safe Harbor", the disclosure of PNR data, and the making available of SWIFT data (see below, para. 29).

Demands for review and redress from Europe:

i. <u>Clarity about the law, and honesty about practice</u>:

21. European States are not blameless when it comes to surveillance: in spite of a much stronger legal regime on paper (under the ECHR), it appears that practice in some (perhaps many) European States also fall seriously short of the European-legal (ECHR) requirements. Several States, in particular the UK, also seem to have worked closely with the USA (in particular, in ECHELON) in establishing a global surveillance network that appears to blatantly violate European and international law. **We need complete clarity about the laws in the EU- and Council of Europe Member States, and complete clarity about the treaties entered into by European States, and full, honest disclosure about the practices of the national security agencies and –bodies of the EU- and Council of Europe Member States too.**

ii. <u>The way to obtain this</u>:

EU:

22. The European Parliament has a crucial role to play. We welcome the European Parliament's decision to establish a committee of enquiry within the Civil Liberties Committee, and urge it to be broad, to encompass all the threats posed to the rights of European citizens by foreign and EU Member States' surveillance activities.

23. We also - but very cautiously and with serious reservations - note the establishment of an EU-US "expert group" to look at these matters. However, we oppose the excessively limited mandate of this group, and demand full transparency about its composition and activities. We demand civil society involvement and complete

openness for the work of this group. Without that, its findings and the arrangements it might propose are likely to be incomplete, will lack credibility and, consequently, will be unacceptable.

24. Although this should be obvious, for the avoidance of any doubt, the EU should make clear, as a matter of urgency, that any disclosure of data on European citizens that is subject to European data protection law (such as financial or airline data, or Europol/Eurojust/etc. data) to, or any access to such data by, national Member States' national security agencies (NSAs), and *a fortiori* by third country agencies, is subject to the European data protection rules governing the processing of such data.

Council of Europe

25. We note the fact that the Council of Europe, which Europe's main human rights guarantor, is not excluded from addressing matters relating to national security that may affect the human rights of European citizens and indeed of "everyone" affected by measures of CoE Member States. On the contrary, the European standards set out in Attachment 1 have been developed by the European Court of Human Rights in what is now established case-law, applicable to all Council of Europe Member States (which includes all EU Member States), and indeed to the EU itself (albeit, for now, still indirectly, through "general principles of Union law" and the EU Charter).

26. Specifically, we call on the Secretary-General of the Council of Europe to exercise his power under Article 52 ECHR to demand of all CoE Member States full disclosure of "the manner in which [their] internal law[s] ensure[s] the effective implementation of" Article 8 of the ECHR in relation to surveillance of electronic communications- and Internet data by their national security agencies; and on the CoE Commissioner of Human Rights, PACE, and NGOs to be fully involved in this enquiry.

iii. The changes to be made

27. Until the full truth has been established, and full, appropriate remedial action has been taken to bring the activities of all relevant US agencies in line with international standards, there can be no close cooperation between US and European agencies, or between US and European State's agencies on the previous, essentially unregulated basis.

28. *Immediate changes:* Given that, as noted above, in para. 20, in the light of the recent revelations, the USA cannot be said to offer "adequate" protection to data in relation to the "Safe Harbor", the disclosure of PNR data, and the passing on of SWIFT data, the current arrangements are in clear and blatant breach of the primary law of the European Union and, consequently, the EU is legally obliged **to immediately suspend all US-related European data protection "adequacy" decisions.**

29. *Changes to the General Data Protection Regulation:* Pending adoption of adequate legislation in the USA, European data protection law should ensure that European citizens are clearly warned that, if they provide data to US companies, or to global Internet companies that have links to the USA, use servers in the USA, or are

otherwise subject to US FISA and other surveillance orders, their data will not be safe from arbitrary, intrusive surveillance by US agencies. This is already proposed by senior EU officials and legislators in relation to the General Data Protection Regulation currently in the process of being adopted. We endorse that proposal.

30. *New treaty arrangements on cooperation between national security agencies:* The post-WWII treaties and arrangements on "national security" and "intelligence" cooperation (including the definitions of these matters) are totally outdated. We need a complete overhaul of the national and inter-State arrangements on "national security" and "intelligence" cooperation. The old treaties - UKUSA, 5EYES, NATO and others - should be openly discussed and reviewed, and fundamentally changed to bring them into line with the international standards we have adduced. Without that, we do not live in the free and democratic societies we are made to believe we live in.

