

# The Principles of the European Privacy Association

Our Priorities & Our Objectives for the Future of Privacy

September 2009



European Privacy Association (ABSL)  
Square de Meeus, 37 - 4th Floor  
1000 Brussels, Belgium

T: +32 2 791 75 18

F: +32 2 791 79 00

E: [info@europeanprivacy.eu](mailto:info@europeanprivacy.eu)

W: [www.europeanprivacy.eu](http://www.europeanprivacy.eu)

## **INTRODUCTION**

The European Privacy Association (EPA) was founded to confront some of the most fundamental challenges of the next few decades for the so-called Information Society, namely data protection and security, in light of European experience and values. If Europe is able to cultivate the opportunity for development offered by innovation and by new web applications, while at the same time protecting the privacy, freedom and security of its own citizen consumers, it will create trust and confidence that will permit the market to grow rapidly and harmoniously. Furthermore, Europe will be in a position to offer best practice solutions to the rest of the world.

Among fundamental rights, the “right to privacy” has been known for centuries but has assumed a new and crucial significance in the internet era, in view of the fact that it is increasingly endangered by the progress of technologies and by increasing governmental encroachment. At EPA we believe in an open society, able to protect this right and defend it from the various threats it faces. However, we also believe that privacy must be interpreted in light of other important rights, duties, and freedoms.

Our guiding principles are as follows.

## **PRIVACY AS AN ASSET**

Companies too often regard data protection as an administrative burden and an imposition on its commercial ambitions. Today, fortunately, things are changing, and many operators are beginning to understand that privacy can be an extraordinary asset: an instrument for improving the competitiveness of their companies, transforming them into allies of citizens, who are also often their customers.

The protection of personal data favours a strong propensity towards innovation and

consequently the circulation of new products and services, heedful of the “human dimension” and, precisely because of this, more useful to and better appreciated by consumers. According to this approach, which we favour and define as “proactive”, the market becomes a place where individuals, governments and firms share a common advantage (win-win scenario). Privacy by design and Privacy Enhancing Technologies are concept we favour and promote at EPA.

## **PRIVACY AND CYBERSECURITY**

With the advent of “cloud computing”, i.e. the progressive transformation of individual users’ computing devices into instruments which draw on applications and archives from vast data centres with servers located around the world, the technical protection of personal data, security of storage, and defence from attacks takes on an absolute importance.

Constantly growing investments will have to be made to guarantee the construction and updating of cybersecurity systems. On a strictly legal level, information concerning attacks, or the theft or loss of personal data, will have to immediately be communicated by internet service providers and, eventually, also by content providers, to the affected users, in accordance with the new rules which have been strongly endorsed by EPA and are currently in the phase of approval with the EU Telecoms Package and review of the E-Privacy Directive 2002/58.

For too long in Europe, cybersecurity has been seen as mainly a subject of national interest, whereas it requires a pan-EU or even a global approach. The EU should thus appoint an authority or a Commissioner for the control and direction of cybersecurity policies across the Communities, with the ability to supervise the protection of community information systems and those of Member States. A nation’s networks and

servers constitute critical infrastructure, and it is not impossible to foresee that future wars or terrorist operations could be fought by means of cyberattacks. The blackout of the information systems of a nation could create chaos by preventing the normal operations of transport, hospitals, and telecommunications, causing the loss or theft of citizens' sensitive personal data. .

We therefore call upon the EU to encourage national governments in their efforts of improving national, European and international coordination of cybersecurity issues. Each Member State should develop specific strategy and organisational structures to address cybersecurity needs, and these efforts should be coordinated at the EU level. It is also important to work with the private sector to promote a coordinated approach.

