Douwe Korff
Professor of International Law
London Metropolitan University
London (UK)
d.korff@londonmet.ac.uk

EU – USA PRIVACY CONFERENCE

WASHINGTON DC, 19 MARCH 2012, SESSION 1

PAPER EXPANDING ON A SHORT INTERVENTION ON BEHALF OF THE EUROPEAN DIGITAL RIGHTS INITIATIVE (EDRi)

www.edri.org

Caveat:
The views expressed in this paper are the author's and do not necessarily reflect the views of EDRi.

Session 1: Privacy protection – approaches to addressing similar challenges in different legal systems and traditions

The European Union and the United States face similar challenges regarding privacy at a time when many individuals are concerned by increased data collection, online tracking and profiling and fear losing control of their data. The EU has decided to clarify and modernise its data protection legislation. The US is also assessing its approach to privacy. Where do the partners stand and what can we build on for the future?

STRUCTURE

1. This paper, like my short intervention, is divided into three parts:
   - An overview of the common challenges facing Europe and the USA (and indeed the rest of the world);
   - A summary of the issues in Europe; and
   - A summary of the issues raised by U.S. law and practices, viewed from a European perspective.

   At the end, I provide a Summary & Conclusions.

THE CHALLENGES

2. In a report I carried out for the European Commission in 2010, with Ian Brown of the University of Oxford and a number of world-wide experts, including Chris Hoofnagle of the University of California, Berkeley, we noted a number of **fundamental global challenges to data protection and informational privacy, arising from a variety of interconnected technological, political and policy developments**, which can be summed up as follows:[1]

[1] Cf. the Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, European Commission, 2010. The reports, working papers and country reports prepared for this study can all be found on the Commission's website, at: http://ec.europa.eu/justice/data-protection/document/studies/index_en.htm (under the date 20.01.2010). The challenges summarised in the bullet-poinst have been somewhat updated in the light of further research by Ian Brown and me.

- the increasingly unthinking **pervasive generation, collection, analysis and use of personally identifiable data**, for myriad purposes, without inherent incentives to minimise the data collection or the data retention/storing, or to strictly limit those purposes (keywords: Social Networking Sites, "smart" phones, RFIDs, "the Internet of Things");
- the **ever-increasing intrusiveness of such data**, either because of their nature (location data, biometrics, genetic or even genomic data) or because of their sheer size or coverage (e.g., Facebook data, browsing/search histories, lifestyle databases), or because of the context (e.g., political interests and -activism, or sexual orientation), or because of the way they can be linked (e.g., the ever-easier "matching" of photographs and other possibly remotely-captured biometrics to identities);
- the ever-easier and ever-increasing **interconnecting, matching and analyses** of these (in origin disparate) data, leading to the creation of ever-more-sophisticated "**profiles**" of individuals, for commercial and public purposes - and the dangers inherent in relying on such profiles (keyword: base rate fallacy);
- the ever-increasing difficulty of achieving real **anonymisation** of such data, and the misleading use of terminology ("masked-out data"; data in "sealed envelopes"; "largely anonymised data") which is intended to suggest that data are not re-identifiable when in fact they are;
- **globalisation**, which inherently involves the global dissemination of personal data on an unprecedented scale, and the related phenomenon of **cloud computing**, which also inherently involves the sending of massive amounts of data to servers anywhere in the world, but in particular in the USA, and which changes the balance of power from controllers to what are nominally processors;
- the increased **blurring of the lines** between general public tasks (such as improving health, education or welfare) and law enforcement tasks; the **additional blurring of the lines** between law enforcement and national security tasks, especially in relation to the fight against terrorism; the old phenomenon of **extending measures** adopted to fight (often already ill-defined) acts of "terrorism", first to even less-defined "extremism", and then to lawful political activities of opponents to State policies (Cobler: *der vorverlegte Staatschutz*, 1976), and the related phenomena of:
  - the massively increased **use of private-sector data for public-sector purposes**, by public-sector entities including law enforcement and national security agencies, and:
  - the increasing **legal duties imposed on ISPs and e-communication services to capture and retain private-sector data** for law enforcement and national security purposes, coupled with:
- the proliferation of **surveillance technologies**, from CCTV to the tracking of Internet browsing, to the recording and analysis of Internet traffic- or e-communication data, to comprehensive "trawling", "mining" or "scraping" of data from all kinds of sources (as noted above), for all kinds of purposes:
  - for purportedly **innocuous purposes** such as website traffic analysis to improve customer satisfaction and web design;
  - for more **intrusive private-sector uses** such as behavioural advertising and –marketing and to facilitate differential pricing; and

- for highly intrusive surveillance **to identify "targets"** for law enforcement or national security/anti-terrorist purposes (including "No-Fly" lists); and
- for the purposes of **State repression**, arrests and torture of dissidents and "extremists", and even extra-judicial killings, including by "drones".

