ICTethics – Report on the Expert Workshop on Human Security

Yorkshire Forward, Leeds, United Kingdom, 26 November 2010
University of Leeds, United Kingdom, 27 November 2010

Human Security in the context of Ambient Intelligence
In search of a shared Ethical, Social and Legal Approach

We make many assumptions about machine-facilitated information exchange. We assume it is simple, based on common and shared legal regulations which are implemented in unproblematic ways. We assume information is 'hard text' and little else. We assume that in the context of combating fraud and crime, information sharing is good operational and organisational practice.

The workshop on **Human Security in the context of Ambient Intelligence** is part of the FP7 ICTethics project (contract no. 230368). It was organised by the University of Leeds whose research focuses on issues of identity, notably, in relation to Security and Biometrics.

This workshop provided an opportunity for the ICTethics team to present their research and have their research challenged and informed by the real world of security experts. The debates focused on the implementation of ambitious local and EU policies to improve security, and how ICTs are used to attain operational and organisational objectives. The ethical controversies of using ICTs were explored in depth.

Feedback was extremely interesting, offering new perspectives and direction to the future of the ICTethics project.

Presentations

Session: *Information exchange in the context of combating crime and fraud*
Chair: *Juliet Lodge*

Juliet Lodge, Professor of European Studies at Leeds University, Director of Jean Monnet Centre of Excellence, chaired the session on **Information exchange in the context of combating crime and fraud**. The session aimed to confront the rhetoric of what biometrics are as well as their reality—whether the use of biometric technologies is as ubiquitous and effective as is commonly assumed and whether and how their uses pose challenges to our understanding of profiling, social sorting, and the impact on society. The challenging question was posed, whether there is need for a specific code on ethical applications of ICTs for security (including biometrics, however defined); how this might be considered. Is it feasible and/or desirable to start with the high ambitions of universal, international declarations of core principles, or should there be local declarations of principles in particular fields as a starting point for harmonising regional, national and EU rules and standards? Or, are both these endeavours utopian and pointless in view of the speed of ICT developments and implementation, the impact of AmI and the actuality of information sharing, mining and mission creep?

1. Daniel Nagel

Top ten ways to transmit and (ab)use data and not get caught

Daniel Nagel highlighted the vulnerability of the data protection legal framework. He presented ten ways to abuse personal data without any legal consequences. Illustrating this with reference to data misuse cases, he noted legal gaps on storage, control and exchange processing of digital data. The main issue he stressed was the difference even within the European Union in the definition of legal terms such as *data controller and data processor*. This leads to gaps in data protection laws, and allows for arbitrary interpretation, according to circumstance. Data outsourcing remains problematic: data gathered in one country but stored in another are subject to different legal regimes. Even strictly enforced data protection law is an insufficient safeguard because the broad interpretation of the term *data* can raise serious privacy issues. The question of consent regarding data collection also remains problematic. He argued that by creating a threat, people tend to agree to personal data collection without questioning the need for it. Finally, he noted that a way to abuse data was facilitated by new ICT capabilities, especially in a cloud which allows someone to be hidden. The cloud splits the data between servers therefore is impossible for the subject to know where his/her data are stored and consequently he/she does not have any means to control these data. The counterpart issue is whether it is easy to collate and match up already split data.

Questions about the ownership of data and liability were posed, along with some questions regarding CCTV and online behaviour data use post collection —i.e., the control and use of these data.

2. DSgt Andrew Staniforth

From Twin Towers to Times Square - Tracking the Evolution of Terror

Detective Sergeant Andrew Staniforth from the Futures & Command Support Team provided a personal account of his work in countering terrorism. Posing as an example the crucial-for-security-area in the aftermath of the 9/11 events, he referred to the 9/11 Commission Report which concluded that domestic agencies were not mobilised in response to the threat and electronic surveillance was not targeted against a domestic threat. The public was not warned. He presented the statistics on security spending in the US. In 2001-2002, the US Administration spent 157 Billion US Dollars on CT and Homeland Security whereas in 2003-2004 - to support the ‘War on Terror’ - this figure rose to 347 Billion, and for 2008-2009 close to $500 Billion. The second part of his presentation focused on the case known as 7th July 2005 – Alexandra Grove, posing the question whether this terrorist attempt was unexpected when CCTV cameras are everywhere. If the target was specific, police officers should have seen it in the data. He outlined scenarios for future terrorist attacks stating that the police lack access to the futuristic technology accessible to terrorists, owing to financial and knowledge constraints. He highlighted how the police are constrained in using existing technology, constrained to strict codes of practice which therefore makes combating terrorism more difficult. He concluded that technology nevertheless could be the key to progress.

