



DIALOGUE

Volume 3 • No. 8 | 2010 March

FROM THE EDITOR

HIDE Roundup

IN THIS ISSUE

- 1 *From the Editor*
HIDE Roundup
- 3 *Focus Group Report*
System Interoperability of
Biometrics and Personal
Detection Technologies
- 6 *News and Notes*

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.

As the HIDE project enters the final phase of its 36-month life, this is a good time to provide an overview of HIDE partners' activities up to this point. Through focus groups, policy forums, and problem-solving workshops, the partners have created numerous opportunities for an ongoing international dialogue on ethical, privacy, and governance issues related to biometrics and personal detection technologies.

The focus groups have been structured around four themes: technology convergence, system interoperability, embedded technologies, and privacy-enhancing technologies. For each theme, two focus group meetings have been conducted. The third set of focus group meetings will take place this year: the privacy-enhancing focus group will meet in May; the system interoperability group will meet in June; the technology convergence group will meet in September; and the embedded technology group will meet in October (see meeting dates on p. 6). The focus groups are designed to monitor and explore each theme over the duration of the HIDE project and to encapsulate the focus group conversations in ethical briefs in a form comprehensible for policy-makers

and lay readers.

HIDE partners also held three policy forums: one on body issues, one on the outsourcing of biometrics and personal detection technologies, and

“To date, the HIDE project has shown that many ethical concerns about biometrics and personal detection technologies have yet to be resolved.”

one on privacy as contextual integrity. The policy forums provided an opportunity for participants to examine a wide range of general policy issues that cut across all technological fields and to reflect on and question basic assumptions and values involved in the public conversation on biometrics and personal detection technologies.

Finally, the HIDE project convened two problem-solving workshops: “International Data Sharing and Biometric Identification—The Ethical

CONTINUES ON PAGE 2



Issues in an Asian and International Context” and “Restrictions in the Implementation of EU Data Protection Directive for Public Interest, Security and Defense.” The workshops were designed to provide a safe environment to address questions that often are difficult to discuss in more formal or structured settings. A key feature of all of the HIDE meetings was the participation of experts and policy-makers from Europe, Asia, and the United States.

In addition to the focus groups, policy forums, and problem-solving workshops, HIDE partners have pro-

duced several reports and ethical briefs that delve more deeply into the ethical, privacy, and governance issues surrounding the use of biometrics and personal detection technologies. These documents reveal that many of the ethical concerns surrounding the collection, storage, and sharing of biometric and other personal data have yet to be resolved; that the public continues to worry about government access to and confidentiality of their personal data; and that policy-makers and data officials need to address many technical issues involving the development and

deployment of personal detection technologies. HIDE partners will continue to explore these issues for the duration of the project and to develop a platform for continued dialogue beyond the life of the project. Information about the previous and upcoming HIDE meetings, the names of meeting participants, the ethical briefs, the policy forum and workshop reports, and back issues of *Dialogue* can be found at <http://www.hideproject.org>.

—Karen J. Maschke
The Hastings Center



System Interoperability of Biometrics and Personal Detection Technologies

By Mary Collins, IBG

On 7 December 2009, International Biometric Group hosted the second meeting of the HIDE project Focus Group on System Interoperability of Biometrics and Personal Detection Technologies. Assembled experts and HIDE partners discussed several topics related to ethical considerations of system interoperability and biometrics.

Privacy and Surveillance: Dual Use and the SAMURAI Project

Caroline Wardle addressed several issues relevant to the HIDE project in her presentation about the SAMURAI initiative and issues related to dual use technologies. SAMURAI (Suspicious and Abnormal Behavior Monitoring Using a Network of CAMeras for SItuation Awareness Enhancement) is a project funded by the European Union under FP7 that seeks to leverage existing closed circuit television (CCTV) cameras all over the United Kingdom and develop additional mobile and sensor capabilities to facilitate intelligent surveillance at critical public sites. This means that rather than CCTV working alone to monitor suspicious and abnormal behavior in public places, networked heterogeneous sensors will be used with CCTV to “create a visualization of a more complete ‘big picture’ of a crowded public space” (<http://www.samurai-eu.org>).

