



DIALOGUE

Volume 1 • No. 3 2008 | December

FEATURE ARTICLE

Surveillance in the UK:

A View from the House of Commons

IN THIS ISSUE

- 1 *Feature Article*
Surveillance in the UK: A View from the House of Commons
- 3 *Focus Group Report*
System Interoperability of Biometrics and Personal Detection Technologies
- 7 *Focus Group Report*
Biometrics and Body Data in Embedded Systems and Ambient Intelligence
- 9 *News and Notes*
- 10 *Partner Profiles*
Cesagen and Zuyd University

DIALOGUE is published quarterly by The Hastings Center, a HIDE Partner.

PRINCIPAL INVESTIGATOR
Thomas H. Murray, *President and CEO*

EDITOR & PROGRAM MANAGER
Karen J. Maschke, *Research Scholar*

ART DIRECTOR
Nora Porter

MANAGING EDITOR
Joyce A. Griffin

CONSULTING EDITOR
Gregory E. Kaebnick

This work was supported in part by the European Commission under contract FP7-217762 HIDE, Homeland Security, Biometric Identification & Personal Detection Ethics.



by Paul McCarthy and Katja Jacobsen, Cesagen

Concerned about public perception that the United Kingdom is becoming a surveillance society, the Home Affairs Committee of the House of Commons recently initiated a wide-ranging inquiry into the collection, storage, and use of personal information to tackle crime, manage borders, and deliver public services. In June 2008, the Committee released its findings and recommendations in a report titled *A Surveillance Society*?¹ The Committee noted that its inquiry reflected an attempt to build on an examination of surveillance issues the Surveillance Studies Network undertook for the UK Information Commissioner. In particular, the Committee said its focus would be on several “large strategic issues of concern to the general public,” including 1) public agency access to private databases, 2) data sharing between government departments and agencies, 3) data use safeguards and data abuse monitoring, 4) privacy impact assessments, 5) privacy-enhancing technologies, and 6) profiling to identify people as potential criminals. With these issues in mind, the Committee examined several forms of data collection and surveillance the Home Office (the governmental department responsible for criminal

matters in the United Kingdom) uses to fight crime: identity cards, camera surveillance (known as CCTV), and the National DNA Database (NDNAD).

“The report’s main argument is that surveillance can lead to citizen distrust of the government, which can damage the social contract between citizen and state.”

The Committee’s report contains chapters organized around several key questions: What is surveillance? Why has the use of surveillance increased? What are the implications of the growth in surveillance for the individual and society? Are existing safeguards strong enough? What role does surveillance play in the work of the Home Office and the fight against crime? To answer these questions, the Committee invited input from key stakeholders in the United Kingdom

CONTINUES ON PAGE 2

and the United States, including law enforcement and other governmental agency officials, academic scholars, and representatives of nongovernmental organizations (NGOs) that deal with privacy and surveillance issues. The Committee identified ground rules it thought the UK government should adopt for the collection, storage, and use of personal information and issued a set of recommendations for data collection, data retention, data processing, and data protection.

The Importance of Trust

The Committee stated at the outset that it rejected “crude characterizations of our society as a surveillance society in which all collections and means of collecting information about citizens are networked and centralized in the service of the state.”² Nonetheless, the Committee agreed that the potential for government surveillance has increased and that the United Kingdom could become a surveillance society in the negative sense “unless trust in the Government’s intentions in relation to data and data sharing is preserved.”³ The report’s main argument is that surveillance can lead to citizen distrust of the government, and that the lack of trust can damage the social contract between citizen and state in subtle, yet lasting ways. Although the Committee recognized that private sector data collection can result in consumer benefits such as convenience when using credit cards and retailer reward programs, it noted that public sector collection, storage, and use of personal information could erode the ability of the state to govern effectively if citizens feel they are continually being monitored as potential criminal or terrorist suspects.

Design, Technological, and Regulatory Safeguards

A central theme of the Committee’s recommendations is the principle of data minimalization. This means that the collection of personal information should be adequate for and relevant to the specified purpose or purposes

for which it is to be used. Ideally, the government would collect only the most basic personal information it needs to effectively deliver public services and carry out other activities, and the data would be retained for the shortest possible amount of time. Moreover, clear oversight structures should be in place governing those who have access to individuals’ personal information.

