The Regulation of IT-Privacy in the European Union[1]

By Prof. Dr. *Wolfgang Zankl*, Vienna[2]

Content: Data Protection, Data Retention, NSA

Privacy

The basic privacy regulation in Europe goes back to the Data Protection Directive 95/46/EC. It regulates the processing of personal data regardless of whether such processing is electronically automated or not. This legal act builds the keystone of European data protection law. At general personal data should not be processed, except when certain conditions are met. These conditions can be classified into the categories:

- Transparency: the data subject shall have the right to be informed if his/her personal data is being processed.
- Legitimate purpose: personal data may only be processed for specified explicit and legitimate purposes and shall not be processed further in a way incompatible with legitimate purposes.
- Proportionality: personal data may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which the data are collected.

This Directive has been supplemented by several other Directives, especially in the field of telecommunication, and by the **E-Privacy Directive** 2002/58/EC, which deals with the regulation of a number of important issues such as confidentiality of information, treatment of traffic data, spam and cookies.

But still the basic concept of European data protection goes back to the Data Protection Directive 1995. It goes without saying that this regulation has been drafted in a technical environment that has, especially regarding the internet, nothing to do with the IT-world we live in today: Many technologies, such as the web 2.0 and most devices (like smartphones) or services we use today, such as Google, Amazon and

[1] This paper is based on a presentation delivered by the author at the Chinese University of Hong Kong on November 16th 2013.

[2] Wolfgang Zankl is a professor at the department of civil law at the University of Vienna (www.zankl.at), former Dean of the Law School of the UFL University of Liechtenstein and founder/head of the european center for e-commerce and internet law (www.e-center.eu), one of the world´s leading think tanks for IT-law operating in Vienna, Berlin, Brussels, Hong Kong, London and New York.

Social Media, like Facebook, have not been invented or even been thought of back in 1995. So it was only a matter of time until the EU had to set up modern data protection standards. This has been done in the past two years and lead to a draft of a **new Data Protection Act** which has been amended on October 21.[3] It is – being a draft – still work in progress, so just the major issues will be pointed out:

1. **Explicit consent** of users that their data will be processed or being passed on.
2. The so called **right to be forgotten** (meaning that users have a right that, especially versus Google and Facebook, all their data shall be deleted upon request) will not come into force. It had been considered in a former draft but the final draft does not regulate it any more, which was a good thing to do as this right would have been hard to be enforced, anyway. Just think of the many ways and channels content is distributed all over the web. It is almost impossible to trace each and every content or picture so that such a right would not have made sense.
3. **The fines** resulting from violations will be severe, reaching up to 5% of the world´s revenues of the company being found guilty of such violations, the problem being that not only deliberate but also negligent infringements shall be fined.
4. **Privacy by Design**: Companies are required to offer their services in such a way, that they acquire as less data of users as possible, and the privacy settings have to be in favor of the user, meaning that he has to actively change such settings if he wishes to submit data. Privacy by design also means the user´s right to interact anonymously[4].
5. **Less bureaucracy:** the requirement to appoint a data protection officer will not depend on the number of employees of a company but on the number of data processings.
6. **One-Stop-Shop**: EU-citizens can appeal to the data protection authorities of their own country, even if the violation has is origin in a foreign (European) country. Companies on the other hand have to cooperate only with the data protection authorities of the (member) states where their head office is located.

---

[3] 2012/0011(COD), http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf (draft); http://www.europarl.europa.eu/document/activities/cont/201305/20130508ATT65776/20130508ATT65776EN.pdf (proposal).

[4] In contrast to the Real Name Policy which has been introduced recently for example in China: http://thenextweb.com/asia/2012/12/28/china-approves-regulations-that-introduce-real-name-registration-for-all-internet-users/; also http://www.huffingtonpost.com/2012/12/28/china-real-name-registration_n_2373808.html and http://www.cpcchina.org/2013-01/04/content_16082234.htm.

7. **Right to information and transparency**: Users shall receive understandable information on how their own data are being processed or how the provider is going to transfer them.
8. **Transfer of data to third countries**: Companies like Google are only allowed to transfer data to third countries, as long as this takes place according to European law or an agreement, based on European law.
9. **Future-proof definitions**: All information that can be directly or indirectly linked to a person or used to single out a person from a larger group, are defined as personal information and shall be protected.
10. **Harmonized enforcement of rules**: A "race to the bottom" in EU member states with weak law enforcement will not be possible, because there is a new European Data Protection Board.

