



DIALOGUE

Volume 1 • No. 1 | 2008 July

EDITOR'S INTRODUCTION

Welcome to *Dialogue*

IN THIS ISSUE

- 1 *Editor's Introduction*
Welcome to Dialogue
- 2 *News and Notes*
- 3 *Feature Article*
Privacy Enhancing Technologies
- 5 *At a Glance*
MarketTrends for Biometric Systems; The European Commission's Biometric-Related Projects; Biometric Technologies: The View from Poland
- 8 *Partner Profiles*
CSSC and Sagem Sécurité

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, *Associate for Ethics & Science Policy*

ART DIRECTOR
Nora Porter

MANAGING EDITOR
Joyce Griffin

CONSULTING EDITOR
Gregory Kaebnick

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



With this issue of *Dialogue*, The Hastings Center launches the first of 10 newsletters from HIDE—Homeland Security, Biometric Identification and Personal Detection Ethics, a 36-month project funded by the European Commission. HIDE is coordinated by the Center for Science, Society and Citizenship (CSSC), an independent research center in Rome, Italy. The project includes 10 other partners from academia, industry, and public and private research centers in Europe, Singapore, and the United States.

HIDE's goal is to develop and support European and international conversation on the ethics and governance of personal detection and biometric technologies. Detection technologies are technologies used to detect something or someone in a security or safety context. Personal detection technologies focus on individuals. These technologies include closed circuit television (CCTV), infrared detectors and thermal imaging, global positioning systems (GPS) and other geographical information systems (GIS), radio frequency identification (RFID), microelectromechanical systems (MEMS), smart ID cards, transponders, and body scanners. Biometrics are the application of technologies that make use of a measurable, physical characteristic or personal behavioral trait to recognize the iden-

tity—or verify the claimed identity—of a previously registered individual. Standard biometric technologies use characteristics such as fingerprints, hand geometry, facial and voice recognition, iris and retinal scans, signature and keystroke dynamics, vein patterns, facial thermography, gait, and hand grip recognition. New biometric technologies include electro-physiological signal recognition

“HIDE's strategy is to test new ideas and reframe issues around Privacy, Sensitive Body Issues, and Identity Management.”

(based on ways of monitoring body cavities using electrodes, such as electrocardiogram and electroencephalogram), speech analytics, and emotion detection.

In a 2006 report, the Commission of the European Communities noted that while personal detection and biometric technologies can serve the security of nations' citizens, they are “inherently intrusive into privacy.”¹ Moreover, other values such as human dignity, individual self-deter-

CONTINUES ON PAGE 2

mination, anonymity, nondiscrimination, and justice are challenged by technology for personal detection, authentication, and identification. Thus, because personal detection and biometric technologies provide "the means of developing surveillance, and surveillance on an unprecedented scale"² their use "needs to be carefully analyzed, in order to establish limitations to their intrusiveness where necessary."³

HIDE will address these issues by promoting international discussion in a structured environment that focuses on shared values rather than on immediate political outcomes. One of the goals of the project will be to reframe the issues and probe more comprehensively into approaches for assessing the use of personal detection and biometric technologies. For instance, framing privacy and other issues through the lens of individual liberty may result in a different assessment of these technologies than framing the issues in terms of national security. Through the use of focus groups, policy forums, a stakeholder meeting, and this newsletter, HIDE will develop a strategy for testing new ideas and reframing issues from three perspectives: Privacy as Contextual Integrity; Sensitive Body Issues (gender, ethnicity, disability, and age); and Blurring the Public-Private Distinction in Identity Management.

The Hastings Center is proud to be a HIDE partner and the publisher of *Dialogue*. Each issue will contain news about the development and use of personal detection and biometric technologies; short commentaries, essays, or articles about the activities of HIDE partners and the ethical and privacy aspects of these technologies; and links to relevant resources. *Dialogue* will also include short profiles of each partner. In this issue we feature CSSC, the project coordinator, and Sagem Defense Sécurité (SAGEM).