- o – O – o -

EDRi and FREE are grateful to Professor Douwe Korff of London Metropolitan University for drafting this paper.

EUROPEAN DIGITAL RIGHTS

Rue Belliard 20, B-1040 Brussels,
Tel:+32 2 274 25 70
E-Mail: brussels@edri.org,
http://www.edri.org

European Digital Rights (EDRi)

European Digital Rights is an association of 35 digital civil rights organisations from 21 European countries. We work together to defend civil rights in the information society.

11 Rue Darwin
1190 Bruxelles
E-Mail: edecapitani@gmail.com

The Fundamental Rights European Experts Group (FREE Group)

The Fundamental Rights European Expert Group is an NGO whose focus is on monitoring, teaching and advocating in the European Union freedom security and justice related policies.

http://www.eafsj.org	

Attachment 1:

SUMMARY OF EUROPEAN HUMAN RIGHTS STANDARDS ON NATIONAL SECURITY SURVEILLANCE:

The case-law of the European Court of Human Rights under the European Convention on Human Rights (ECHR) shows the following considerations and requirements of European human rights law relating to surveillance:[4]

- A system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it.
- The mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied.
- In view of these risks, there must be adequate and effective guarantees against abuse.
- The first of these guarantees is that such systems must be set out in statute law, rather than in subsidiary rules, orders or manuals. The rules must moreover be in a form which is open to public scrutiny and knowledge. Secret, unpublished rules in this context are fundamentally contrary to the Rule of Law; surveillance on such a basis would *ipso facto* violate the Convention.

The following are the "minimum safeguards" that should be enshrined in such (published) statute law, and adhered to in practice:

- the offences and activities in relation to which surveillance may be ordered should be spelled out in a clear and precise manner;
- the law should clearly indicate which categories of people may be subjected to surveillance;
- there must be strict limits on the duration of any ordered surveillance;
- there must be strict procedures to be followed for ordering the examination, use and storage of the data obtained through surveillance;
- there must be strong safeguards against abuse of surveillance powers, including strict purpose/use-limitations (e.g., preventing the too-easy disclosure of intelligence data for criminal law purposes) and strict limitations and rules on when data can be disclosed by NSAs to LEAs, etc.;
- there must be strict rules on the destruction/erasure of surveillance data to prevent surveillance from remaining hidden after the fact;

[4] See the cases of *Klass v. Germany* (Judgment of 6 September 1978), *Weber and Saravia v. Germany* (Admissibility Decision of 29 June 2006), *Liberty and Others v. the UK* (Judgment of 1 July 2008), and *Kennedy v. the UK* (Judgment of 18 May 2010). See in particular the summaries in *Weber and Saravia*, paras. 93 – 95, and in *Kennedy*, paras. 151 – 154 (which quote *Weber and Saravia*, paras 93 – 95, thus reemphasising that the approach there summarised is now regarded as settled case-law).

- persons who have been subjected to surveillance should be informed of this as soon as this is possible without endangering national security or criminal investigations, so that they can exercise their right to an effective remedy at least *ex post facto*; and
- the bodies charged with supervising the use of surveillance powers should be independent and responsible to, and be appointed by, Parliament rather than the Executive.

Under the ECHR, these principles must be applied to anyone who is affected by surveillance measures taken by any Council of Europe Member State under domestic law.

In addition, European States have a "positive obligation" to protect their citizens from surveillance contrary to the above, perpetrated by any other State. *A fortiori*, they are under a legal obligation not to actively support, participate or collude in such surveillance by a non-European State.

- o – O – o -

Attachment 2:

BRIEF NOTE ON WIDER UNITED NATIONS/INTERNATIONAL STANDARDS ON NATIONAL SECURITY SURVEILLANCE:

Attachment 1 above summarises the European Court of Human Rights' standards set for "national security" surveillance. Here, we briefly note that the same standards are also reflected in law and guidance issued at the global level by the United Nations, and by other international organisations, albeit not always in the same detail.

The primary instrument in this respect is the UN International Covenant on Civil and Political Rights (ICCPR or "the Covenant"), the most important binding global human rights treaty, to which all European States and the USA (indeed, almost all UN Member States) are parties. It is applied and interpreted by the Human Rights Committee, which has issued important relevant guidance.