According to the Committee, “every system for collecting and storing personal information should be designed with a focus on security and privacy.”⁴ One way to do this is to carry out privacy impact assessments (PIAs). However, the Committee expressed concern that PIAs might be viewed as empty bureaucratic exercises implemented after technological systems and policies for data collection have been established, “by which time their value as a practical risk assessment tool would have been lost.”⁵ Thus, PIAs and other privacy and security measures should be implemented before and during the design phase of any technological system, not after the system is already in place.

The Committee also noted that individuals can use privacy enhancing technologies (PETs) to protect their private information but recognized that the value of these technologies is limited. For instance, PETs could exacerbate the class-based “digital divide” between those who know about PETs and can afford to buy them and those who don’t have the knowledge or money and, thus, are more vulnerable to public and private entities collecting and using their personal information. Because of this, the Committee stressed the need for design processes and policies that shift the responsibility of protecting personal information to those who collect and use such information, rather to the individual whose information is being obtained.

With regard to the collection and sharing of personal information to fight crime, the Committee called for increased oversight—and, in some cases, additional regulation—of gov-

ernment surveillance activities. The Committee criticized plans for both larger and merged, interoperable databases and suggested that larger databases should be created only when there is a clear, demonstrable need to do so. In addition, the Home Office was called on to clearly explain and document its use of the Regulation of Investigatory Powers Act (RIPA). The Committee also recommended that any further expansion of camera surveillance be justified by showing a demonstrable need and by explaining to the public how such surveillance will be effective in fighting crime. Although CCTV schemes are popular with the public, it’s difficult to quantify their benefit and to show that the benefits outweigh infringements on individual liberty. Thus, the Committee recommended that the Home Office 1) develop ways to increase public awareness and manage public expectations of CCTV, 2) foster greater transparency regarding camera surveillance, 3) promote the principle of data minimalization when developing camera surveillance schemes, and 4) reject surveillance schemes that include the use of microphones.

On the matter of the soon-to-be launched National Identity Scheme—which will involve biometric identity cards for foreign nationals beginning in late 2008 and for British citizens in 2009 (and a National Identity Register)—the Committee raised several concerns. According to the Home Office, the National Identity Scheme is not designed to be a surveillance tool, but a mechanism to “protect individuals’ identities from abuse and provide a secure way for people to prove their identity more reliably, helping to tackle illegal immigration, crime and terrorism as well as improving public services.”⁶ Yet the Committee warned about the potential for governmental surveillance and recommended that the Home Office produce a report identifying the intended functions of the program regarding crime control and containing an explicit statement that admin-

CONTINUES ON PAGE 4



System Interoperability of Biometrics and Personal Detection Technologies

By Victor M. Lee, IBG

Thanks to technological advancements in communications and transportation, the world has become increasingly interconnected. This phenomenon has prompted increased regional and international cooperation to facilitate the flow of information across national borders. Yet the efficiency, success, and resulting value of such information exchange depend on system interoperability—the ability of two or more systems to exchange information and to use the information that has been exchanged. Although system interoperability is a fixture of the modern information society, concerns about privacy, data protection, and other ethical issues surface when personal information obtained from biometric systems or from personal detection technologies becomes part of global, interoperable data networks.

On September 15, 2008, HIDE partner International Biometric Group (IBG) hosted a focus group meeting to examine some of these ethical issues. The focus group meeting began with Victor Lee framing the issues to be discussed and summarizing the background document that participants received prior to the meeting. Next were contextualizing presentations from Asbjorn Hovsto and Benjamin Schouten, followed by an open discussion of all three presentations and the broader ethical issues pertaining to system interoperability. Lee and Michael Thieme moderated the focus group discussions.

Presentation Sessions

In his presentation, “Ethical Dimensions of System Interoperability,” Lee created structure for the focus group meeting by introducing key terms and concepts. He noted that system interoperability is driven mainly by two motivations: security/safety needs and economic needs. Security/safety needs include border security, as well as identification and surveillance of those within a country or region. Lee cited US-VISIT and the Schengen Information System II as examples of biometrics border security programs whose large scale necessitates system interoperability. He also mentioned the London “Ring of Steel” project, an expansive surveillance deployment around the City of London that combines CCTV camera and license plate recognition technology. Lee then broke down economic needs driving system interoperability into three categories: the desire for economies of scale; freedom from dependency on specific proprietary solutions; and the pursuit of standardization efficiencies.