We look forward to working with our HIDE partners and other stakeholders in creating a successful dialogue to promote innovative policy solutions to emerging ethical, social, and legal problems involving surveillance technologies. We encourage you to invite others to read *Dialogue* and to visit the HIDE website for additional information about the project's activities (<http://www.hideproject.org/>).

—Karen J. Maschke

Associate for Ethics & Science Policy, The Hastings Center

—Thomas H. Murray

President and CEO, The Hastings Center

1. Commission of the European Communities, Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and Other Security Authorities, Brussels, 1.9.2006 COM(2006) 474 final, p. 4.

2. Article 29, Data Protection Working Part, Opinion 1/2007 on the Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and other Security Authorities, Brussels, 00039/07/EN WP129, January 9, 2007, p. 3/8.

3. Commission of the European Communities, Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and Other Security Authorities, Brussels, 1.9.2006 COM(2006) 474 final, p. 4.

HIDE 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, Netherlands

Recent Publications

- March 2008. Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulations (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents by Member States. http://www.edps.europa.eu/EDPSWEB/webdav/shared/Document/s/Consultation/Opinions/2008/08-03-26_Biometrics_passports_EN.pdf
- February, 2008. Québec.Commission De L'Éthique De La Science Et De La Technologie, Position Statement, In Search of Balance: An Ethical Look at New Surveillance and Monitoring Technologies for Security Purposes. <http://www.ethique.gouv.qc.ca/In-Search-of-Balance-An-Ethical.html>
- 2008. Eurobarometer Survey Reveals that EU Citizens are Not Yet Fully Aware of Their Rights on Data Protection. <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/08/249&format=HTML&aged=0&language=EN&guiLanguage=en>
- 2007. European Commission. Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs). http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=3403
- 2007. U.S. Government Accountability Office. Homeland Security: Prospects for Biometric US-VISIT Exit Capability Remain Unclear. <http://www.gao.gov/new.items/d071044t.pdf>
- 2007. Article 29 Data Protection Working Party. Opinion 1/2007 on the Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and other Security Authorities. http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm



Privacy Enhancing Technologies

By Paul McCarthy and Katja Lindskov Jacobsen, *Cesagen*

On May 30, 2008, HIDE partner Cesagen (Centre for the Economic and Social Aspects of Genomics) held the first of three focus group workshops on Privacy Enhancing Technologies (PETs). These technologies are designed to protect sensitive personal data within information systems. PETs include data encryption; logical access control; user authentication and authorization; routers, cookies, and file management tools to anonymize data; and privacy rights management.

The focus group was framed by three objectives the European Commission (EC) established in May, 2007 in its Communication on PETs: 1) support the development of PETs, 2) encourage the use of PETs by data controllers, and 3) encourage the use of PETs by consumers. An additional aim of the focus group was to start discussions on the key issues that Cesagen needs to address and include in its final HIDE project report. Thus, the discussion regarding the potential ethical and social impacts of PETs was framed by the issues of autonomy, privacy and social justice.

The morning focus group session involved a traditional speaker/presentation/question format where the aim was to provide sufficient information on the background and context of PETs and the social and ethical issues involved. The speakers were Michiel van der Veen, Jonathan Bamford, Juliet Lodge, and Niovi Ringou. Ruth Chadwick moderated a discussion with all participants in the afternoon session.

Key Themes at Presentation Session

In his presentation, “The Dilemma of Biometrics: Privacy or Identity?” Michiel van der Veen used the case of BAA (the owner of Heathrow Airport) deciding to suspend its plans to use fingerprint biometrics in Heathrow Terminal 5 to point out the discrepancy between the perceived advantages that biometrics are thought to deliver—for example, enhanced security such as more accurate identification in airports on the one hand and the perceived disadvantages (privacy threats) on the other. He went on to describe what technology experts can do to resolve this dilemma by developing technology solutions that can deliver both “enhanced biometric security” and “privacy enhancing biometrics.” van der Veen presented an example of a specific PET such as priv-ID that Philips (Royal Philips Electronics of the Netherlands) is developing. This technology enhances privacy by protecting the biometric data subject—i.e., the person from whom the data is being obtained—against the threat of function creep (linking discrete biometric databases). Priv-ID is a one-way encryption function that translates a biometric representation into an anonymous number that can be thrown away (without throwing away the person's entire identity) and renewed (a new anonymous number