Further important guidance has been provided in the 1996 Johannesburg Principles on National Security, Freedom of Expression and Access to Information (drafted by Article 19 and other NGOs but endorsed by the UN Special Rapporteur on Freedom of Opinion and Expression) and more recently in statements and reports by that Special Rapporteur and special rapporteurs from other international organisations. Also relevant is the guidance issued by the Organisation for Security and Co-operation in Europe (the OSCE), to which again all European countries and the USA (and Canada) are parties.

Here, it may suffice to note that all of these stress the same core principles as are stressed by the European Court of Human Rights:

- **"national security" must be defined narrowly** (see the "Tenth Anniversary Joint Declaration" by the UN Special Rapporteur on Freedom of Opinion and Expression, together with the OSCE Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information; also the Johannesburg Principles, Principle 2(a) as well as Principle 1.2);
- any interference with the freedom to seek, receive and impart information by any medium (including the Internet), including e-communications- and Internet surveillance, must be based on "**law**", i.e., on **clear and specific, *published* legal rules** (and *published* legal interpretations of the rules): an interference with privacy and communications can be "arbitrary" - and thus in breach of international human rights law, including the ICCPR - even if it is in accordance with domestic law;
- the law must limit any such the interference to what is "**necessary**" and "**reasonable**" or "**proportionate**"; and
- the law must provide for an "**accessible and effective remedy**" against the interference.

  On all of the above, see General Comment 16 on Article 17 ICCPR, paras. 3 and 4; General Comment 31 on General Legal Obligations Imposed on States Parties to the Covenant, para. 15ff.; and the reports by the Special Rapporteur *passim*).

- the requirements of "law", "necessity" and "proportionality" also apply in relation to measures taken to protect **national security** (Johannesburg Principles, Principles 1.1.(a) & (b), 2(a) & (b)).

Moreover, in assessing the questions of "necessity" and "proportionality" in particular, the Human Rights Committee and the UN Special Rapporteurs will take into account exactly the same kinds of factors as are listed in the case-law of the European Court of Human Rights.

Two related matters deserve special mention in the present context: the application of international human rights law to the extraterritorial accessing (or "pulling") of data from servers in another country; and the duty to extend the rights enshrined in the ICCPR to all individuals without distinction as to nationality or other status. Specifically:

- Article 2(1) of the ICCPR requires all States Parties "*to respect and to ensure to* ***all individuals within its territory and subject to its jurisdiction*** *the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.*"
- In the view of the Human Rights Committee:

> This means that a State party must respect and ensure the rights laid down in the Covenant to **anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party**. ... **[T]he enjoyment of Covenant rights is not limited to citizens of States Parties** but must also be available to **all individuals, regardless of nationality or statelessness**, such as asylum seekers, refugees, migrant workers and **other persons**, who may find themselves in the territory or **subject to the jurisdiction of the State Party**. (General Comment 31, emphasis added)

- Although the Committee has not yet issued any further views or general comments on the matter, it must be assumed that if a State gives itself legal powers to access (or "pull") data on individuals, when those data are situated outside its physical territory, that State is "exercising jurisdiction" (to be specific: "enforcement jurisdiction") extra-territorially, in the State where those data are located. As noted in the body of this paper with reference to the *Lotus* case, if this happens without the consent of the other State, it violates the sovereignty of that other State. Here, it should be noticed that that aside, such extra-territorial action by the first State would also mean that that State is asserting "jurisdiction" over those data. In respect of their data, the individuals concerned are made to be "*subject to [the State's] jurisdiction*".
- In any such extra-territorial cross-border accessing (or "pulling") of data, the State in question must therefore comply with all the general requirements of the Covenant (clear, foreseeable "law"; "legitimate aim", "necessity" and "proportionality"), and with the requirement of Article 2(1), that it affords the protection of Article 17 to the persons affected irrespective of their nationality or other status.

In sum: The UN standards are fully concordant with the European ones set out in Attachment 1.

- o – O – o -

Attachment 3:

SUMMARY OF UNITED STATES STANDARDS ON NATIONAL SECURITY SURVEILLANCE:

In the USA, communications data and personal information on US citizens (and on some minor categories of non-US citizens living in the USA) are in principle granted protection under the First and Fourth Amendments to the US Constitution, providing protection of free speech and freedom from unreasonable searches.