According to Lee, system interoperability is typically achieved through standardization, establishment of central databases, and/or reciprocity of system/database access. Lee gave the

example of EURODAC, a European fingerprint database under European Commission management that facilitates the identification of asylum seekers and deters “visa shopping” within Norway, Iceland, and all EU member states except Denmark. Lee emphasized that the drive towards

“ How can “scope creep”—using databases for broader purposes than originally intended—be minimized? How can access to centralized databases be balanced among nations? ”

system interoperability was counterbalanced by restraining forces, such as respect for individual rights, data protection obligations, and privacy concerns. He pointed out that at minimum, there was a need to respect the provisions in the Charter of Fundamental Rights of the European Union and European Parliament Directive 95/46/EC (1995), which sets out requirements for sharing personal information. He acknowledged, though, that enforcing such provisions would be difficult without an active enforcement mechanism and/or the creation of market incentives to deter abuse or overzealous pursuit of system interoperability.

CONTINUES ON PAGE 5

istrative information collected and stored will not be routinely used to monitor individuals' activities.

As to the NDNAD, the Committee agreed that it is a valuable investigative tool, particularly for older, unsolved cases. However, the Committee said there should be an established and observed "regulatory framework which protects individuals from unnecessary invasions of privacy and loss or unauthorized use of their genetic material and information gleaned from it."⁷ In addition, the Committee said there was a need for 1) government assurance that the NDNAD would not be used to correlate particular genetic characteristics with propensity to commit crime, 2) clarification of the purposes and processes of DNA collection and retention, 3) new legislation to replace the current regulatory framework that includes "a more accessible mechanism by which individuals can challenge the decision to retain their records" in the database, and 4) Home Office and police review of the identifiers used for samples and the sample retention policy. Finally, the Committee said that the Home Office should not undertake or sponsor work that involves the use of patient data or information about children for the purpose of predictive profiling regarding criminal behavior.

Policy Questions and Discussion Points

Overall, the Committee encourages the UK government to give greater consideration to the types of personal information it collects, how that information is stored, who will use it, and for what purposes. The Committee expressed concerns about the amount of overlapping and often unnecessary personal information the government collects and questioned the manner in which personal information is shared by governmental agencies without informing citizens about those data sharing schemes. The Committee also expressed concern about government plans to develop larger databases than currently exist to make all its databases interoperable.

The importance that recent data losses in the United Kingdom may have on the governmental and public response to the Committee's report cannot be overestimated. Over the last 18 months, military personnel and credit card data have been lost, not to mention the personal information of 25 million welfare recipients.⁸ These data losses received widespread media coverage and have likely contributed to increased public concern over the nature of data being collected, which agencies and actors are storing the data, and the regulation of access to and use of personal information. Moreover, there is a growing unease among UK citizens about increasing government surveillance, especially when local governments turn to emergency terror laws to conduct surveillance on citizens for trivial matters such as truancy and the failure to recycle waste. Yet the reluctance of law enforcement representatives to address in their comments the Committee's concerns about the NDNAD retaining DNA samples for 100 years suggests that it may be difficult to alter current policy on some matters involving the collection of personal information. Moreover, it's unclear whether the Committee's recommendations will be applied to citizens and noncitizens, including "bad" citizens who have violated the social contract. Distinctions among "trusted citizens," "untrustworthy citizens," and "others" could be just as damaging to the social contract between a government and those living within its borders, especially in a diverse, multicultural society that includes a large population of noncitizens such as the one in the United Kingdom.

The Committee's report suggests that many of the issues the HIDE project will address are on the agenda of at least some UK government officials and that those issues are being examined within an EU framework (as is the case, for example, with PETs). Listed below are several questions and discussion points that might inform further dialogue for HIDE partners and key stakeholders:

- Can the United Kingdom be considered a surveillance society by the standards of other countries?
- Is privacy a core part of the social contract between citizens and government, and is this only relevant to UK conceptions of citizenship?
- What relevance will the Committee's report have for other data collection schemes modeled after those in the United Kingdom, such as the National DNA Database?
- Data losses in the United Kingdom have been widely reported. Are there instances of data losses within other countries? How have they been reported?
- Is data minimization a principle the HIDE project should recommend in relation to the use of privacy enhancing technologies, as well as for general guidelines for personal detection technologies?
- Are we correct to point out the distinction between "others" and "trusted citizens"? Are there ethical observations to be made from such divisions? Have we overemphasized such differences?