The discussion focused on whether ICTs can be the answer to terrorism. This led to further discussion over the nature of ICTs “life time”. What do we mean by “life time”? What happens if the police are faced with information overload and too much information that cannot be used. This situation would raise new questions about the ethical limits of surveillance.

3. Dr Angela Carpenter

Maritime Security and EU Seaports

Dr Angela Carpenter presented the situation of maritime security. She stated that EU seaports are a gateway to Europe for both goods and services, where over 90% of EU external trade goes by sea and over 404 million passenger journeys were made through EU seaports in 2009 (Eurostat). Illustrating the security threats, Angela referred to bombings, narco-terrorism, people and weapons trafficking, illegal immigration, smuggling, drugs, arms etc. She presented the EU LRIT which is administered globally by the International Maritime Organization under SOLAS (Safety of Life at Sea Convention, 1974) amendments of May 2006. This administration is integrated into the wider LRIT system with a Data Centre operational since June 2009. The EU LRIT aims to track and monitor all EU flagged vessels and links to International Data Exchanges for information on foreign flagged vessels. She presented the SafeSeaNet (SSN) maintained by the European Maritime Safety Agency. This is a system for receipt, storage, retrieval and exchange of information for maritime safety, port and maritime security, marine environmental protection and efficiency of maritime traffic and maritime transport. THETIS is also a system developed by EMSA to facilitate and support Port State Control inspections and it is to be linked with SSN to identify vessels requiring inspection and to record the result of inspections.

The discussion focused on the security threats in ports. It was seen as paradoxical that airport security is being boosted while ports seem to be left largely unprotected. The discussion concluded that no matter how advanced ICT uses may be, human intervention remains crucial.

4. Det Insp Howard Atkin

Detective Inspector Howard Atkin argued that the driver is not the technology but human beings. Individuals affect change in the world of Information Technology. Different cultures bring different perspectives and fashions that influence adoption or rejection of any new technology. Atkin stated that among all data trafficking online, 53% occurs in Facebook. Culture, he argued, changes rapidly in parallel. He disagreed with Staniforth on the pivotal focus on using technology to solve problems, arguing that more advanced technology does not equal more effectiveness. Referring to ethics, Atkin stated that crime is a global phenomenon, which includes the use of ICTs but also means that across the world, people's attitudes and perspectives on ICTs differ. There is no single legal code or understanding and this is why we cannot apply the same code or method across the world. Regarding cost, he stated that we should not focus on the notion of cost-efficiency in relation to data gathering. Data interpretation is very expensive and data handling officers would need to be much better paid if outsourcing – including to the private sector – is not to introduce further risks. Atkin stressed that information is not intelligence and we have to concentrate on realistic methods that can stop terrorists accessing and using personal or other data. Finally, Atkin stated that the activities of terrorists play into the hands of dominant business models which encourage the proliferation of ICTs for security, and that the 9/11 attack was in fact a "business message". Far more people die from traffic accidents or on the streets each year than did in the 9/11 attack.

5. David Fortune

David Fortune stated that UK is the most surveilled society, not because there is a need for it but because this situation is financially driven and Police officers consider an action ethical if it is legal. Fortune also explained that nowadays police use the technology just because it is available. If they do not use available new technology they can be criticised. According to David Fortune data gathering is not the issue as such. People are quite willing to give up their data when they have something to gain, not simply security but even something trivial. The challenge lies in building from data relevant and usable knowledge and in an appropriate way.

6. Dr Michael Carpenter

Dr. Michael Carpenter talked about medical information. He argued that what is stored is opinion and not hard facts. Drawing on the practice of medicine, he stressed the difference between fact and interpretation in what it is that the 'information' is. Consequently, accuracy – in the medical field - depends on the acquisition of hard factual data and their correct interpretation in the light of available technology. Regarding DNA, Michael Carpenter referred to the threat of "knowing". DNA could give information not only about the present health condition of a patient but future one as well. Apart from the fact that patients have the right to ignorance there is a great concern over the misuse of such data. He gave the example of insurance companies that might use knowledge of potential risk of cancer for a client to deny selling him/her insurance. The interpretation of data was also in this case a point that led to debate.

Session: *Security in the context of Ambient Intelligence*
Chair: Guido Van Steendam

During the second session of the workshop, members of the ICTethics Consortium illustrated the social, ethical, legal aspects respective to the responsibility to maintain security, and looked at through the prism of a critical analysis of Ambient Intelligence developments.