can be created), thus protecting the individual against the risk of biometric identity theft. Moreover, priv-ID protects the privacy of the individual by providing a safeguard against the threat of function creep as the technology allows the creation of different anonymous numbers for different applications (making it technically more difficult to link databases).

Jonathan Bamford's perspective on PETs explored a different dilemma

“How do PETs interact with existing data protection legislation? What are the ethical ramifications of PETs in relation to autonomy, privacy, and social justice?”

than the one outlined by van der Veen. For Bamford the question is how PETs can possibly serve to close the gap between the limitations of data protection laws and the emerging proliferation of data collecting biometric systems. He described steps the UK Information Commissioner is taking to promote data protection compliance by designing information systems that incorporate PETs. This approach differs from van der Veen's because it focuses on privacy as an issue of system design, rather than a technology to be added on to existing systems. Thus, Bamford posed a different set of privacy questions: Why does personal data need to be collected in the first place? Why does it need to be retained for long periods of time? Why is there a need to use

CONTINUES ON PAGE 4

the same templates in different applications? He urged us not to forget or neglect these questions in our discussion of PETs.

Introducing yet another approach to the issue, Juliet Lodge focused on a range of political implications that arise from the use of PETs. She asked whether PETs may in fact produce an inclusion/exclusion divide between individuals who have access to these technology solutions and those who do not. In other words, there is a risk that PETs may only enhance the privacy of specific groups of people. Another issue she raised is the governmental context, i.e., the way in which the interest in an ever-increasing use of biometrics ties in with a government's interest in managing the flow of people. The risk is that a narrow debate on PETs might neglect this important political dimension.

Focus Group Participants

- Jonathan Bamford, *Assistant Commissioner & Director of Data Protection Development, UK Office of the Information Commissioner*
- Prof. Ruth Chadwick, *Centre for the Economic and Social Aspects of Genomics*
- Prof. Lucas Introna, *Lancaster University*
- Katja Jacobsen, *Centre for the Economic and Social Aspects of Genomics*
- Prof. Juliet Lodge, *University of Leeds*
- Sonia Massari, *Centre for Science, Society and Citizenship*
- Dr. Paul McCarthy, *Centre for the Economic and Social Aspects of Genomics*
- Prof. Emilio Mordini, *Centre for Science, Society and Citizenship*
- Niovi Ringou, *European Commission, Deputy Head, Media and Data Protection*
- Dr. Antoinette Rouvroy, *Information Technology & Law Centre/Centre de Recherche Informatique et Droit*
- Michael Thieme, *International Biometric Group*
- Dr. Richard Tutton, *Centre for the Economic and Social Aspects of Genomics*
- Dr. Richard Twine, *Centre for the Economic and Social Aspects of Genomics*
- Prof. Irma van der Ploeg, *Zuyd University*
- Michiel van der Veen, *Philips, General Manager priv-ID Biometrics*
- Dr. Maria Veloso, *Centre for Biomedical Law*
- Dr. Steve Wright, *Leeds Metropolitan University*

Finally, Niovi Ringou stressed the importance of the EC's 2007 Communication on PETs but added that this is not the first time the EC addressed the issue of PETs, pointing out the relevance of Article 17 of the Data Protection Directive which specifies the data controller's obligation to implement appropriate technical and organizational measures and to ensure a level of security appropriate to the nature of the data. She defined three different EC interests in relation to the issue of PETs: the evolution of technologies and detecting emergent dangers associated with these technologies; the use of available PETs and their economic benefits; and encouragement of consumer use of PETs. Ringou linked the EC's interest in promoting PETs to the results of a recent survey which demonstrated that most EU citizens feel uneasy when transmitting personal information over the Internet. From the EC's point of view, it is hoped that PETs will play an important role in overcoming these concerns.