Wardle raised several ethical considerations relevant to SAMURAI. Because all surveillance projects capture various types of personal infor-

mation, surveillance projects must consider privacy and data protection issues. In addition, surveillance projects raise complex issues about *dual use*—i.e., the idea that technology originally developed for civil applications may be appropriated for government or military uses. For instance, military funding in the United States is a primary driver for technological research, and thus, technologies developed for antiterrorism purposes are now finding broader applications in the commercial arena. When considering the ethical implications of dual uses of technology, then, the direction in which the development of technology moves becomes important. Focus group participants agreed that the movement of technology from military to civil applications is more ethically acceptable than when technology developed for civil applications is repurposed or appropriated for military use.

Although the European Union requires an ethical checklist to be completed for each project it funds, Wardle noted that very few projects, if any, indicated that dual use was an ethical concern. Why might this be? A key reason may be that many researchers are typically more concerned with advancing development of new technologies than with worry-

ing about their potential misuse. Thus, they may think that indicating their project might raise ethical concerns could create complications for the later use of the technology. It’s also possible that researchers may be reluctant to acknowledge that their

“As voice technology continues to develop, standards and legal frameworks must be updated to accommodate the technology’s unique aspects and how it impacts privacy.”

work has ethical implications for fear of not being funded. The focus group agreed that promoting ongoing discussion of ethical issues is important to increase awareness and inform legislation.

Voice Recognition and Biometric Vulnerabilities

Sapna Kapoor from AGNITIO, a company that provides voice biometric solutions for the public sector, provided several case studies and examples of recent uses of voice biometrics. Because the voice is the only biometric that can be collected remotely (i.e., through a telephone), it is relatively easy to integrate into existing telephone and voiceover-IP infrastructures.

CONTINUES ON PAGE 4

Focus Group Participants

- Strahinja Brajuškovic
The Anti-Trafficking Center
- Sapna Capoor
AGNITIO
- Mary Collins
IBG
- Katarzyna Cuadrat-Grzyvbowska
European Data Protection Supervisor
- Simon Dobrisesk
University of Ljubljana
- Catherine Edlin
SAMURAI Project
- Bénédicte Havelange
European Data Protection Supervisor
- Paul McCarthy
CESAGEN
- Philip Statham
CESG, Retired
- Michael Thieme
IBG
- Philip Tresadern
MOBIO Project
- Silvia Venier
CSSC
- Caroline Wardle
SAMURAI Project
- Xuebing Zhou
Fraunhofer IGD

Voice technology has followed the opposite trajectory of fingerprinting: it was first developed for commercial applications, but is now used in the forensic arena. Wardle asked about the issue of *scope creep*—the potential for AGNITIO's voice database, which is maintained by the Spanish police, to be exploited for commercial purposes. Capoor said there are pros and cons to any biometric deployment, and it is important for biometric solutions providers to establish the benefits of biometric systems to help justify potential risks taken on by users. As voice technology continues to develop and becomes more widely deployed, standards and legal frameworks must be updated to accommodate unique aspects of the technology and how it impacts privacy. Capoor briefly discussed relevant work in progress to develop a standard for voice models and a secure voice biometric template.

Simon Dobrisesk cautioned against relying purely on voice recognition in

court cases because error rates—especially those associated with short samples—are too high to justify convictions beyond a reasonable doubt. Capoor agreed and said that convictions should never be based purely on voice or any other biometric data, but rather on a combination of evidence. However, voice data are often enough to compel settlements, and it may be possible for law enforcement to use the technology effectively as a deterrent to criminal activity.

Wardle brought up the issue of spoofing, which involves a person or program that masquerades as another. There are many techniques which can be used to encrypt the voice stream or to change the quality of voices within recordings, such as adding or manipulating acoustical voice vectors. While voice may be easier to spoof than a modality with a more dynamic interaction, such as a fingerprint or iris scan, this should not undermine deployment of voice systems. Rather, extra care should be taken to carefully plan system protocols in advance of deployment to anticipate possible attacks or misuse of the technology.

