Presentation to the LIBE Committee of the European Parliament. How to strengthen the EU legislation, improve international cooperation and secure the growing market of internet services

ENISA - Alain Esterle, Barbara Daskala, Giles Hogben

The European Network and Information Security Agency (ENISA) was created in 2004 to provide an independent and transparent view on security issues concerning networks and information, including privacy. Acting on the request of national and European representatives, ENISA has, inter alia, supported the EDPS in setting up an audit programme and conducted a feasibility study on a partnership to collect incident data (notably privacy breaches). ENISA recently issued position statements on security issues and recommendations for online social networks, as well as a security analysis of online reputation systems [1]. Currently, ENISA is gathering expert opinion through its Working Group on Privacy and Technology.

We take the principles of the 95/46 and 2002/58 Directives on the Protection of Personal Data and its interpretation through the Article 29 Working Party (e.g. 2) as a basis for the discussion of EU legislation in this area. We note the November 13 proposal to amend the 2002/58 directive [3], including inter alia by strengthening powers given to NRA's and the mandatory reporting of security breaches. We also acknowledge the difficulty of strengthening cooperation with countries having privacy principles quite different from those of Europe.

Current developments in the area of search, behavioural marketing and, as outlined in our recent position statement, in social networking pose a serious challenge to the European Union's ability to uphold the principles of transparency, informed consent, purpose limitation and the right to rectification as established in the 95/46 directive. For instance:

- Social discrimination on the basis of specific attributes of a person often falls outside the bounds of data protection legislation simply because the data collected may not be classed as personal data. As a prominent example of this, behavioural marketing privacy policies often claim not to be transmitting personal data to third parties, because names or contact details are not transmitted. However we note that such a claim is extremely questionable with respect to the definition of personal data outlined by the Article 29 Working Party in [2], whereby an IP address may be considered personal data. Data on hobbies, friendships and search terms etc… may be extremely personalised and may serve to identify an individual just as much as their name, address and birth date. Furthermore their knowledge by a third

party may result in negative consequences on their personal or economic life and/or discriminatory exclusion from services.
- While the principles of the 95/46 directive apply to legal entities, they do not apply in the more symmetric data collection scenarios created by Web 2.0. (i.e. individuals communicating directly with each other). For example, individuals or peers collecting data about each other may abuse that data in any way without being subject to sanctions. The same change in communication patterns leads to grey areas of responsibility for example for security flaws in user-generated scripts and code common in Web 2.0 applications.
- Business models relying on viral marketing are extremely common in Web 2.0 scenarios. Current sanctions against abuse of data may be ineffective when set against huge financial incentives offered for fast-spreading, "promiscuous" and data-hungry Web 2.0 applications.
- The principle of the right to access and rectification expounded by the 95/46 directive is often not upheld when it comes to user-generated content. It is very rare for example to be able to remove or alter comments linked to a social network profile or other personal data, when they are made on another person's profile.

Despite these threats, ENISA hopes and believes that the core principles of the 95/46 directive can be upheld. In order to bring this about, ENISA recommends several lines of action:
- Automated audit tools and stronger audit regimes for high volume data consumers (surveilling the surveilors). In particular standardised logging schemes with built-in non-repudiatability mechanisms should be encouraged in order to improve the scalability and easy-of-use of audit regimes.
- Standardised, portable formats for personal data and especially for privacy preferences. Formats such as portable social-networks discourage locking in consumers, encourage competition based on good data-handling practices and most importantly allow users to set sensible privacy preferences because they have to invest less time in setting them up.
- Awareness-raising campaigns among end-users to stimulate more cautious behaviour with respect to disclosure. Information should also be transmitted in the context of applications themselves (e.g. in mouse-overs, educational videos etc…).
- Research and development into reputation-based services to stimulate more positive behaviours. Reputation schemes based on a web-of-trust aggregate multiple sources of trust and often provide a more dynamic and ultimately more trustworthy system. Services such as unsubscribe-reputation and mutual evaluation of peers in social networks are particularly important. We refer to the recommendations of [1].
- Security-conscious design-principles and "privacy-by-design" should be promoted among application developers. For example, confidentiality (e.g. through encryption) in the collection of personal data should be promoted so as to avoid leaking personal records.

- Legislative review and interpretation to clarify some of the grey-areas outlined above, such as the responsibility of data controllers who are not legal persons. For example, should limits be set on the collection of personal data by natural persons, over which they become subject to the provisions of data protection legislation? (Registration with relevant authorities, obligation to provide subject access, breach reporting etc…)?
- Clarification should also be given in respect to the legality of data collection in behavioural marketing.
- Certification schemes can be a strong incentive towards better data handling practices by service providers. Initiatives in certification concentrating specifically on data protection are still in their infancy, requiring considerable research and development. As a useful model, we would propose the Swiss federal data protection act, which sets out voluntary certification requirements and motivates businesses to comply by providing exemption from expensive reporting requirements.
- Certification schemes may also be combined with standardisation work to define best practices. Such best-practices might also be considered as input to liability rules on service providers to ensure that security and operational measures that point to the protection of personal data are duly implemented.

ENISA provides independent advice on policy and technical issues in Network and Information Security (NIS). This paper is part of ENISA's work on identifying emerging risks and promoting best-practice in NIS.

---

[1] http://www.enisa.europa.eu/pages/position_papers.htm
[2] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf
[3] http://ec.europa.eu/information_society/policy/ecomm/library/proposals/index_en.htm