1. House of Commons, Home Affairs Committee. *A Surveillance Society?* Fifth Report of Session 2007–2008, Volume 1, May 2008.
2. *Ibid.*, p. 10.
3. *Ibid.*
4. *Ibid.*, p. 6.
5. *Ibid.*, p. 61.
6. *Ibid.*, p. 70.
7. *Ibid.*, p. 85.
8. Bowcott O. FBI wants instant access to British identity data. *The Guardian*, January 15, 2008, <http://www.guardian.co.uk/uk/2008/jan/15/world.ukcrimep>; Oates J. 2007 worst ever year for data protection. *The Register*, January 7, 2008, http://www.theregister.co.uk/2008/01/07/lib_dems_data_losses/; Summers D and Stratton A. Brown apologizes for data blunder. *The Guardian*, November 21, 2007, <http://www.guardian.co.uk/politics/2007/nov/21/economy.uk>; Darling A. Another day, another disaster. *The Guardian*, November 21, 2007, <http://www.guardian.co.uk/commentis-free/2007/nov/21/economy.politics>; O'Brien C. Personal data of 380,000 welfare recipients stolen. *The Irish Times*, August 12, 2008, <http://www.irishtimes.com/newspaper/ireland/2008/0812/1218477342243.html>.

Drawing from the current landscape of interoperable systems, Lee noted that there is a tension between the desire to expand system interoperability and the need for containment. This tension raises several questions: How can “scope creep”—using databases for broader purposes than originally intended—be minimized? How can access to centralized databases be balanced among nations with varying data protection standards? What are the criteria for determining the extent to which data protection standards should be open? How should the benefits and costs be assessed when combining interoperable personal detection and/or biometric systems? How should the importance of informed consent regarding the use of personal information be evaluated? On the matter of informed consent, Lee proposed that the greater the need for regulatory protections and safeguards, the greater the need for informed consent and for justifying the need for system interoperability.

In his presentation on “Identity Management in e-Health,” Asbjorn Hovsto built upon his work with biometrics in e-health deployments to introduce practical challenges and considerations that could impact system interoperability. Hovsto stressed the importance of providing clear directions to users enrolling in systems. Varying directions for different systems, for example, could inhibit system interoperability and check system expansion. Hovsto also noted that certain biometrics, such as fingerprints, could wear down over time—another potential inhibitor of system interoperability and system expansion for systems that vary in sensitivity and frequency of updates.

Additionally, Hovsto raised concerns over the lack of auditing that contributes to uncertainty about whether biometric data are being deleted after use, as some data holders claim to do. System interoperability could increase the risk that any data accidentally left over would be inappropriately accessed. It could also introduce the challenge of ensur-

ing that data deleted from one database are also deleted from all interoperable databases.

Hovsto suggested that a “well-targeted promotion of standardization” would be “generally effective” at addressing many of the aforementioned concerns. He also argued for the use of biometric templates rather than images, while still advising against the use of “open” templates that could be “captured.” System interoperability could expand the potential impact of any such data capture.

Benjamin Schouten discussed the difference in perspective of users versus end users in his presentation, “User Empowerment in Biometrics.” Schouten noted that end users—who typically are the subjects of data collection efforts—often have different motivations and attitudes toward system interoperability than do users of data, who typically are involved in the collection and distribution of the data. Schouten argued that because end users can be negatively impacted by the collection and use of their data, they should be empowered to exercise control over their data. End users also tend to have a more stable attitude towards their data than, say, government users, who are affected by frequent changes in attitudes driven by political expediency.

For Schouten, government users should not mandate that data on end users be collected. Rather, government users should have the burden of demonstrating to their citizenry why they should participate in an interoperable system involving biometric or personal detection technologies. To do so, a user convenience case would have to be developed emphasizing the usefulness and necessity of system interoperability, the ease of using system interoperable technology, and the importance of trust in the service provider who uses the technology.

Schouten contended that each data use case or addition of a technology for system interoperability should be explicitly approved by data subjects. He also noted the importance of ensuring that the choice of technologies utilized (and, by extension, the degree to which they support system interoperability) should be proportional to actual needs. Schouten additionally argued for the development and use of revocable identifiers rather than core identities, a practice that would help limit the scope of potential damage if an element of an interoperable system were to be compromised.