3. *Data protection and informational privacy are not the only defences against all the dangerous trends noted above, but without serious, comprehensive, global, strict, binding, and strongly enforced data protection and privacy rules, covering private-sector entities, public-sector entities, and the data flows between them, world-wide, it is impossible to counter them.*

EUROPE:

4. In Europe, data protection is a **fundamental right**, firmly rooted in the European equivalent to the U.S. Bill of Rights, the European Convention on Human Rights and in the EU Charter of Fundamental Rights, in which it is also made a special right *sui generis* (Article 8). The right to data protection is strongly endorsed in the case-law of the European Court of Human Rights, the EU Court of Justice, and the constitutional courts of many European States.

5. Under European human rights law, this right applies to "**everyone**", and not just to citizens or residents of European states. Data on U.S. citizens, held by EU-based companies or authorities, are fully subject to the protection of the ECHR, the CFR, and the Council of Europe and EU data protection instruments.

6. European data protection law is built on a set of broad **core principles** enshrined in Council of Europe Convention No. 108, in the EU Data Protection Directives and –rules (including "Third Pillar" rules), and in national constitutional (case-)law.

7. But on these broad principles has been built a strong structure of **detailed rules**, giving real meaning to the principles in terms of purpose-specification and limitation (the principle at the heart of European data protection law); data quality; when consent is required or when personal data can be processed on the basis of "law" - and what the "quality requirements" of "law" are in that regard; how, when, and in what detail data subjects must be informed of processing; rights of access, correction and objection; rules on disclosures and secondary uses of personal data (also for law enforcement and national security); and the application of those detailed requirements in transnational contexts (i.e., in relation to activities of non-European controllers that impact personal data on individuals in Europe, and in relation to transfers of data from the EU to the USA and other "third countries").

8. Moreover, the broad principles and detailed rules are supposed to be **rigorously enforced** by competent, independent authorities, armed with strong powers of supervision (including powers of seize and search), direction (including powers to order cessation of processing), co-regulation (including approving of codes), and procesecution.

9. In view of the strong constitutional status of data protection in Europe (at both the European level and at the level of national constitutions), these basic tenets of European data protection law - **tight substantive rules built on firm core principles, rigorously enforced** - are essentially non-negotiable: ***Europe legally, morally and politically cannot and should not accept an erosion of these basic constitutional European data protection tenets in the context of globalisation, pervasive personal data processing or the world-wide fight against crime and terrorism.***

10. The above is not to say that all is perfect or indeed quiet on the European front - far from it. Civil society and human rights organisations have for a long time been deeply concerned about **evasion of the strict rules, and betrayals of the basic principles**, by the EU and European states, in many contexts, even in terms of the texts of the relevant laws (and unduly broad exceptions and exemptions); about **wide divergencies** between the laws; about **weak enforcement** of the laws in several countries; and about the **special weakness of the transnational arrangements** (i.e., the arrangements concerning transborder data flows and concerning the application of European rules to non-European actors ["applicable law"]).

11. We therefore agree that European data protection law needs a **fundamental shake-up**, both as regards the former "First Pillar" (processing in an economic context, especially by companies) and as regards the former "Third Pillar" (processing in relation to law enforcement). In addition, disclosures of data from these areas to the further area of **national security purposes**, and processing of data (including thus-obtained data) for these purposes cannot be left outside all European protection, but rather must be subject to the same core principles, also clarified in detail and also strictly enforced (albeit of course with regard for the special context).

The proposed EU Data Protection Regulation:

12. **EDRi generally welcomes the draft Data Protection Regulation**, insofar as it seeks to strengthen data protection in the EU with much more consistency between Member States, through stronger procedures, and with more effective enforcement. In relation to the topic of today's conference, we welcome in particular the proposed rule that stipulates that the Regulation will apply also to:

    - non-EU (including U.S.) companies that specifically offer goods and services to EU citizens and residents online; and
    - non-EU (including U.S.) companies and Government agencies that "monitor the behaviour" of EU citizens and residents. (Article 3(2) of the draft Regulation).