## **PROFILING ON INTERNET AND TELECOMMUNICATIONS NETWORKS**

There is an increase in the profiling of personal data in both the private and public sectors. Controls must be adopted on the automated monitoring or filtering of users' traffic data and contents of users' communications and browsing without prior informed consent. To date, almost all the European legislator's attention in this area has been directed towards ISPs, but risks are also presented by profiling activities in other business sectors as well. Furthermore, an increasing number of public sector projects in the EU result in an unacceptable level of profiling activities. Clear prohibitions and sanctions are needed to prevent the illicit profiling of users. A related issue is that users are often in an unequal bargaining position with operators who offer them the use of services on the Internet in exchange for their personal data; this problem is particularly acute, for example, with regard to excessively long retention periods for personal data, and with regard to the processing of so-called "sensitive data". Consumer protection must apply to the processing of personal data on the Internet as it does in other areas.

## **PROMOTING “PRIVACY BY DESIGN”**

People’s personal data and confidentiality cannot be protected only through legal rules, best practices and sanctions. There is a need for the promotion of the production of privacy-friendly and privacy-enhancing technologies which limit the processing of personal data to what is necessary, and which ensure - through technical design - compliance with privacy requirements. To do this, the producers of information and operating systems, including both hardware and software, should consider users’ privacy already at the planning and design phase. This applies not only to Internet technologies, but also to everyday things such as electrical appliances, the use of RFID labels, or “intelligent” cars. On this point, the recent European Commission recommendation about RFID, which refers explicitly to the need for RFID system designers to make a “privacy assessment”, might be considered as a good point of departure to be extended to other technologies and information systems.

## **PROMOTING THE ADOPTION OF PROFESSIONAL CODES AND “BINDING CORPORATE RULES”**

Data protection is a global topic, rather than one of national or even regional importance, and individual States have progressively less influence over the development of legislation while having to take into account (international) principles and best practices. Two European models can be of help to involve the private sector in the development of a sustainable privacy-system at the global level. In the first instance the so-called “codes of practice” as set out in Art. 27 of the EU Data Protection Directive 95/46/EC should be further developed and promoted to advance data protection specific sectors. These codes are an efficient method of furthering data protection because they involve “stakeholders” and favours privacy regulation which takes into account the specific requirements of particular sector.

The second example is so-called “binding corporate rules” (BCRs), which are the internal policies, developed by multinational companies in line with EU standards and are approved by national data protection authorities (DPAs). Such BCRs result in the exportation of rights to countries with differing or non-existent privacy standards, and can be a useful and efficient method to ensure privacy compliance throughout all the subsidiaries of large corporations

Both these models need to be fostered and promoted more forcefully. In this regard, it is essential that the European Commission develop pan-European approval systems for both codes of practice and BCRs that are more efficient than those that now exist.

## **THE ADOPTION OF AN INTERNET BILL OF RIGHTS AND OF A MORE GLOBAL APPROACH TO PRIVACY PROTECTION**

We share and appreciate the efforts of those who are working towards the approval of an Internet Bill of Rights. It is, in accordance with the WSIS Tunis Agenda, our endeavour that privacy principles should be protected globally, and this Bill of Rights should be endorsed by the majority of the Nations in the world. As privacy is a topic of global importance, States and regions should work together to improve harmonization of differing privacy standards, with a final goal of developing international standards to protect the privacy of all citizens of the world (though this is a long-term goal that will take time to achieve).

## **FOR MORE USER-FRIENDLY METHODS OF PRIVACY CONFLICT RESOLUTION**

These developments must be accompanied by users’ efficient and accessible means of protection: it is unthinkable that the seat where the right to privacy can be enforced should be distant from the interested person or require excessive effort for him to assert

his right to the protection of data. Once the instruments for disciplining even extreme scenarios such as cloud computing have been found, the Courts must develop a jurisprudential culture which is able to weigh more and more, both in decisions and their application, on company regulations, “third generation” deontological codes and the charters of international principles, without running aground in the close network of ordinary national regulations. There must be growing incentives for systems of alternative conflict resolution either contained in company regulations or generally recognized for users, following systems already in force for consumers, through access to simple, rapid and low-cost procedures not only in the ambit of commercial negotiations but also in that of privacy.