Along with Lee, Schouten stressed the importance of quantifying and valuing identity information to help deter the inappropriate handling and

“Government users should demonstrate to their citizenry why they should participate in an interoperable system involving biometric or personal detection technologies.”

treatment of sensitive identity data. Scope creep, for example, would potentially be kept better in check if the cost of using identity information for purposes beyond the originally approved purpose were made more tangible. The value versus risk of centralizing and sharing data would also become clearer. To help value identity information, Schouten proposed either utilizing an independent assessor/certifier or empowering end users with the right to refuse participation in an identity-collecting program, letting the market decide at what point an end user would accept collection of their data.

Focus Group Discussion

Inspired by the issues raised in the presentations, focus group participants explored additional ethical

IBG Focus Group Participants

- Natasha Burns
University of Central Lancashire
- A. Mark Cutter
University of Central Lancashire
- Asbjorn Hovsto
ITS NO
- Katja Jacobsen
Centre for the Economic and Social Aspects of Genomics
- Victor Lee
International Biometric Group
- Sonia Massari
Centre for Science, Society and Citizenship
- Paul McCarthy
Centre for the Economic and Social Aspects of Genomics
- Emilio Mordini
Centre for Science, Society and Citizenship
- Nikola Pavesic
University of Lubljana
- Benjamin Schouten
Center of Mathematics and Computer Science
- Michael Thieme
International Biometric Group

challenges associated with system interoperability. One of these challenges involves the impact that attempting to achieve system interoperability on the basis of accepting minimal standards would have on individual rights. For example, system interoperability could result in the integration of systems that can only accommodate conventionally healthy individuals. But this could unfairly disadvantage disabled individuals who were able to interact

with their original systems, but not with less capable systems after the achievement of system interoperability through “least common denominator” approaches. Another key discussion was the issue of informed consent and user empowerment. Paul McCarthy warned about the challenge and difficulty of obtaining truly informed consent from individuals whose personal information is collected and stored in various databases. He mentioned the example of the UK Biobank, which requires blanket consent for future research use of participant’s genetic materials. A consent process that permits individuals to specify the type of research for which their DNA can be used (the ideal approach under a user empowerment model) was deemed impractical for the population-based research the UK Biobank supports. He also mentioned the challenge of placing consent-based restrictions on databases and enforcing them for derivative databases.

Exacerbating the problem of obtaining informed consent for the collection and use of personal information is the lack of trust in some service providers or government users. McCarthy noted that some end users simply do not trust their governments to protect their data adequately, particularly when data are shared via interoperable systems with governments that have weaker privacy protection policies. To help address the trust issue, Schouten proposed the utilization of trust providers who could act as intermediaries. For

instance, to allow for system interoperability through exchange of data between two entities without a preexisting trust relationship, Schouten proposed the use of third parties, with preexisting trust relationships with both entities, as arbiters and certifiers.

Emilio Mordini also raised concerns over the “convergence of technologies,” by which he meant the use of technologies that had a preexisting usage or capability in one area, but that could also be used for identification applications. He gave the example of ECG and EKG technology, which could be used both to generate distinct “biosignals” for identification purposes, as well as to reveal sensitive medical information about individuals. Hovsto mentioned that, through ISO/IEC JTC 1/SC 37, the International Organization for Standardization was actively looking into such questions of “multiple use technologies.”

Finally, Mordini discussed the “tripod concept” of the unity amongst law, ethics, and social issues. While weakening any of these three “legs” would impact the stability of the other two, a truly effective solution to the ethical issues revolving around system interoperability of biometrics and personal detection technologies would require addressing all three aspects. Throughout the term of the HIDE project, this focus group will continue to lead inquiries into solutions that can meet this standard.



FOCUS GROUP REPORT

Biometrics and Body Data in Embedded Systems and Ambient Intelligence

By Isolde Sprenkels, Zuyd University

One of the most influential developments in information and communication technologies will be the shift away from PC and desktop configurations to computing technologies located in the physical environment. This technological future includes embedded software, ubiquitous computing, ambient technology, smart objects, and the Internet of Things.

On October 31, 2008, HIDE Partner Zuyd University (Infonomics and New Media Research Center) held a focus group meeting to explore the social and ethical aspects of identification in embedded systems and ambient intelligence.

