The New PII: Privacy-Impacting Information

27 February 2013

Panellists

- Michael Donohue, Senior Policy Analyst, Organisation for Economic Co-operation and Development (OECD)
- Marian Gordon, Director, International Telecommunications and Information Standards, Office of International Communications and Information Policy, Bureau of Economic and Business Affairs, Department of State, USA
- Maria Michaelidou, Programme Advisor, Data Protection Unit, DGI – Human Rights and Rule of Law, Council of Europe
- Wendy Seltzer, Policy Counsel, World Wide Web Consortium (W3C)
- Matthew Shears, Center for Democracy and Technology (CDT)
- Bill Smith, Technology Evangelist, PayPal

Due to unforeseen circumstances, Kimon Zorbas, Vice-President, Interactive Advertising Bureau (IAB) Europe was not able to participate in the session.

Moderator: Christine Runnegar, Senior Policy Advisor, Internet Society

Remote Moderator: Luca Belli, Doctorant en Droit Public CERSA, Université Panthéon-Assas, Sorbonne University

Summary of presentation and/or debate:

Please note: this was an information and perspective sharing exercise. The points set out below are a summary of some of the views expressed by the participants on key issues.

The Internet Society introduced the session with some preliminary results from a micro survey the organisation conducted regarding the scope of the data protection. A full report will be available shortly.

Some observations on the scope of personal data:

- There is no bright line between personal data and anonymised data – the idea that data is privacy binary (i.e. personal data or not) is becoming less relevant, and even problematic.
- The OECD *Privacy Guidelines* state that they apply to personal data, which because of the manner in which they are processed, or because of their nature or the context in which they are used *pose a danger to privacy and individual liberties*. In today's terms, we might think of risk rather than danger.
- The T-PD, in the modernisation of Convention 108, considered the scope of personal data, deciding to retain the definition. However, it clarified that "identifiable individual" means a person who can be easily identified, and that the notion also refers to what may single out one person among others (and thus allow then to be treated differently) . Similarly, the Article 29 Working Party issued an opinion stating "… that a natural person can be considered identifiable when, within a group of persons, he or she can be

distinguished from other members of the group and consequently be treated differently”. Maryland (USA) is also considering legislation that would extend the scope to “any information that can be used to distinguish an individual”.

- When thinking about scope it is important to keep in mind that privacy concerns vary from individual to individual. They need to be equipped with tools to understand and control their perceived privacy risks. However, as data science improves, privacy does not depend on matters only within our control – e.g. a third party may learn something about an individual through observable facts about his or her associates.
- There is a general lack of awareness among users concerning the degree to which individuals are identifiable and that there is a fundamental blurring of the division between data which is personal and data which is not. Coupled with identification, there is also the issue of user observation, sometimes across multiple devices.
- Perhaps we need to analyze this question from the perspective of risk: Is there a risk in disclosing the information? What is the risk in using or not using the information? Who decides whether the risk is acceptable? Who bears the consequences of that decision?
- Perhaps we should focus more on the use of data and for what purpose, rather than whether data is personal or not.
- While data collectors and users may want a traffic light indicator as to what is permissible, the approach that may need to be taken is to require that they respect the privacy and interests of the individuals whose data they are collecting – a transparency and a context-based approach.
- More nuanced responses as to how personal data should be treated are needed because, for example, there more players in the data ecosystem, with different roles and objectives.

What is “anonymised” data?

- It is an oxymoron. It might be achievable within a data set, but even over time we might discover that individuals are identifiable. If law simply prevents the combination of data sets to avoid de-anonymisation, it might be unwittingly preventing innovation (e.g. in medical research).
- We cannot anticipate what information will be available to be combined with “anonymised” data, which is why a risk-based approach would be preferable to a definition of personal data that tries to anticipate what data may be combined in the future.

Multistakeholder processes and the privacy dynamic

- Given the complex facets of privacy and identification, multistakeholder processes hold promise to develop privacy policy, law and technical standards.
- The privacy dynamic might change if all users were fully aware of what is happening with their data online.

Some additional discussion items:

- Initiatives on user-managed access
- Security to support privacy
- Licensing for data sets – e.g. creative commons

- Tools to “fuzzy” data
- The right to be forgotten
- Accountability and trust

Recommendations from the session.

"We encourage all stakeholders to help raise awareness among Internet users about online privacy and data protection issues, as well as privacy-protecting tools and strategies."