

**e-Forum privacy working group
Second meeting, Sheffield, UK, 15 April 2010
Minutes**

Attendees

Pedro Antunes (University of Lisbon), Juliet Craig (Futurage/University of Sheffield), Xiudian Dai (Hull University), Illesh Datani (GENOM project), Mick Davies (Local Authority Smartcard Standards e-Organisation), David Fisher (University of Sheffield), Margaret Ford (Consult Hyperion), David Fortune (Yorkshire Forward), Jonathan Gay (Diginus), Alexander Hanff (Privacy International), Stephan Heim (Goethe University, Frankfurt), Iain Hinchley (University of Sheffield), Dominic Mayes (University of Sheffield), Viera Murinova (European Union Agency for Fundamental Rights), Pia Reinthaler (University of Sheffield), Megan Roberts (University of Sheffield), Gary Simpson (EASY Connects), Mark Smith (University of Sheffield), Shaun Topham (e-Forum), David Waring (University of Sheffield), Bridgette Wessels (University of Sheffield), David Willis (Hull University), Robin Wilton (Kantara), Hannah York (Sheffield Hallam University)

The second meeting of the e-Forum privacy working group (PWG) took place on 15 April 2010 at the Showroom Cinema and Workstation, Sheffield, UK. The meeting was part of an event hosted by the University of Sheffield and e-Forum, entitled 'Yorkshire and the eUnion: Responding to the Malmo Ministerial Declaration'. More details about this event can be found at <http://www.yorkshire-eunion.com/>.

Opening

The PWG meeting was opened by Bridgette Wessels of the University of Sheffield, who gave a brief overview of the **seven objectives approved by the PWG** at its inaugural meeting in Brussels, 8 February. These objectives are:

1. Define the personal sphere: what is an identity?
2. Map privacy to different contexts
3. Define an holistic view on privacy: legal, technical and sociological
4. Make people aware of the value of and ability given by data ID
5. Prepare a (privacy) roadmap; understand what is on the horizon (including implications of the Stockholm Programme for privacy)
6. Map (privacy) cultural differences across Europe
7. Consider what level of interoperability is needed, considering that more interoperability leads to less privacy

Bridgette passed on the apologies of David Newman, of the HUWY project, who was scheduled as a speaker but unable to attend because of a flight cancellation. HUWY is an eParticipation project funded by the European Commission. It deals with young people and privacy, and related online problems such as cyberbullying and identity theft. Bridgette Wessels noted that younger people have a different view of privacy from older people, and this has in part been conditioned by lifelong exposure to online technologies. The HUWY project will be featured at the next PWG meeting.

Defining identity

Alexander Hanff of Privacy International started a wide-ranging and at times lively discussion by considering some of the issues identified for further work by the PWG first meeting. On the question of defining identity, he put forward suggestions such as DNA and social identity, but said that a basic definition of identity was a dataset that defines an individual. With the advent of modern technology, this dataset has expanded, and now includes a wide range of microdata, such as online surfing habits, which when put together in a profile generate a digital fingerprint that can identify an individual.

It was noted that identity in the digital age is based on profiling, which is being developed by companies and authorities at a rapid rate, enabling them to identify patterns of individual behaviour. One use of this information is as the basis for targeted advertising, which, Alexander Hanff noted, is far more successful from the advertisers' point of view than generalised advertising.

The question then arose of who owns and has rights over profiles? This is a key issue at present with service providers such as Facebook and Google. In some cases, individuals react to profiling by changing their behaviour, but where there are trust relationships with providers (eg Facebook), this tends not to happen. However, few people grasp what is being done with their profiles. Alexander Hanff noted that Facebook offers certain protections to its users with regard to the collection of information, but protection does not necessarily apply for third-party apps linked to Facebook. He added that there is a risk of the value of privacy being diluted until individuals simply accept they no longer have privacy.

Hanff also said there was a risk of "function creep", whereby having information in digital form means it is easy to exchange and there can be a perception that more use can be made of it. Insurance companies might want direct access to health records, for example. Hanff also warned that companies are developing uses for data on the fringes of the law and are in this way trying to push for fewer restrictions on data use.

On the working group objective of mapping privacy to certain contexts, Hanff said that for Privacy International, privacy is an absolute, with principles that do not change whether the context is public, private or commercial. The next step for the group could be to define the contexts against which privacy is to be mapped.

Enforcement

Alexander Hanff said that EU data protection legislation is strong, but there is an enforcement gap. There is a tendency to react to events, for example terrorism, with privacy-invading technologies, such as full body scanners, and then to attempt to deal with privacy or data protection concerns *ex post facto*. Instead, questions should be asked at the outset if the reaction is appropriate to the problem. Electronic identity cards, for example, should have a limited use of proving an individual's identity to people that do not know him or her, and should not be a means of monitoring movements or behaviour.