13. EDRi also welcomes in principle the serious attempt in the draft Regulation to ensure **consistent application** of the provisions in the Regulation, but fear that the proposed procedures lack transparency and give too much devolved powers to the European Commission, also in the matter of **"adequacy" determinations**, including assesments of arrangements such as the "Safe Harbor", which have been shown to be ineffective in practice (see para. xx, below). Open debate, with full input from civil society and others, including national and EU parliamentarians must be actively facilitated.

14. EDRi also has a number of **further concerns**, which must be addressed and resolved in a fundamental-rights-compatible way. The ones most directly relevant to the EU – USA relationship and arrangements are:[2]

    - the lack of even a simple reference to the **Council of Europe Convention No. 108**, which is the only existing *binding* international data protection instrument open to all States, including the USA: we believe that the main objective of the EU – US negotiations should be to have the USA sign up to, and implement legislation fully in accordance with, this open, international treaty (as shortly to be amended and improved);

[2] EDRi's full "*Initial comments on the proposed EU Data Protection Regulation*" can be found on the EDRi website, at: http://www.edri.org/CommentsDPR. More detailed and comprehensive comments on the Regulation are in preparation (as are comments on the proposed Law Enforcement Data Protection Directive, which apart from one brief mention we do not address in this paper at all yet).

- the apparently legally unavoidable total exclusion from the Regulation - *and from the Law Enforcement Data Protection Directive* - of processing of personal data for "**national security**" purposes (because all matters pertaining to national security are said to be completely outside of the European Union legal framework): we believe that the disclosure of personal data to law enforcement and national security bodies, both within the EU and (especially) in "third countries" (including the USA), and the processing of personal data by such bodies, should be extremely tightly controlled by EU- and wider European law;

- the totally avoidable continued separate application of the e-Privacy Directive and the Data Retention Directive, outside the framework of the new Regulation, which means that processing and retention of **e-communications data, including traffic- and location data**, by ISPs and e-communication service providers, and disclosures of such data to third parties, including law enforcement and national security bodies (in the EU and elsewhere), will continue to be covered by dozens of different national laws: we believe that the rules on the processing and disclosing of such data should also be fully harmonised, and strictly controlled, in, or under, the Regulation, and that compulsory suspicionless mass surveillance (as under the current Data Retention Directive) should be abolished and replaced with an also strict and harmonised expedited data preservation regime under judicial control;

- the regulation of **trans-border data flows**, particularly with regard to cloud computing, which appear to allow for transfers in circumstances in which full protection of the data and continued compliance with EU law is not ensured: we believe that the EU should insist on legally binding assurances and technical measures to ensure that U.S.-based companies offering cloud hosting services will not be able to disclose personal data to U.S. Government authorities without the *knowledge and consent* of the relevant EU-based controllers *and* Data Protection Authorities. Using U.S.-based cloud services that will not, or cannot, provide watertight and verifiable assurances to that effect should be unlawful; and more specifically:

- the fundamental flawed suggestion that **binding corporate rules** (BCRs), and even BCRs for processors, could achieve the above, when they manifestly cannot do so (see para. xx, below); and

- the arrangements on **DPA jurisdiction and cooperation**, which place the main responsibility for overview over controllers in the hands of one DPA, the DPA of the country of establishment of the controller if the controller is a EU entity, or the DPA of the the country of establishment of the representative in the EU of the controller if the controller is a non-EU entity, although subject to a system of joint investigations by and cooperation between all the relevant DPAs. While we welcome the idea of joint investigations and cooperation, we feel that the ultimate outcome of cases involving data on data subjects from several (or in the case of online services and monitoring, often all) EU Member States should not be left primarily in the hands of any one DPA; that will inevitably lead to forum-shopping by non-EU (in particular major U.S.) corporations: we believe that in cases involving data on data subjects from several or all EU Member States, the outcome should take the form of a joint decision of all relevant DPAs, with cases in which they could not agree being referred up to the ECJ.

UNITED STATES OF AMERICA (From a European perspective):[3]

Constitutional law:

15. There is no explicit, comprehensive concept of privacy or data protection on the European lines (where, as we have seen, it has turned into a constitutional *sui generis* right) in the U.S. Constitution.