Focus Group Introduction

In the morning session, focus group leader Irma van der Ploeg introduced the topic of embedded systems and ambient intelligence. The focus group exploring ethical and social issues in relation to embedded technologies is one of the four technological areas of HIDE's Work Package 3 on Critical Issue Identification. Since only a limited number of embedded systems actually involve personal identification, the related and partly overlapping technological areas referred to as ambient intelligence, pervasive technology, ubiquitous computing, and the Internet of Things were also included. These technological areas all denote a view of a near future that will involve a shift away from PCs and desktop configurations to devices embedded in the physical environment. Essential to this devel-

opment are radio frequency identification (RFID), miniaturization, and wireless, sensor, and networking technologies that enable people to move through and interact with their environments in new ways. These technologies will also enable objects to interact, communicate, and send information about themselves, their users, or their environments to electronic networks and databases.

On one hand, these technologies offer end users huge gains in convenience, efficiency, and safety. On the other hand, they could lead to a loss of privacy because third parties can track the activities and trace the whereabouts of end users. The information generated on the behavior of people resulting from the collection and processing of personal data might form highly tempting resources for law enforcement, crime prevention, and security policy. Moreover, with their emphasis on unobtrusiveness, ease of use, efficiency, personalization, and convenience, embedded systems and ambient intelligence appear to be on a collision course with the requirement stipulated in the EU Data Protection Directive that data subjects should at all times be aware and informed of personal data collection (art. 7, par. 1).

After van der Ploeg's introductory

comments, Emilio Mordini gave a short presentation about the HIDE project, which was followed by two expert presentations.

Presentation Session

Dimitroz Tzovaras, coordinator of the project ACTIBIO (Unobtrusive

“ The information generated on people's behavior from embedded systems and ambient intelligence might form tempting resources for law enforcement, crime prevention, and security policy. ”

Authentication Using Activity Related and Soft Biometrics) at the Informatics and Telematics Institute in Thessaloniki, Greece, and Ruud van Munster, senior consultant for biometrics and surveillance at TNO Science and Industry in Delft, the Netherlands, informed focus group participants about the state of the art in biometric identification technologies applied in ambient intelligence and embedded contexts. Tzovaras described two projects funded by the European Commission (EC): ACTIBIO and HUMABIO (Human Monitoring and Authentication Using Biodynamic Indicators and Behavioural Analyses).

CONTINUES ON PAGE 8

Zuyd University Focus Group Participants

- Larry Busch
Centre for Economic and Social Aspects of Genomics
- Franck Dumortier
Centre de Recherches Informatique et Droit Namur
- Serge Gutwirth
Brussels University
- Katja Lindskov Jacobsen
Centre for the Economic and Social Aspects of Genomics
- Stacey Mannari
Centre for Science, Society and Citizenship
- Paul McCarthy
Centre for the Economic and Social Aspects of Genomics
- Emilio Mordini
Centre for Science, Society and Citizenship
- Geert Munnichs
Rathenau Institute
- Vlad Niculescu, *Zuyd University*
- Nikola Pavesic
University of Ljubljana
- Antoninette Rouvroy
Centre de Recherches Informatique et Droit Namur
- Rene von Schomberg
European Commission
- Isolde Sprenkels, *Zuyd University*
- Dimitrios Tzovaras
Informatics and Telematics Institute
- Irma van der Ploeg
Zuyd University
- Ruud van Munster, *TNO*
- Raymond Veldhuis
Twente University

HUMABIO (2006–2008) was designed to address issues that biometric solutions face, such as the limited use of multiple biometric modalities, the increased spoofing possibilities, and biometric template aging. Its aim was to develop multimodal biometric authentication and monitoring systems that utilize a biodynamic physiological profile (brain and heart activity as measured by EEG/ECG) and advancements in behavioral and other biometrics like facial, speech, and gait recognition and seat-based anthropometrics (the way a person sits on a seat and his or her body shape). The project introduced novel sensors aiming at the user’s conven-

ience and system unobtrusiveness and developed a security framework to guarantee trust and privacy concerning a person’s personal template and data.