Thanks to the fruitful combination of the bill of rights, best practices of participation of market operators and “user-based” instruments which however have global impact on the defence of citizens, a new and non-bureaucratic system for applying the protection of personal data in the internet era can emerge. Finally we must remember the huge and highly-meritorious multi-lateral efforts of several subjects and organizations to, *inter alia*:

- a) amending the Brussels Regulation on recognizing and enforcing foreign judgments;
- b) enhancing international arbitration procedures and access;
- c) better implementing the Hague Conventions on Choice of Courts and Evidence Gathering.

The whole relevant body of private international law is going through crucial evolution and it is possible to constructively contribute to the on-going debate and efforts to enhance the existing tools and identify new and more user-friendly and adequate ones as they relate to privacy protection.

## **SIMPLIFYING PRIVACY BUREAUCRACY**

There are still too many bureaucratic traps in the ambit of privacy in Europe. With the intention of ensuring perfect protection for citizens, some Member States have interpreted the rules indicated by the Directives in an excessively restrictive manner and the results are evident: excellent abstract regulations are established, but their application encounters difficulties which render them useless and at times damaging. Many of these regulations have more to do with bureaucracy than with privacy protection, and can result in operators being suffocated under mountains of complex obligations (an example are the differing systems for notification of data processing to the DPAs in the EU Member States; it would be more efficient, and more protective of privacy, to have a single EU-wide notification system). Among our objectives there is therefore that of making privacy regulation both more efficient and more effective.

## **STATE INTRUSION IN CITIZENS' PRIVACY**

Safety is a right which ought to be and is protected by the state. But as with every other right, public security and the fight against crime cannot be seen in opposition to other fundamental rights such as privacy. We are concerned about the tendency of governments to seek to monitor European citizens' every movement (online and offline) for the purpose of the prevention of crime and other kinds of offences, which presents a real risk of intrusion in people's private spheres. It is one thing to intercept a communication or a flow of data in the presence of concrete evidence of guilt in order to look for evidence, and another to use a priori filters, records, video-surveillance, or interceptions as means to conduct "fishing expeditions". One cannot, for security reasons, monitor or profile millions of innocent citizens, hoping – sooner or later – to find a few guilty ones. This presents the risk of a "Big Brother" state, with two further concrete dangers: first, that

the sensitive data collected in this way by governments may be ceded to other States outside the EU (this is the case of the PNR agreements between EU and US), making the protection of citizens difficult and remote; second, that governments also burden private operators with the task of monitoring citizens for reasons of security and public order.

EPA is against automatic systems of control and profiling of individuals against or in spite of their will, whether by private or public operators. In order to combat this risk, there should also be provision at the EU and Member State levels for the adoption of “privacy impact assessments”, in order to evaluate - before approval - whether every new national regulation is compatible data protection and privacy law. This would prevent laws from coming into force which are manifestly damaging to the citizens’ right to privacy.

## **PRIVACY AND INTELLECTUAL PROPERTY**

Closely linked to the problem of the invasion of the “public eye” is the theme of the protection of intellectual property. While EPA is against the application of generalised network filters or monitoring, we are also aware that intellectual property must be protected, because an informative society which does not attach importance to intellectual goods and investments in creativity is unthinkable. Governments should thus protect privacy, while allowing for the development of non-invasive methods of intellectual protection, as foreseen in a recent judgement of the European Court of Justice.

## **PRIVACY AND PUBLIC ADMINISTRATION**

New technologies have improved public administrations, making them more efficient and bringing them closer to citizens. However, all public offices must give top priority to citizens' privacy. We are against actions which, in the name of hypothetical transparency, distribute the personal data of citizens without any need or justification, as has already occurred in the EU (for example the data concerning taxpayers' income). Every project carried out by public administration, as well as every measure it applies, must be preceded by a privacy impact assessment (PIA), so that personal data may be protected and treated proportionally, without exceeding the purposes for which it has been gathered. These principles take on even greater value regarding platforms of e-health or projects of electronic welfare files that are presently being developed in every European country. Finally, any outsourcing of data processing to private operators must provide protections to avoid citizens' data being transferred to operators who do not entirely comply with European privacy regulations. Just as public administration financial accounts are controlled, so must a periodic audit of the level of protection of personal data be conducted for public authorities, with the possibility of inflicting sanctions being imposed to enforce such rules