16. That is not to say that privacy rules and -rights cannot be derived from the Constitution. As far back as 1965, the Supreme Court recognized a "zone of privacy" created by the "penumbras" of the First, Third, Fourth, Fifth, and Ninth Amendments (*Griswold v. Connecticut*, 381 U.S. 479 (1965)), and many courts of appeal have recognized a right to information privacy in the US Constitution.

17. However, from a European perspective the concept appears undeveloped in U.S. constitutional law, in particular because it has to fit in and compete with other constitutional requirements in ways that are quite different from the European legal approach.

18. In particular, institutions (such as banks or car rental firms, or even pharmacists) who obtain "voluntary" information from their clients are given extremely wide protection under the First Amendment to do with the information whatever they want, irrespective of the purpose for which they originally obtained it. The main exception in this regard appears to be any self-imposed restriction: if a company declares to a customer that it will use the customer's data for certain specified purposes, but not for other specified purposes (or for no other purposes), the company is bound by this assurance under "fair trading" rules that can be enforced by the FTC. But that is self-imposed, albeit statute-backed restraint; it is far from a legal requirement to abide by such purpose-limitation, and certainly not a constitutional requirement.

19. Moreover, as Justice Sotomayor pointed out in the very recent case of *United States v. Jones* (No. 10-1259, 23 January 2012), for now, Fourth Amendment jurisprudence still essentially "treat[s] secrecy as a prerequisite for privacy", and information "voluntarily disclosed" by an individual to someone else, or to some institution such as a bank, is still normally denied Fourth Amendment protection. This is the result of the so-called "third-party doctrine" which establishes that people have no expectation of privacy in the documents they share with others:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed. (*United States v. Miller*, at 443)

[3] This section draws (and in parts simply repeats) a note I wrote on comments by the US Ambassador to the EU at the hearing of the European Parliament's LIBE Committee on "Data Protection in a Transatlantic Perspective", Brussels, 25 October 2010. This in turn drew on the Country Report on the USA, produced by Chris Hoofnagle for the EU Study into "New Challenges to data protection", mentioned in footnote 1, above. The note is available from the European Parliament's website at: http://www.europarl.europa.eu/meetdocs/2009_2014/organes/libe/libe_20101025_1500_audition.htm. The Country Report on the USA is available from the European Commission's website, at: http://ec.europa.eu/justice/data-protection/document/studies/index_en.htm (under the date 20.01.2010, scroll down to Country Reports/Non-European countries and jurisdictions).

20. The above applies *a fortiori* to any information that is made public by the data subject him- or herself, e.g., on a Social Networking Site: it effectively looses all privacy protection.

21. In *Jones*, only Justice Sotomayor seemed to be willing to consider changing this approach. As she put it, with references to other cases:

> I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection. See Smith, 442 U. S., at 749 (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes"); see also Katz, 389 U. S., at 351–352 ("[W]hat [a person] seeks to preserve as private,even in an area accessible to the public, may be constitutionally protected").

However, this is tentative at most: the Justice felt that, in the case at hand, this matter needed not be settled, as it could be decided on a narrower basis, as was done by the majority. And it is in any case certainly not (yet) the view of a majority of the Court: on this (as on certain other issues), Justice Sotomayor is very much an outrider (or more advanced, as Europeans would see it).

22. The main approach outlined above contrasts starkly with European data protection law, under which personal data are always in principle protected, even if they are made public (although of course the level of protection may vary); and under which the core issue, also and even for public data, is still always the issue of purpose-specification and –limitation. Institutions such as banks or car rental firms or employers are strictly limited in the personal data they are allowed to collect, and in the uses and disclosures of such data. ***This quite simply is not the case under U.S. constitutional law.***

23. Last but far from least, there is the serious question of whether U.S. constitutional guarantees, even where they might exist, actually extend to non-U.S. citizens. From a European (and indeed, any non-U.S.-) perspective, it is one of the most disturbing features of U.S. policy in the fight against terrorism, that it has consistently sought to deny constitutional-legal protection to non-U.S. citizens: *Guantanamo Bay* is merely the most egregious example of this, but it is also demonstrated by the limitation of concern even by civil liberty organisations to the interception of phone calls *of U.S. citizens*, and even to the extra-judicial killing, by drones, *of U.S. citizens*. ***The underlying assumption, apparently shared even by civil liberty lawyers, is that the U.S. Constitution protects U.S. citizens from undue searches, undue arrests, imprisonment without charge or trial, extra-judicial killings, and mass surveillance and monitoring of communications - but that none of that applies to people outside the USA, who are essentially "fair game".*** This is in stark contrast to the modern human rights principle that States must accord the guarantees in international human rights treaties to "everyone" in respect of whom they take action (as is the approach also taken in Europe, as explained earlier).