Building on the results of HUMABIO, ACTIBIO (started March 2008) intends to increase technological performance and unobtrusiveness and enhance safety and security in controlled environments by introducing activity-related, multimodal biometrics combined with unobtrusive behavioral and “soft” biometrics, which focus on height, weight, and body structure. To do this, unobtrusive sensors for activity-related signals like the “sensing seat” are being utilized, and new application scenarios for unobtrusive authentication and monitoring are being designed.

Next, van Munster focused on TNO’s development of a new concept of airport security based on semiautomatic, automatic, and knowledge-based observation. He described three innovations: 1) the listening camera, which not only provides visual information but analyzes and classifies sounds as well; 2) the camera-as-a-team, which prevents the person under observation from disappearing by filming from different angles; and 3) integral observation, a new approach for airports that profiles passengers through monitoring. Different sensors are used to recognize special patterns in body features that indicate arousal (like perspiration and heart beat frequency), behavior (like motion analysis and trajectory analysis), and possession of objects and materials (like metal detectors and low energy X-ray) without people actively visiting observation stations. A person’s risk level increases when combined observations indicate a deviation in behavior or possession, and this person then becomes a candidate for closer examination. Thus, each solution in this system of airport security functions as a filter that supports the decision the observers have to make, with the aim of reducing the current checking of all passengers to the “2% that actually need it.”

These two presentations provided

key information about recent developments in biometric identification technologies and inspired the focus group participants to raise several topics discussed during the afternoon session.

Focal Issues and Roundtable Discussion

Prior to the focus group meeting, participants received a document containing an introduction to the topic, some discussion notes developed from a review of a number of recent key documents published by various European Commission bodies (see key reference documents at the link below), and some questions to discuss in the focus group meeting. In the afternoon session van der Ploeg introduced these focal issues and some important questions.

The key reference documents showed that in the European policy context, RFID and the Internet of Things dominate the regulatory and legislative discourse. To avoid revisiting this debate, van der Ploeg suggested that participants focus on a particular subset of the technical developments and applications within the broad area of embedded systems and ambient intelligence—namely, the identification, authentication, and monitoring of the human body using biometrics and/or other body sensing and scanning devices. Participants were invited to concentrate on identification of critical issues potentially arising from the use of biometrics (and other personal and/or identifying body data) in, or in combination with, the technologies subsumed under embedded systems, ambient intelligence, the Internet of Things, and RFID in particular, as well as applications of the latter that especially involve the human body.

Several questions in this context were identified: What type of applications and systems enable surreptitious identification, tracking, and tracing of individuals, and how? How should issues of transparency, consent, and democratic control be negotiated in such systems? What type of

CONTINUES ON PAGE 9

systems and applications targeting the human body give rise to which issues in particular, and why? What specific new vulnerabilities emerge from these systems, and whom do they threaten? During the vivid roundtable discussion, participants identified several issues and made recommendations for further consideration:

- Investigate the concept of privacy because it seems to evolve with technological development.
- Investigate the unobtrusiveness and convenience of these technologies because these characteristics in particular seem to be of moral and legal concern.
- Discuss the argument about the distinction between machine and human in monitoring and judging suspicious behavior: is a machine really more objective, reliable, and just in making such evaluations?
- Specify the particularities of the use contexts of these technologies.
- Devote attention to databases, data mining, and profiling.
- Think of issues concerning proportionality and (automated) discrimination, the link between body and data, bodily differences, and the implications of shifting from rule-based to risk-based approaches to security.

Zuyd's Infonomics and New Media Research Center will draw from participants' contributions to the focus group discussions to draft an ethical briefing paper that will be discussed, developed, and finalized in the course of the next focus group meetings. In addition, participants agreed to immediately and collectively work on a policy brief concerning the recent controversy involving the proposal by European Commissioner for Transport, Antonio Tajani, to introduce body-scanning technologies in European airports in 2010. The European Parliament has criticized the EC's support for this technology, doubting the justifiability, proportionality, and necessity of the measure, and has asked for prior assessment of the impact on privacy, data protection, and human dignity.

Background documents and the focus agenda are available at http://www.hideproject.org/events/fg-embedded_technology.html.

