verbraucherzentrale Bundesverband

30.12.2009

Answers to the Consultation on the EU General Data Protection Framework

Verbraucherzentrale Bundesverband
German Federation of Consumer Organisations

New challenges, current legal framework and future action to address identified challenges

Verbraucherzentrale Bundesverband e.V. – vzbv
Fachbereich Wirtschaft
Markgrafenstr. 66

22.12.2009

10969 Berlin
wirtschaft@vzbv.de
www.vzbv.de

Effective Consumer Data Protection for the Second Decade of the 21st Century

The German Federation of Consumer Organisations is glad to provide answers to the questions of the European Commission:

1. Please give us your views on the new challenges for personal data protection, in particular in the light of new technologies and globalization
2. In your views, the current legal framework meets these challenges?
3. What future action would be needed to address the identified challenges?

Summary:

Personal data has gained a level of economic importance which is not properly accounted for in the existing legal framework and the actual implementations by member states.

The General Data Protection Framework is a successful, well-proven framework, but needs to be further improved since it does not provide sufficient protection mechanisms for consumers data. Personal Data and Personally Identifiable Information both are challenged by the digitization processes which we do not refer to in the meaning of occuring on the Internet only.

Globalization is therefore not to be seen as a challenge to privacy, it's merely a chance to promote European privacy standards.

Existing legal and enforcement loop holes have to be closed before the predictable upcoming technological progress leads to a factual privacy wipeout.

The vzbv asks the EU commission to:

1. **Require member states to ensure that data protection authorities act independently and effectively on behalf of the consumers interest. This includes the right to take over control in case of misbehaviour. It also means implementing efficient data protection as a crucial duty. Data protection, whenever business is affected, also means consumer protection.**

2. **The undoubted usefulness of personal data in many ways – such as energy saving by using smart meter techniques – has to be shaped in a bullet proof way. Without consumers prior explicit informed consent, no combination of different data sets shall be allowed.**

In detail:

1. Views on challenges for personal data protection

The application of network technology has become one of the main keys to productivity gains in the field of economic progress. Innovation in smart grids as well as all kind of advertising is mainly driven by apparently boundless possibilities of available enhanced data processing technologies.

Whether in the field of smart metering the consumer households power consumption , in the field of behavioral advertising on the internet and forthcoming on the mobile, in the field of location based behavioral services[1] but also in nowadays neolithic appearing direct mailing, consumers are not aware of what kind of data are processed, the purpose of processing and under which circumstances they are allowed to take action against collection and processing.

Most of these new techniques are subtle and promise benefits without asking the consumer for explicit and informed consent, but throwing them off. These techniques usually show their power only when the data is being mashed up with data from other sources.

Inventing services for the information society does obviously happen on calculating a formula of first to raise attention and reach the critical mass of users and only afterwards to comply with laws protecting consumers and their right to privacy.[2]

Since most data transmission will happen via some kind of online technologies in the near future, we appreciate that EC95/46 Directive does not distinct between different ways of collecting, but by the way of storing data.

When the directive was established, there were two ways of storing data: analogue or digital. Today we may distinct a third category which is obviously a threat to consumers privacy: cloud computing is going to change the infrastructure of real world hosting facilities and by that also the place where personal data is stored. This causes a bunch of questions to the directives scope.

We urge the commission to find out whether the provisions of Art. 25 and 26 of the directive are sufficient answers to the legal challenges caused by data centers providing Infrastructure-, Software- and Platform-as-a-Service solutions around the globe. It is quite reasonable that a large share of personal data related processes has to be expected to move into cloud computing based environments within the next years, legal answers have to be found .

[1] Services such as provided by Sense Networks, http://www.sensenetworks.com/, Navteq Media, http://www.navteqmedia.com/solutions/advertising-agencies/, and others.

[2] Verbraucherzentrale Bundesverband had to send cease-and-desist letters based on laws against unfair contracts to five social network providers in July 2009, incl. US based MySpace and Facebook, due to unfair terms of services and privacy policies. Facebook and StudiVZ previously signed the “Safer Social Networking Principles” of DG InfSo earlier in 2009 but did not comply to consumer laws.

a) 'Behavioral' shall be taken into account as a diminutive of Surveillance

On a even more personal level, consumers are threatened by overwhelming interest in their behaviors, which are expected to give better insight in their real demands than surveys do. Right now we have identified two main areas where behavioural data is used or proposed to be used.

The first one is the area of behavioral or tailored advertising: without notice and prior consent of the consumers, their online behaviour is tracked by companies usually working to improve targeting quality for advertisement companies. But data belongs to the customer, not to the companies. Customers may allow companies to make use of their data, but without prior comprehensive informed consent no data possibly identifiable to an individual shall be processed. Regarding the key issues we have with behavioral targeting, we may refer to BEUCs answer.

vzbv is aware that the systems used for behavioral targeting may vary, but what does not vary is the missing consent and lack of information of consumers – whether web bug and cookie, location or deep packet inspection based. Many techniques in marketing terms called behavioral, in our view should more honestly be called surveillance mechanisms. Data mining of users behaviors is also expected to be implemented in new digital tv devices and technically already implemented in mobile phones.

One of the already established systems of behavioral based data mining is the so called scoring, where credit checks of customers is said to be estimated on their behavior. In fact, a study conducted by the German Ministry for Consumer Protection revealed that a high percentage of the data sets is flawed and misleading[3]. These flawed data in combination with the lack of knowledge on the applied methods of calculating score values leads to intransparent and misleading prices. In our opinion a price which only applies to consumers with a score value out of reach for most human beings may not be considered as a price information but as misleading in terms of the unfair contract terms directive. Data becomes an increasingly important role here: obviously behavioral techniques are in some cases misleading the business and detrementing the consumer.