Legislation - general:

24. When it comes to lower-ranking law, the situation is patchy: privacy law in the USA is a disparate patchwork of Federal and State-, common- and statute law. In some areas covered by federal law (such as cable tv), and in some State constitutions and -laws, there are some protections that come somewhere near to the European standards. However, even in the better-protected areas (which mostly relate to private-sector

controllers), standards do not really meet the European ones, especially again when it comes to the (to us Europeans, absolutely core) requirement of "purpose-limitation".

25. What is more, these laws all tend to contain sweeping exemptions in respect of disclosures of data by private-sector entities to law enforcement and anti-terrorist agencies. And outside of these special fields, as we have seen, there is essentially no protection against such disclosures, because of the "third-party doctrine".

26. In addition, there is inadequate oversight and enforcement by independent authorities (cf. the discussion of the "Safe Harbor" in para. xx, below).

27. Until and unless U.S. laws that seek to provide privacy to individuals are seriously tightened up, especially as concerns purpose-limitation and clauses concerning disclosures of data to U.S. Government agencies, and properly enforced, also when data on E.U. citizens are being processed, they fall far short of European standards, and can in no way be considered "equivalent" to European data protection laws, or "adequate" in terms of transborder data transfers.

The Privacy Act, the ECPA, the PATRIOT Act and FISAA

28. The (Federal) Privacy Act too does not really come close to the European standards, even when its terms are fully appicable (which in important respects they are not, as noted below). To quote Chris Hoofnagle:[4]

> The Privacy Act governs how federal government agencies collect, use, and disseminate personal information of citizens. Like the FCRA [Fair Credit Reporting Act], the Privacy Act reflects a broad range of Privacy Guidelines. However, much of its impact has been limited through liberal employment of a "routine use" exception, which has allowed agencies to transfer personal information without violating the statute. A routine use is one that, "is compatible with the purpose for which it was collected." This exemption has been so liberally applied that agencies have crated "blanket routine uses" that apply to every information system housed at the agency. For instance, the Department of Defence has created a list of 16 such uses. Thus, any system of records, no matter its content or context, can be disclosed for law enforcement, counterterrorism, historical archives, and for the "Information Sharing Environment." Specific systems of records may contain their own routine uses, meaning that discretionary information sharing can be quite broad and determined by the agency itself, rather than by Congress.

29. But more important even than that, the Privacy Act is explicitly limited to data on US citizens and permanent residents. In that regard, before the European Parliament,[5] the U.S. Ambassador to the EU referred to "the controversy over whether or not the Privacy Act protects EU citizens". That was disingenious: there is no "controversy" about this: the Privacy Act expressly and explicitly excludes its application to data on non-US citizens and -residents (unless one is talking about EU citizens living in the USA, which would be fatuous). The only "controversy" is about whether this exemption is justified. We submit it is not, and that until the Privacy Act is considerably strenghtened, with the "routine uses" examption removed for starters, and fully extended to data on non-U.S. citizens held by U.S. corporations and Government agencies, U.S. privacy law cannot even begin to be considered even basically compatible with European data protection standards.

---

4 Country Report on the USA for the "New Challenges to data protection" study, see footnote 3, above.

5 At the LIBE Committee hearing mentioned in footnote 3, above.

30. In that respect, it is worth noting that the Ambassador categorically rejected the idea that the Privacy Act might be reviewed:

> "Congress will not re-open the Privacy Act. It is not going to happen."

If this is true, it will kill all meaningful negotiations on EU – USA privacy cooperation.

31. The Electronic Communications Privacy Act (ECPA) allows for the monitoring of "mega" communications data (data on the devices involved in the communications, time, duration, 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". This is the lowest requirement for receiving a court order under any of the ECPA's three titles; there is no need to show "probable cause". 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 ruling held that only the content of a conversation should receive full constitutional protection under the right to privacy, since pen registers do not intercept conversation. There are no good, complete and reliable statistics on the use of these easily-obtainable warrants. (see: http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html under the sub-heading "The stats don't cover all forms of law enforcement surveillance".)

