vienna | brussels | berlin | hong kong | london | new york
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

International Data Privacy Rules

Presented by Wolfgang Zankl at Harvard University, Berkman Center for Internet & Society, 28.10.2014

I appreciate being here and would like to especially thank Prof. Urs Gasser for arranging this meeting and giving me the opportunity to share some thoughts about Data Privacy with you.

Before we get into that let me just briefly introduce myself. I am a former Dean of the law school at the Private University of Liechtenstein and I am currently and since 1997 a professor for Private and Comparative Law at the University of Vienna, which is one of the oldest (1365) and with 13.000 students the largest German speaking law faculty. In 2001 I founded the e-center, the european center for e-commerce and internet law; it was, by the way, September 11, 2001 and it was 3pm European time (which is 9 am your time) when our kick-off meeting started in Vienna. As we all know, at that very time the tragic and horrific attacks of 9/11 unfolded. The e-center being established on exactly that day was pure coincidence, of course, but it had tremendous significance for our activities in the years to follow, because many regulations regarding data issues have been and still are driven by this event. Anyway, in the meantime the e-center has come quite a long way and evolved into a large international IT-law network. We now operate in Berlin, Brussels, London, Hong Kong, New York and Vienna and we cooperate with a number of business partners like Microsoft and other big players. Furthermore, we are supported by an advisory board of almost 100 members all over the world.

Now, this international focus of our activities has led us to the question - and this gradually takes us to the topic of my introduction - why Europe has such a problem with so many American IT-companies. An initiative called Europe vs Facebook complaining about data privacy breaches has been launched recently for example. Or the German

graben 17|10
1010 wien
fn 171119x, hg wien
tel: +43 1 5354660
fax: +43 1 5338966
www.e-center.eu
office@e-center.eu

Government wanting to restrict Google in many ways, recently for example by asking Google to become more transparent by disclosing exactly how it ranks search results. So there is a great deal of both mistrust and misapprehension between Europe and US-companies as far as data transparency and data privacy is concerned. That and especially how we might manage to find common ground in the end, is basically what I would like to discuss with you.

Before doing so we should, in order to fully understand the problem, first have a look at a few facts of European IT-law in general and it´s Data Privacy approach in particular.

To begin with Europe has a problem of it´s own because many European countries still have very old laws (in Germany for example the Civil Code is almost 120 years old, in Austria the Civil Code even goes back to the 18th century). It is clear that such traditional legal frameworks are not prepared to deal with modern technologies. And this problem, European law being out-dated, not only applies to specific national regulations but also and especially to European-wide Data Privacy Directives. The basic concept of European Data Protection Regulation goes back to the Data Protection Directive of 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 world we live in today: Many technologies, devices or services we use today as a matter of fact, such as Google, Amazon and Social Media, like Facebook or Twitter, 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 Rules. This has been accomplished in the past two years and lead to a draft of a new Data Protection Act which has been amended a year ago, in October 2013. I and many others believe that this new Data Protection Framework is still old school, still based upon the approach of 1995 with only scattered real innovations. One of these novelties has been the so called right to be forgotten. The European Court of Justice has just recently accepted this right, too, and held Google responsible to delete links to online articles containing outdated facts about individuals. I personally rather doubt this decision for several reasons, but let´s leave that for our discussion. What I should mention though, is that the right to be forgotten has in the meantime been removed from the European draft (and then been added again) and it has also been rejected by German and Dutch High Courts. So what that reveals is a certain inconsistency of European Law and Law making.

The same applies to the so called Data Retention Directive of 2006. According to this Directive, internet and telephone service providers have to store the telecommunications