In most cases, consumers are neither informed nor do they even suspect that companies are using scoring mechanisms to estimate their personal creditworthiness. This also means they are not aware of their rights to have wrong data corrected and often also deleted. It is unclear who is to be taken into account for damages caused by use and distribution of flawed data sets.

The second area is the smart metering of power consumption in consumer households, as promoted by European Commission[4]. Smart metering of power consumption is one of the first infrastructural areas, where the concept of smart grids becomes consumer reality. In our opinion, smart metering has to be implemented fast but with a proper concept of privacy by design.

The legislation has to be double checked whether consumers are still in control of their privacy, when – even for good purposes such as carbon reduction – they are

[3] http://www.bmelv.de/cln_173/SharedDocs/Pressemitteilungen/2009/178-Verbraucherinformation-Scoring.html

[4] 93/76/EEC, 2006/32/EC, 2004/22/EC

systematically under pressure to give up their right to privacy or simply have to pay more.

Privacy may not be understood as a means of payment, a commodity, since consumers own it just once and are unable to regain it within a reasonable period of time, if once lost.

b) Complexity of Privacy

We have found that many providers of businesses based on or making extensive use of personal data try to keep their users lulled in the feeling of private areas. For example data driven businesses such as social networks still do not put their responsibility for users privacy in the first line, but their pure economic interest of binding users to their platforms and make them most accurately available targets for advertising.

The German Federal Constitutional Court in a ruling as early as 1983 stated that the 'fundamental right to informational self-determination' goes beyond the protection of privacy in a narrow sense: it confers on the individual, in principle, the power to determine for himself or herself the disclosure and use of his or her personal data. It is explained in the ruling with the assumption, that being unable to know the knowledge of the opponent may cause being inhibited in the ability to decide and plan independently.

This principle should also be kept in mind while evaluating the data protection framework. It does not only apply to the relationship of citizens and states, but also to the relationship of consumers and the economy. Consumers being unable to assess the knowledge their economic counterpart has are without any doubt systematically disadvantaged. To prevent consumer detriment, the core principle of prior and explicit consent, the right to proper and consumer understandable information must be one of the leading ideas.

2. Current Legal Framework

a) Technology neutral

The technology neutral principles have proved to be the right approach to protection of consumer data in the General Data Protection Framework. It obviously is the only way to keep up with the speed of innovation in one of the most dynamic, fast changing environments we know. The concept of common technology neutral principles is much appreciated by countries around the world, being a model for other countries – especially those, who want to have their legislation to comply with European standards.

b) Lack of enforcement

2009 was a bad year for data protection in Germany, as it turned out that many companies are still avoiding proper data protection while obviously considering it not to be cost efficient.

A bank giving unallowed access to their customers account movements for sales reasons (Postbank), online shops being certified for safe online shopping having a publicly available invoice system including all customers financial data (Libri), a social network service for pupils not fixing a well-known bug allowing privacy invasion to data not set to be public and several million users data being crawled (SchülerVZ), call center employees selling customer bank account data in millions and the national legislation acting just half-hearted on these occurences.

The data protection authorities are not equipped adequately, they especially lack manpower and the possibility of enforcement, even though the German implementation of the data protection directive is exceeding the European standard by far.

On behalf of the provisions of Articles 6 and 7 of 95/46/EC we strongly doubt they are as respected and enforced as they should be. Our experiences with companies are often not pursuant to these articles, which might be caused by the lack of enforcement. We consider that often personal data is collected for purposes not covered by the consent of the consumer. In our opinion it must be clarified that large scale or deliberate violation of national implementations of the data protection framework directive is not a minor but a major offence.

3. Future Action

a) General remarks

We believe that the use of personal data is both, a potential risk and a potential chance to both, consumers and economy. But for the moment, economy is highly advantaged by the factual developments, since data breaches and violations of the general principles of data protection are merely dealt with as minor offences.

Dispossessing someone of his privacy by revealing it to a third party, passing it out of control for the individual is not a minor offence, regardless whether caused by sloppiness or deliberately. The cost effectiveness of saving expenses on privacy issues must be challenged.

We also believe that consumers have the right to decide on their own whom to expose their behaviors to and under which circumstances. Surveillance without consent for economic reasons shall not be seen as an appropriate interest conflicting with consumers right to keep control of his/her personal data and personal identifiable information.

Proper information of consumers means consumer understandable information. Not having to study law when deciding on whether to give consent to data collection and processing or not should be a general principle, which to us seems only be properly implementable by having clear rules of the reach caused by an opt-in. Personal data shall not be allowed to roam freely without rerequesting consent of the consumer, information and communication technology might be a key to implementation of this principle.

b) Further steps

vzbv welcomes the idea of implementing a general data breach notification. Since a first adoption of this idea was implemented in German data protection law (BDSG) in 2009, we do recommend discussing the question of an individual notification duty. The German legislator also offered the alternative publication of two advertisements of at least half a page in two nation wide newspapers or adequate public information, which we do not consider to be a sufficient reaction to data breaches.

Given the importance of having international binding rules on collecting and processing personal and personally identifiable data, we expect as a further step to evaluate the Safe Harbor framework, which is not sufficiently guaranteeing European data protection standards in our opinion. Especially when it comes to infringements, consumers are lacking the possibility of enforcing their rights. Data protection means in the end better consumer protection, but consumer organisations and consumer protection authorities are often not entitled to take companies into account for misbehaviour. Data breaches in the view of an individual consumer often harm in a hard to amount minor way, compared to the expectable discomfort of taking a company to the courts for compensation, which is hard to prove for an individual anyway. Collective redress in case of data breaches shall be discussed as a serious option to help European citizens making use of their rights in the future.