32. The surveillance carried out, even on U.S. citizens, is extensive and includes massive amounts of e-communications data:

> Internet service providers and telecommunications companies play a significant, yet little known role in law enforcement and intelligence gathering.
>
> Government agents routinely obtain customer records from these firms, detailing the telephone numbers dialed, text messages, emails and instant messages sent, web pages browsed, the queries submitted to search engines, and of course, huge amounts of geolocation data, detailing exactly where an individual was located at a particular date and time.
>
> These Internet/telecommunications firms all have special departments, many open 24 hours per day, whose staff do nothing but respond to legal requests. Their entire purpose is to facilitate the disclosure of their customers' records to law enforcement and intelligence agencies -- all following the letter of the law, of course.
>
> (http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html)

33. One ISP, Sprint, apparently maintains an "electronic surveillance group" of some 110 staff, purely to serve the "millions and millions" of requests from law enforcement. Reportedly, Sprint even built a special portal that "lets officials log in and pull down all kinds of info on millions of customers without any questioning or hand-holding from the carrier," while AT&T "had let the NSA build a secret room in one of its network facilities, for the purpose of snooping Internet traffic." (see:

(see, e.g.,: http://arstechnica.com/telecom/news/2009/12/sprint-fed-customer-gps-data-to-leos-over-8-million-times.ars; http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html; http://www.wired.com/cloudline/2011/12/us-cloud/ - and many other webpages).

34. Given the cavalier manner in which these kinds of data are surveilled on a massive scale even as concerns U.S. citizens, it would be more than surprising if ECPA in any way restrains the U.S. law enforcement-, or even less the U.S. national security agencies, in the monitoring of similar information on non-U.S. citizens.

35. Until the massive loophole of "pen register and trap and trace" warrants is removed from ECPA, it too can in no way be considered to offer protection even remotely similar to European data protection law.

36. The PATRIOT Act further undermined such limited restrictions as there were (under the Privacy Act, ECPA and basically all other laws) on the disclosure and use of data held by any private company or public authority to law enforcement and anti-terrorist agencies. Most pertinent to the present discussion are the "National Security Letters" that can be issued under the PATRIOT Act, under which the FBI can demand disclosure of customer records held by banks, telephone companies, Internet Service Providers, and others, and at the same time order them to tell anyone about their receipt of the NSL. According to EPIC, "the Number of NSLs issued has grown dramatically since the Patriot Act expanded the FBI's authority to issue them." (http://epic.org/privacy/nsl/).

37. Furthermore, under the Foreign Intelligence Surveillance Act (FISAA) 2008, s. 1881a, the US government can conduct unlimited surveillance on the data of Europeans, without any suspicion of criminality, in respect of entirely lawful democratic political activities. Under this section, cloud companies can be ordered to extract the data of EU citizens and hand them over to without any meaningful guarantees against such strategic surveillance by foreign governments.

38. And to top it all, there is no transparent, independent oversight, and no real, effective control over these activities, and no effective way to challenge the outcomes of these activities: see the discussion of the proposed PNR agreement, below.

39. Overall, under the PATRIOT and FISA Acts, U.S. law enforcement and national security agencies are actively "Hoovering up" massive amounts of personal data on non-US citizens (and sometimes, illegally, on US citizens too - which seems to be the only time there is an outcry over this in the USA), and they use them in truly scary programs, including "profiling" and "threat-" or "risk-assessment" programs, with little or no constraint or oversight. Yet the outcomes of this unfettered and unreliable processing of truly enormous amounts of personal data do affect (non-US) individuals, in that they feed into the US "no flight"- or "watch"-lists (or worse), without offering them any effective remedy.

40. We agree with serious concerns expressed by companies, States and civil liberty organisations in many countries that it is unsafe for non-U.S. companies or entities to have their data hosted by any cloud host (service provider) whose servers are in the USA, or who is otherwise subject to U.S. jurisdiction: there is quite simply no guarantee under current U.S. law that the data hosted on such cloud-host's servers will not be accessed by U.S. law enforcement and national security agencies under NSLs. Such access would not be limited to data on people reasonably suspected of involvement in terrorism, but rather, could include mass disclosures of data for "data mining" or "trawling" exercises; and it would be kept secret from the non-U.S. (*in casu*, European) controller and data subjects.

Special arrangements:

41. Finally, we must consider a number of special arrangements which are said, by the U.S. authorities, to offer adequate protection to EU citizens, and the new White House proposal for a "Consumer Privacy Bill of Rights", which it is claimed will do the same on a larger scale in future.

The "Safe Harbor"

Safe Harbor

PNR Agreements

The proposed Consumer Bill of Rights