data of their customers for a certain period of time. The provisions of the Directive allow law enforcement authorities to request access to the stored data in order to detect severe crimes. In such cases authorities are, for example, enabled to find out who the sender and recipient of an email was, who was calling or texting whom at what time and, as far as mobile communication is concerned, where a mobile device was located at a given time. Sounds reasonable, but in fact this Directive is the most criticized of all European Directives. It was a reaction to the terrorist attacks in London and Madrid in 2005 and 2006 and was therefore originally designed to prevent and solve terror related crimes. 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 as long as surveillance would really be able to prevent and solve such crimes and therefore be justified. That this is not the case with Data Retention can easily be proved by German statistics which have produced clear evidence that Data Retention has no influence whatsoever on crime detection rates. From this point of view it can hardly be said that Data Retention is justified. And it can of course be easily avoided by simply surfing not from your office or at home but from a public internet access. No trace will be left and so no Data Retention is possible. It can be expected that terrorists and criminals are aware of that, too. 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 justified. For this and various other reasons the European Court of Justice has recently declared the Directive void. But what is the reaction of national European governments? They want to start the whole thing all over again by simply applying the former Directives Rules to offences more severe than before. Again this is inconsistent, because this approach completely ignores the main objective, that data collection is taking place on a general basis independent of any specific suspicion. In the end that means that European governments want to carry on with supervising European citizens ignoring not only the European Court of Justice but at the same time making a huge fuss of the NSA surveillance (it couldn´t get any more inconsistent than that). So, summarizing what we have seen so far, is that European IT law is too out-dated and too inconsistent in order to successfully harmonize with other frameworks or approaches like the American.

But there is one more point, which is a consequence of these two peculiarities and which I consider even more important when it comes to explaining why European Data Privacy Law is not really working in a globalized environment which American IT-companies represent: it is the fact that common European Data Privacy regulation neglects the fact that personal data are nowadays, in a social media society, usually given away voluntarily and upon contractual agreement (we could refer to such data as new data). When using

Google, Amazon, Facebook and others we all agree with these companies´ terms and conditions. So Data Privacy should not only consider mere Data Protection but also contractual principles. And one of the oldest and most fundamental contractual principles is "do ut des" which is Latin and goes back to ancient Roman Law meaning that there is or should be a certain balance between what you give and what you get in return. That would explain why companies like Google or Facebook for whose services the customer does not pay should basically have the right to use his personal data (that would be the balance: data for service). But this is only a first approach. Applied to modern data environment the balance has also to be struck in relation to other relevant parameters when it comes to contractual aspects of data privacy:

- since data is a contract matter we have to consider what kind of personal data we are dealing with (especially sensitive and non-sensitive data has to be distinguished and treated differently)
- and since contracts are concluded by mutual consent the extent of such consent also has to be taken into account (has it to be declared explicitly or is accepting terms of use sufficient)

So what I am suggesting is that these three parameters should be balanced. I tried to do so by putting them into a set of privacy rules considering American standards (like the FIP – Fair Information Practices), European standards (Directives and recent draft of Data Protection Act) and International Standards (like OECD Privacy Principles).

So let me come to the final point of my introduction and present you my proposal for six international data privacy rules for commercial applications:

Companies in compliance with international data privacy standards commit to

(1) complying with national data protection or privacy law, national contract law and other legal requirements or regulations referring to data privacy

(2) complying with current security standards to protect stored personal data from illegitimate access

(3) implementing an easily perceptible, accessible and comprehensible privacy policy with information on why and which personal data is collected, how this data is used, who will receive this data, how long this data is stored, whether and which data will be deleted upon request

(4) not using or divulging any customer data (except for statistical analysis and when the customer's identity remains anonymous) unless the company is obliged to do so by law or the customer agrees to such use or circulation

(5) in case of a contract between the company and the costumer committing the costumer to pay for services or goods:

- informing the costumer individually and as soon as reasonably possible in case of data breaches with regard to personal data

- informing the customer upon request about which specific data of this costumer is stored and deleting such data upon request unless applicable laws or regulations require the company to continue storing such data

- not using or divulging content-related personal data

- not using or divulging any other personal data without the costumer´s explicit, separate and individual consent

(6) in the absence of a contract between the company and the costumer committing the costumer to pay for services or goods:

- informing the costumer as soon as reasonably possible in case of data breaches with regard to sensitive data (referring to, e.g., sexual, financial, medical, political or ethnic issues)

- informing the customer upon request what type of sensitive data of this costumer is stored and deleting such data upon request when such data is outdated unless applicable laws or regulations require the company to continue storing such data

- not using or divulging sensitive data without the costumer´s explicit, separate and individual consent