FUTURAGE

Juliet Craig of the University of Sheffield gave a presentation on FUTURAGE (<http://futurage.group.shef.ac.uk/>), a European Commission funded research project to identify the needs in the next 10-15 years for research into ageing. The project had already considered a number of data protection/privacy issues, Juliet Craig said. For example, as individuals age, more health information is collected about them, and this is exchanged "behind the scenes". Data may also need to be transferred across borders, for example if northern Europeans retire to the warmer countries of the south. Data can also be used to identify patterns related to vulnerable older people, for example if particular care homes or doctors report more injuries or problems than others, triggering an investigation. A further issue is the question of "healthy ageing". According to Juliet Craig, how individuals age is due to a lesser extent on genes, and to a greater extent on lifestyle and habits. Lifestyle information can therefore be used for profiling to determine what individuals' healthcare needs will be in old age. The presentation raised the issue of "care versus control" -- at what stage does monitoring of people's behaviour in order to care for them become intrusive?

Discussion

Following the presentations, a discussion took place on two themes: care vs. control, and the enforcement of data protection of legislation.

In the **enforcement** discussion, it was noted that EU legislation is robust, with only Canada having stronger privacy protection laws. However, the PWG could focus on making the rights enshrined in data protection law more "real". Alexander Hanff said that in the UK, for example, the law in this area is wide-ranging, but in practice the powers of the UK Information Commissioner are limited, and there have been a number of breaches of the law by public authorities, with no real sanction applied.

The aim should be to identify realistic ways of enforcing the current legislation, rather than changing the legislation. For this, the engagement of policymakers is needed, with the European Commission especially important in this respect.

The discussion on **care vs. control** was longer and at times lively. Participants discussed, for example, care schemes for elderly people and how these must take into account dignity and the right to privacy. One view was that there should be a clear line between care and control, and that steps should be taken to ensure that care is appropriate, and that the choices made about offering services do not lead to the normalisation of intrusive behaviour. It was felt that the current framework within which such services are provided is adequate, as long as the fundamental aims of current policy are kept to.

Gary Simpson for the FASTeTEN project gave concrete examples of services currently under consideration that require exchange of data and trust between participants. In South Yorkshire, the FAST secure infrastructure for information exchange (see <http://www.eu-fasteten.eu/>) could be used for six mini-projects:

- Exchange of confidential information between the police and Neighbourhood Watch services;

- Sharing of health information with teams outside the health authority;
- Sharing of information as part of "good neighbour" schemes, with the aim of helping communities help themselves;
- Exchange of information between public authorities and the voluntary sector, for example groups providing hot meals for elderly people;
- Enabling local public services (eg doctors) manage budgets and contract with their suppliers individually, rather than through the health authorities;
- Giving parents tools to give permissions for, for example, school trips, securely and electronically.

Alexander Hanff said that these examples did not present privacy problems in themselves, but problems may occur in implementation. The services provided should always be proportionate, with data used ethically.

Shaun Topham of e-Forum said problems for local authorities often come up because data protection rules are "a blur". This leads to a risk-averse mentality, where public workers may not make decisions for fear of breaking the rules. More clear and simple rules are needed.

Discussion then centred around the idea of information technology as being "remote" from people and communities. The FASTeTEN sub-projects outlined by Gary Simpson would in effect consider how technology could be used to reinforce trust within communities by working with trusted partners (for example, Neighbourhood Watch). Would technology enable the building of communities around services, and thus reinforce trust within communities? Alexander Hanff said doing this would require more than having a checklist of rules that must be observed as the basis for "trust". Instead individuals and communities must feel involved in the services aimed at them, which can be difficult for service providers to do when information technology is often seen primarily as a way of cutting the cost of services.

Conclusions

To conclude the meeting, the PWG split into three groups, with the aim of identifying ways in which data protection legislation can be better understood, and how the care vs. control tightrope can be walked. For both of these, it was noted that more bottom up trust of information technology is needed.

The conclusions were:

- Companies/service providers need to come closer to communities by building "common sense" into their services;
- There may be a gap for eSecurity companies to look after the online security and privacy of individuals and organisations, in the same way that security companies operate in the physical world;
- Privacy needs to be "by design" and built into ICT infrastructures;
- Accountability needs to be strengthened, with better redress and enforcement of legislation; for example, local authorities could have their own information commissioners;
- Bottom-up understanding of technology needs to be improved, with better education about online services;

- Identification should not require excessive data exchange, implying more use of federated keys; for example an ID card as proof of age does not require name and address details;
- National data protection bodies should have dual roles, with powers to help individuals manage identity (for example, providing websites showing who has access to one's data), and robust enforcement powers.

Next meeting

The next meeting will be held in Brussels last week of May/ first week of June on a date to be decided.