However:

1. There is no general, cohesive, broadly-applicable federal privacy law. Rather, there is only a largely incoherent and sectorally-based patchwork for federal and state laws, which provide serious privacy protection only in certain areas and respects. See: Chris Hoofnagle, Country Study on the USA, prepared for a wider EU study on *New Challenges to Data Protection*, at:

   http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B1_usa.pdf

2. The Electronic Communications Privacy Act (ECPA) allows for the monitoring of communications "meta" data (data on the devices involved in the communications, time, duration, location, etc., but not the contents of communications) on the basis of a "pen register or trap and trace device" warrant, that will be issued on the basis of simple certification by a government attorney that such information is "relevant" to an "ongoing criminal investigation"; there is no need to show "probable cause", and there is no meaningful judicial oversight. This is because in *Smith v. Maryland*, the Supreme Court ruled that use of a pen register does not constitute a search, and is thus not protected under the Fourth Amendment. The surveillance carried out under ECPA, even on US citizens, is extensive and includes massive amounts of e-communications data. For further details, see: Douwe Korff, Presentation on behalf of EDRi at the EU – USA Privacy Conference, Washington DC, 19 March 2012, available at:

   http://edri.org/files/korff120319.pdf

3. The PATRIOT Act and FISA Acts allow even more extensive surveillance over US citizens. Even on their face, the rules in these Acts fall far short of international-legal requirements. However, the rules have been even further weakened, to the extent that they now reportedly provide hardly any constraint at all, even in respect of US citizens, in relation to national security and "foreign intelligence" matters, by means of secret rulings by the secretive FISA Court. See: New York Times, 6 July 2013, In secret, court vastly broadens powers of NSA, at:

   http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html?nl=todaysheadlines&emc=edit_th_20130707&_r=1&

4. The constitutionality of these secret FISA Court rulings is doubtful, and they are being challenged in the US courts. See: http://www.aclu.org/national-security/fix-fisa-end-warrantless-wiretapping and http://epic.org/privacy/terrorism/fisa.

5. In any case, and most worrying to Europeans, the First Amendment does not protect the relevant rights of non-US citizens not in the USA (so-called "excludable aliens"):

> **"[T]he interests in free speech and freedom of association of foreign nationals acting outside the borders, jurisdiction, and control of the United States do not fall within the interests protected by the First Amendment."**
>
> (*DKT Memorial Fund Ltd. v. Agency for Int'l Dev.*, 1989, quoted in *Chevron Corporation v. Steven Donziger et al.*, U.S. District Judge Kaplan order of June 25, 2013).

6. Non-US citizens not resident in the USA similarly do not benefit from the protection of the Fourth Amendment, which does no apply if the person affected by a "search" does not have a "significant voluntary connection with the United States (*US v. Verdugo-Urquidez*, 1979). Like the First Amendment, the Fourth Amendment only protect "the people", i.e., US citizens and some eligible (US-resident) aliens.

7. Finally, the FISAA §1881a allows US agencies, including in particular the NSA, to capture and trawl through any data, including e-communications and Internet data, of or on any non-US citizen with essentially no constraints. All that is required is that the capturing and trawling does not inadvertently relate for more than 50% to US citizens, and that the data that are being looked for are "of interest" to "foreign affairs matters" of the USA: the exercise of these essentially arbitrary powers is not limited to serious offences or terrorism, or to threats to US (or US allies') national security. See the report by Caspar Bowden et al. to the European Parliament, Fighting Cybercrime and Protection Privacy in the Cloud, 2012, and the subsequent article by him and Judith Rauhofer, Protecting their own: Fundamental rights implications for EU data sovereignty in the cloud, 2013, available at, respectively:

   http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050

   http://ssrn.com/abstract=2283175

In sum: The US Constitutional Amendments' protections (as applied) and US Federal and State laws fall short of international standards. Under ECPA and the PATRIOT and FISA Acts, as further weakened by the secret rulings of the FISA Court, even US citizens enjoy little protection against widespread and intrusive surveillance by US national security agencies in relation to over-broadly-defined "intelligence" matters, in particular in relation to "meta" communications data and Internet data. In relation to US citizens, this may be unconstitutional. But non-US citizens outside the USA enjoy not even the (already too low) protection accorded to US citizens: they can effectively be spied upon arbitrarily, without any meaningful substantive or procedural limitations. Moreover, the US surveillance activities under FISAA in particular do not appear to be limited to matters of "national security", properly (restrictively) defined, for neither US citizens or non-US citizens.

- o – O – o –