What is the result of these developments? Except from point 6 (one-stop-shop) it seems to bring along a rather significant intensification of data protection requirements. Considering other requirements in e-commerce[5], Europe is gradually becoming an overregulated area making it a rather unattractive place to do IT-business B2C. On an international scale that will do Europe no good. On a mere European scale it is of course not only a negative development for companies but can – at the same time - also be a motivation to react to legal requirements better than competitors. In other words: a strict data protectional environment could eventually turn out to be a competitive edge within Europe, but still, on a global scale, and especially in comparison with much less regulated regions like Asia, Europe will stand no chance.

Let us now move on to one of the other relevant Directives regarding IT-privacy: The so called **Data Retention Directive** 2006/24/EC.

According to this Directive, providers have to store the telecommunications data of their customers for 6 to 24 months (the Member States are free to choose within this period of time). The provisions of the Directive authorize law enforcement authorities to request access to the stored data in order to detect severe crimes. In such cases law enforcement authorities are, for example, enabled to find out who the sender and recipient of an e-mail was, who was calling or texting whom at what time and, as far as mobile communication is concerned, where a mobile device is located at a given time. A request to get access to the data sets will be possible only in a necessary and proportional way.

[5] For example the tremendous amount of information the supplier has to deliver to the consumer in regard to online contracts or the consumer´s right to withdraw from online-contracts (both recently extended in favour of the consumer under the new **Directive on Consumer Rights**, 2011/83/EC).

This Directive is the most criticized of all European Directives. It is a reaction to the terrorist attacks in London and Madrid in 2005 and was therefore originally designed to prevent and solve terror related crimes (the ignition signal for the bomb in Madrid was transmitted by mobile communication). In the course of its draft this aim has changed to prevent and solve all sorts of severe crimes though, which would basically be OK. The main objective, however, is that the storage of the mentioned data has to take place on a general basis independent of any specific suspicion. In the end that means that all European citizens are permanently supervised. The much more adequate way in terms of human rights would have been a quick freeze procedure storing only data of individuals being at least suspected of committing or having committed a crime.

Quite on the contrary, what we now have is a clear breach of the **European Convention on Human Rights** which provides in Art 8 a right to respect for private and family life. § 1 states that "every one has the right to respect for his private and family life, his home and his correspondence". According to § 2 "there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

The emphasis of the exemption to the right of privacy according to the mentioned Art 8 lies on the word necessary. The interference with the right of privacy has to be necessary in order to be justified. That this is not the case with Data Retention can easily be proved by European statistics which have brought clear evidence that Data Retention has no influence whatsoever on crime detection rates.[6] From this point of view it can hardly be said that Data Retention is necessary. And it can of course be easily avoided by simply using prepaid anonymous devices or by surfing not from your office or at home but from an internet café. No trace will be left and so no Data Retention is possible. It can be expected that terrorists and criminals will bring up enough additional criminal energy to realize and consider that. So what we get in the end is not surveillance of those who should be observed but of those who should not. This can obviously not be necessary!

Another objective concerns the fact that the content of a specific communication (for example the content of telephone calls or e-mails) is exempt from supervision under the Directive. In many cases, it is easily possible, though, to still trace certain content information. If a person is frequently calling a certain lawyer, it is quite clear that this

[6]The statistics show the detection rate of various crimes, for example, bank robberies, computer crime, etc. The Max-Planck Institute determined that the accessibility to data storage, did not change the crime detection rates (for example computer crime statistics 2007: 50%; 2008: 40%; 2009: 42%). The Institute came to the same result in connection with child pornography crimes. July 2011; direct link: https://www.bmj.de/SharedDocs/Downloads/DE/pdfs/20120127_MPI_Gutachten_VDS_Langfassung.pdf?__blob=publicationFile.

person is a client. If a person keeps sending and receiving e-mails to and from a doctor specialized in HIV diseases it is very likely that such person suffers from HIV and so on. For these and many other reasons many Member States initially refused to transform the Data Retention Directive into national law.[7] In other Member States (such as Germany) the constitutional courts have suspended such transformation.[8] So the situation is quite complicated and unclear.[9]