Dr Kristrún Gunnarsdóttir (Lancaster) stated that Ambient Intelligence research has not matured enough in the last ten or so years to enable incremental developments. According to Gunnarsdóttir, the vision of AmI and the promotion of AmI research and development – originating and maintained for the most part at Philips – has focused on the role of seamless intelligent environments that understand and adapt to the presence of people, and to situations such as moods or ordinary expectations. The idea has been that intelligent applications and environments should free people from having to control their surroundings. Gunnarsdóttir posed critical questions about the current status of AmI research and development:

- How well is the technical problem domain known, i.e., AI, reliable detection of moods, expectations, etc?
- When we read and hear about AmI, should we not be suspicious that the term “automation” is used in relation to socially and emotionally relevant settings?
- Will a fully integrated AmI landscape be implemented in another 10 years time?

Gunnarsdóttir stated that a new wave of ICT innovations for AmI applications shifts our thinking about monitoring and surveillance technologies away from issues of safety and security to issues of everyday private and occupational lives supported with advanced ICT applications. Applications are developed for commercial purposes, although they have been and can be sold in the name of safety and security. But, there are still unanswered questions about new applications for safety and security purposes:

- To what extent do the technological developments as they stand undermine rather than support the discourse of securitization?
- How is the criticalness of outliers addressed in system that are designed for safety purposes, when they collect ever more data and use ever more sophisticated collection and processing methods to find the single critical anomaly?

Gunnarsdóttir concluded here by posing the question whether we should rely on the concept of Ambient Intelligence for the work done for the ICT ethics project. Finally, Gunnarsdóttir posed some ethical questions regarding developments to-date with focus mainly on professional accountability.

Professor Juliet Lodge and **Pinelopi Troullinou** (Leeds) illustrated the social aspects of ICTs, using the example of biometric passports. What is it about security in the context of emerging AmI environments that will impact society? How will the person be regulated by ICTs in AMI environments? How is the person identified and individual identity made instrumental to human security? Their presentation examined identity tokens and their potential impact on society. Through the presentation of a case study, they focused on identity tokens and inequality. They stated that the decision to include biometric identifiers in passports in the EU does not mean that the same biometric is enrolled, or that a uniform European biometric passport exists or has been adopted simultaneously by all the member states. Technical issues have delayed decisions about implementation in some member states. Furthermore, member states may be obliged to collect and store the same biometric identifiers, but there are differences in the technologies used for enrolment, the price of the resulting travel document, and the duration of the validity of the passport. Does this flexibility compromise EU citizens' equality? Some questions they posed:

- Will biometric security tokens boost collective and individual security in AmI environments?
- Do biometric security tokens promote social discrimination in ways and with consequences and practices that might be considered (un)ethical?
- Do biometric security tokens raise further risks to collective and individual security?
- Do biometric security tokens belong to the individuals or, is it ethical that after their collection and storage, they belong to the government or private companies, and become their property, possibly open to commercialisation?

The concluding question was if new biometric technology goes beyond the token. Should the token be abandoned as unnecessary?

Rocco Panetta (Fondazione Basso) illustrated the legal aspects of AmI in the context of human security. Panetta stated that the notion of security has a strong impact on the development of Ambient Intelligence. Privacy is a key concern and Data Protection authorities aim to protect it but the notion itself is replete with misunderstandings. The PNR case illustrated this in his view. Private and public sector involvement is a matter of concern, and highlights the need to monitor privacy and data protection. While he welcomed privacy by design, he referred to the continuing relevance of the law. While there is a trend to consider privacy as obsolete and irrelevant because it cannot be protected, new problems arising from new ICTs prove the opposite. The EDPS is the only body to keep the balance between data and human security. He stressed that the belief that this body does not have any power is wrong. Panetta concluded his presentation by arguing that the solution is to find symmetry among the EU27 and across the world over the notion of privacy and its protection.

Guido Van Steendam (IFB) presented Ambient Intelligence in the present and its potential ubiquity. Van Steendam stated that the promotion of security is older than ICT, and privacy has always been a problematic concept. There is not a pure private sphere when dealing with social matters. ICTs seek to minimise risk to society by profiling people so in a world full of diversities and conflicts the question is what do we do.

The workshop closed with a brainstorming for further research and debate and what the next steps will be. It was agreed to collaborate on writing a paper on the issues under review.

- It was agreed that a new concept for privacy and security is necessary.
- The balance between security and privacy was underlined.
- Crucial questions were posed:
    - Who decides ethics?
    - Is there any role left for ethics in modern societies?
    - ICTs redefine the borders?
    - What is the future of security and data protection?