Mobile Biometrics

In his presentation, Philip Tresadern discussed the MOBIO (Mobile Biometry) project and related privacy and ethical considerations. The MOBIO project is an FP7 program that investigates the use of biometrics for securing private data that can be accessed through mobile devices. Tresadern outlined several key project considerations related to privacy and data protection and grouped the concerns into two main categories: misuse of data and misuse of technology.

Misuse of data involves who has access to stored data, how the data are controlled, and whether data can be obtained without individuals' consent. If data are stored in a centralized database, measures must be in place to ensure that it is not transferred to a memory stick/CD/laptop that could be lost or used for unintended purposes. An alternative storage

approach is to store data on a mobile device, though this poses risks of data theft if the device is ever lost or stolen. Raw data are rarely retained, not only for privacy reasons but because, in most cases, not all data are useful and storage space is precious. An additional consideration is determining what data must be sent to the server. Transmitting biometric data allows the opportunity for interception and copying. However, conducting all processing directly on the mobile device and simply sending an accept/reject instruction to the server may open the door to hacking by mimicry.

Misuse of technology concerns the effect of using technology for other tasks to which the user did not consent. Because of the prevalence of security cameras, automatic identification in surveillance applications is a major concern. Face recognition on such a large scale raises serious issues with respect to false positives (i.e., wrongful accusation). The face modality presents unique ethical concerns because of the fact that faces can convey information such as gender, age, race, religion, and health. Additionally, there are a variety of ways in which signals from mobile phones can be used to track individuals. GPS technologies provide even more accurate means of pinpointing location. Tresadern stressed the importance of careful reading of any agreements that discuss what data phone companies may collect and distribute without consent.

Data Protection and System Interoperability

Bénédicte Havelange and Katarzyna Cuadrat-Grzyvbowska gave a joint presentation on their work at the European Data Protection Supervisor (EDPS) and relevant system interoperability and privacy considerations.

Data protection is considered of utmost importance in the European Union; it has been defined as a fundamental right and is a precondition for establishing mutual trust between authorities. Data protection protocols

are not only ethically relevant but actually help make systems more effective. They should not be considered an obstacle to deployment of new technologies.

Havelange and Cuadrat-Grzyvbowska outlined several key principles of data protection:

■ **Purpose limitation principle:**

Data collection must be justified by an explicit, clear, legitimate purpose.

■ **Proportionality principle:**

Superfluous data should not be collected; all data should be stored no longer than necessary.

■ **Data quality:** Accuracy and quality checks must be performed routinely to ensure that data are reliable and up to date.

■ **Transparency:** The data subject

“ Data protection protocols are ethically relevant, can make systems more effective, and should not be considered an obstacle to deploying new technologies. ”

must be informed of the purpose of collecting and using his or her data.

■ **Security:** Appropriate measures should be taken to prevent accidental or unauthorized access, alteration, dissemination, destruction, or loss of data.

■ **Data subjects' rights:** The right of data subjects to have access (directly or indirectly) to their data and the ability to rectify or erase their data must be considered; such rights can actually increase the quality of data in the systems.

System interoperability can help avoid the risks associated with double storage—the fewer copies of sensitive information that exist, the better. However, it also increases risk of function creep and merging of databases with different purposes. Michael Thieme noted that standards are built to facilitate openness, but this could be seen as a potential drawback if one opposes system

interoperability because of the potential risks associated with it.

Havelange again advocated the need for case-by-case assessments, taking into consideration the data protection principles of necessity, proportionality, and purpose limitation. Open democratic debate should lead to clear and careful policy choices. Cuadrat-Grzyvbowska noted there is sometimes a disconnection between practical application and the legal process.

Biometric Standards: Security, Usability, and Privacy

Philip Statham's presentation focused on biometrics standards relating to security, usability, and privacy. He discussed work done by subcommittees ISO/IEC JTC1 37 on

Biometrics and ISO/IEC JTC1 27 on IT Security Techniques and also provided links to several current reports and standards drafts. ISO recently created a new Privacy Steering Committee

to lead new standards work on privacy. Statham also addressed the notion of renewable biometric references, a claimed solution to some common privacy concerns about biometrics. The key feature is anonymization of biometric data through translation to a renewable password. Such technology may not be suitable for 1:N applications, however, and more testing is needed to determine performance and error rates.