Anyway, at this point you might ask yourself why Europe makes such a big fuss of the global NSA-surveillance of internet and telephone traffic when at the same time Europe is being supervised by providers according to the Data Retention Directive. Probably because there are a number of significant differences:

1. The European surveillance is a problem, but it is at least taking place on a regulated basis whereas NSA and other intelligence services act without public legal frameworks.
2. The NSA is obviously cooperating with national foreign services which is, at least according to most European national laws[10] not allowed for such national authorities as far as their own citizens are concerned.
3. The supervision on the basis of the Data Retention Directive does not include content of an e-mail or a telephone call. To supervise such content a judicial authorization is required in each and every specific case which is obviously not the case when the NSA is supervising.

So what the NSA is doing is a clear and severe breach of European Law. This has been considered by the mentioned draft of the new European Data Protection Act: Article 43a has been added. It deals with "transfers or disclosures not authorized by Union law" and states: "No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any manner, without prejudice to a mutual legal assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State" .

---

[7] So for example Austria (ECJ, C-189/09) and Sweden (ECJ, C185/09).
[8] Judgment 02.03.2010, 1 BvR 256/08 (German Constitutional Court); https://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html. ECJ, C-329/12, http://www.statewatch.org/news/2012/sep/eu-com-mandret-germany.pdf.
[9] Yearbook Human Rights 2011, 321 (*Dörnhöfer*).
[10] See, for example, article 319 of the Austrian Criminal Code: "*Who installs in domestic territory for a foreign power or an international institution or a military intelligence a military intelligence service or operates an intelligence service shall be punished with imprisonment up to two years"*; similar in Germany: Art 99 German Criminal Code.

This provision obviously does have the NSA in mind. The question is whether the NSA will care. We do not know and we probably will never know. But either way, it is not only legally but also from a socio-political point of view substantial to create clear data protection standards. Now, knowing what can be done and what is being done, even more than in Orwell's 1984 and more than a few years ago when I pointed that out in my book "On the way to a surveillance state"[11]. I then mentioned that one of the primal fears of mankind – being controlled by machines – has in a certain way come true. The internet, being an indefinite number of interacting machines, cannot be switched off any more. You can switch off or destroy some connections and machines, but still the information stored in and transported by the internet will find its way through the remaining channels – that is, by the way, what the internet was originally invented for: to enable communication without a central server which might be switched off or destroyed by enemy activities. This is becoming philosophical but it still shows the many aspects of the topic and why in such an environment of potentially being controlled and observed at least a clear legal framework is helpful. That such framework can be disobeyed – as it obviously is by the NSA at the moment – is another question. But that is the case in all matters of regulation not only in data protection. But even if not all regulations are obeyed, they still create an environment of awareness, which may keep authorities and intelligence services from pushing it too far (in this sense the US-American Secretary of State, John Kerry, just recently mentioned, that the American surveillance by the NSA "may have gone too far"[12] – the tapping of the German Chancellors cell phone[13] being the best example for this). So it remains to be seen how the NSA will react to the new European Data Protection Regulation.

Conclusion

The European legal framework regarding IT-privacy and data protection basically goes back to the Data Protection Directive of 1995 and the Data Retention Directive of 2006.

The latter is highly controversial (establishing surveillance independent of a specific suspicion) and should be withdrawn or at least be replaced by quick freeze procedures.

The Data Protection Directive is not up to date anymore as it has been drafted in a technical environment that has nothing in common with the modern IT-world. It will therefore be replaced by a new Data Protection Enactment that has recently been drafted

[11] Zankl (Hg), Auf dem Weg zum Überwachungsstaat (2009).
[12] The Hindu: http://www.thehindu.com/news/international/world/nsa-spying-may-have-gone-too-far-kerry/article5304234.ece.
[13] The Guardian: http://www.theguardian.com/world/2013/oct/26/nsa-surveillance-brazil-germany-un-resolution; http://www.spiegel.de/international/world/merkel-calls-obama-over-suspicions-us-tapped-her-mobile-phone-a-929642.html.

and will – from a supplier´s point of view – bring along a severe intensification of data protection requirements. It also contains a new article directly reacting to the NSA´s activities which are, already under existing European law, a violation of data protection principles.