HIDE Past Events

- *9 September 2008*
Technology Convergence Focus Group, Paris, France
- *15 September 2008*
System Interoperability Focus Group, London, UK
- *31 October 2008*
Embedded Technology Focus Group, Maastricht, the Netherlands

HIDE Upcoming Events

- *6 February 2009*
Policy Forum on Outsourcing of Systems for Detection, Identification and Authentication, London, UK
- *3–4 March 2009*
Policy Forum on Body Issues, Brussels, Belgium
- *5–6 June 2009*
Policy Forum on Privacy as Contextual Integrity, Prague, Czech Republic
- *1–3 July 2009*
Problem Solving Workshop on Transatlantic and International Data Sharing and the APEC Privacy Framework, Singapore

For more details, visit www.hideproject.org.

Recent Publications

- Australian Law Reform Commission. *For Your Information: Australian Privacy Law and Practice*. ALRC Report 108. <http://www.austlii.edu.au/au/other/alrc/publications/reports/108/>
- Bennett CJ, Lyon D, eds. *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*. Routledge, 2008.
- Brown J. Pan, tilt, zoom: Regulating the use of video surveillance of public places. *Berkeley Technology Law Journal* 2008;23:755-781.
- Mordini E, ed. *Identity, Security and Democracy*. IOS Press, Nato Series, in press.
- Mordini E, Massari S. Body, biometrics and identity. *Bioethics* 2008;22(3):488-498.
- National Research Council. *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment*. National Academies Press, 2008. http://www.nap.edu/catalog.php?record_id=12452
- Solove DJ. *Understanding Privacy*. Harvard University Press, 2008.

PARTNER PROFILES

CENTRE FOR BIOMEDICAL ETHICS— YONG LOO LIN SCHOOL OF MEDICINE, NATIONAL UNIVERSITY OF SINGAPORE



The Centre for Biomedical Ethics, with a dedicated professor supported by a team of researchers, is South East Asia's first academic center for biomedical ethics in a medical school. It will promote interdisciplinary collaborations with other faculties

at NUS including law, science, arts, and social science, as well as with key stakeholders in Singapore's health care sector and the research community. The objectives of the Centre include initiating multidisciplinary research projects in biomedical ethics in collaboration with academics and professionals in the biomedical sciences and in clinical medicine; planning and implementing an integrated teaching program in medical ethics for NUS undergraduate medical students; fostering international research collaborations, linking with centers in Asia, the United States, Australasia, and Europe; collaborating with ethics governance and advisory bodies in Singapore, especially the Bioethics Advisory Committee; enhancing public understanding of ethical issues in biomedicine; promoting conferences and seminars in biomedical ethics at national, regional, and international levels; and focusing on ethical values in the Asian context.

UNIVERSITY OF LJUBLJANA— FACULTY OF ELECTRICAL ENGINEERING

University of Ljubljana
Faculty of *Electrical Engineering*



The University of Ljubljana has strong programs in the humanities, the scientific and engineering fields, medicine, dentistry, and veterinary medicine. Research work at the Faculty of Electrical Engineering operates in nine major fields, which are fully covered by 287 registered researchers and 31 technical collaborators working in 26 research groups. These fields are: electrical energy, electric

machines and power electronics, electronics, microelectronics, biocybernetics and biomedicine, measuring systems, automation and cybernetics, robotics, and telecommunications. In the Laboratory of Artificial Perception, Systems, and Cybernetics (LUKS), the main research is on biometrics-based recognition of people focused on integration of face, voice, signature, palm, digit print, and fingerprint recognition; and speech recognition, understanding, and synthesis, particularly the development of spoken dialogue systems for information services. LUKS pioneered biometrics research in Slovenia in 1975. Since then, it has participated in several international projects, including Copernicus Project COP 1634, CEEPUS Project HR-006, HP Initiative Project, COST Action 175 Biometrics-Based Recognition over the Internet, and several bilateral Slovenian-German, Slovenian-Portuguese, and Slovenian-Croatian projects.

HIDE Partners

Centre for Science, Society and Citizenship
Rome, Italy

Centre for the Economic and Social Aspects of Genomics
Lancaster and Cardiff, UK

Centre for Biomedical Ethics—Yong Loo Lin School of Medicine
Singapore

Eutelis Italia SRL
Rome, Italy

Fraunhofer Institute for Computer Graphics Research
Darmstadt, Germany

International Biometric Group
London, UK

Optel Ltd
Woclaw, Poland

Sagem Sécurité
Paris, France

The Hastings Center
Garrison, NY

University of Ljubljana
Ljubljana, Slovenia

Zuyd University
Heerlen, the Netherlands