With biometrics, there is a trade-off between False Accept Rate (FAR) and False Reject Rate (FRR). A low FAR is correlated with increased security, whereas a low FRR is correlated with increased usability. With passwords, length and randomness (entropy) are security factors and represent the same trade-off between security and usability. With tokens, technical design and manufacture are security factors but do not have any bearing on usability. All authentication meth-

ods have potential security weaknesses. Biometrics may be subject to spoofing, capture and replay, and database attacks. Passwords may be easy to guess or difficult to remember. Tokens can be lost or stolen. Both passwords and tokens are easily shared and subject to software and hardware attacks, respectively. Multifactor authentication offers the potential to optimize the trade-off between security and usability. The strength of one factor may be able to compensate for the vulnerability of another.

Usability is a concern for all human/system interactions, and problems associated with biometric systems may not have anything to do with the biometric. The main challenge associated with deployment of iris systems in U.K. airports, for example, was finding an optimal height for the sensor. The U.S. National Institute of Standards and Technology (NIST) has defined several usability criteria for biometrics, including success rates (effectiveness), time on task (efficiency), time to learn a task (learnability), number of errors made over time (memorability), and user satisfaction level (satisfaction).

Because of different values across cultures, it is difficult to establish a global definition for privacy or security. While standards will define common concepts, it will be left to countries to create their own policies and determine compliance. The professional standards community was quick to define many terms and requirements relevant to interoperability but is now slower when it comes to issues of usability, security, and privacy. This gives work like the HIDE project particular meaning and the potential to make a significant impact on the future landscape of system interoperability and biometrics.

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, USA

University of Ljubljana
Ljubljana, Slovenia

Zuyd University
Heerlen, the Netherlands

HIDE Upcoming Events

- **14 May 2010**
Focus Group Meeting on Privacy Enhancing Technologies, Manchester, UK
- **21 June 2010**
Focus Group Meeting on System Interoperability, London, UK
- **14 September 2010**
Focus Group Meeting on Technology Convergence, Paris, France
- **8 October 2010**
Focus Group Meeting on Embedded Technology, Maastricht, the Netherlands

Other Upcoming Events

- **June 7–9, 2010**
2010 IEEE International Symposium on Technology and Society (ISTAS '10) "Social Implications of Emerging Technologies," Wollongong, New South Wales, Australia
ISTAS '10 will be held at the Novotel Northbeach near the University of Wollongong
<http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=05246992>

Recent Publications

- Browne S. Digital epidermalization: Race, identity and biometrics. *Critical Sociology* 2010;36(1):131-150.
- European Commission. Consultation on the future European Union – United States of America international agreement on personal data protection and information sharing for law enforcement purposes.
http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0005_en.htm
- Liptak A. When American and European ideas of privacy collide. *New York Times*. 26 February 2010.
<http://www.nytimes.com/2010/02/28/weekinreview/28liptak.html>
- Mayer-Schönberger V. Review of Newman, AL. *Protectors of Privacy: Regulating Personal Data in the Global Economy*. Ithaca, NY: Cornell University Press, 2008.
<http://www.surveillance-and-society.org/ojs/index.php/journal/article/viewFile/mayer-sch%C3%B6nberger/mayer-sch%C3%B6nberger>
- Robinson N, Potoglou D, Kim CW, et al. *Security, At What Cost? Quantifying People's Trade-Offs Across Liberty, Privacy and Security*. RAND Europe Board of Trustees, 2010.
http://www.rand.org/pubs/technical_reports/TR664/
- Shaikh SA, Rabaiotti JR. Characteristic trade-offs in designing large-scale biometric-based identity management systems. *Journal of Network and Computer Applications*. 2010 (in press).
- Wright D, Gutwirth S, Friedewald M, et al. Privacy, trust and policy-making: Challenges and responses, *Computer Law & Security Report* 2009;25(1):69-83.