Focus Group Discussion

Prior to the meeting, focus group participants received a primer outlining the EC's objectives regarding PETs and grouping the ethical and social issues of PETs under three headings: autonomy, privacy, and social justice. Linked to these headings were a number of discussion points: How can PETs be defined? How do PETs interact with existing data protection legislation? What are the ethical ramifications of PETs in relation to autonomy, privacy, and social justice? The discussion highlighted the extent to which attempting to reach a definition of PETs was a challenging task to undertake due to the difficulty of defining what type of privacy would be enhanced. Some participants noted that the idea of developing PETs itself might be problematic as it could suggest that privacy was something which needed additional technological solutions to protect data, rather than companies, states, or other organizations seeking to min-

imise their data collection activities.

Concerns were also raised about how to define autonomy and about the curtailment of PETs when national security issues arise. Participants thought that the difference between notions of thick and thin autonomy was important because there is probably wide variability in the extent to which consumers easily understand complex data protection technologies. This point has important social justice implications because it raises the question whether everyone will have access to PETs. Discussants also noted that the inherent unpredictability of control built into complex automated systems of data collection might also forestall effective consumer use of PETs in the face of a bewildering array of biometric technologies. In addition, concerns were raised about definitions of privacy that are static or inflexible. In this sense privacy is seen as negotiated space where fixed notions emphasized by rigid technological solutions might not be appropriate. Examples include usage patterns of Internet social networking sites, where users may have a friends-list where much more information is provided than might be deemed safe.

The final phase of the discussion group returned to the issue of defining PETs. Michael Thieme suggested that there are three potential categories by which PETs might be differentiated: privacy by design, biometric encryption, and "plugged into your computer." Discussants suggested that these categories are useful starting points because they synthesize various approaches as well as technological forms of PETs that are in development.

The first focus group illustrated the scope of the issues Cesagen will address during the HIDE project. Several discussion points require further exploration, including disagreements about how to define PETs, privacy, and autonomy.



Market Trends for Biometric Systems

By Valerio Cusimano, *Eutelis Italia SRL*

Since the tragic events of September 11, 2001, national security officials have increasingly focused on the use of biometric systems to control access to public and private areas that may be targets for terrorist attacks. These locations include airports, banks, public offices, parks, and tourist attractions, as well as private offices of large national and multinational corporations. However, biometrics systems can also be used effectively on a smaller scale, and changing the industry's emphasis to reflect this will provide the foundation for its substantial and sustainable economic growth.

By definition, biometric systems are measurements of an individual's particular physical or biological character-

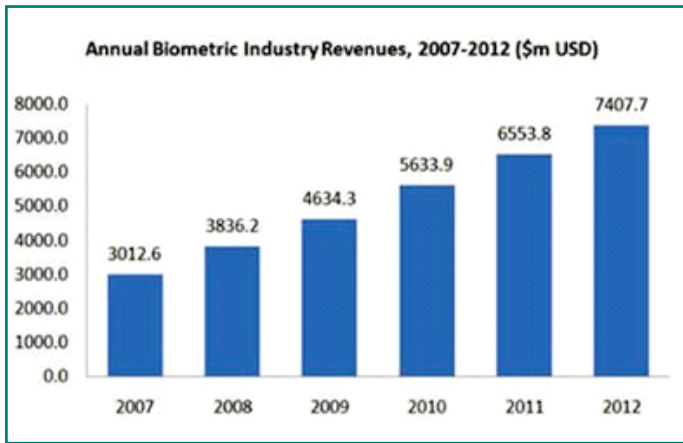


Figure 1.

istics, creating a unique identifier that can be electronically stored, retrieved, and compared for positive identification purposes. Devices such as fingerprint scanners are biometric systems, as are facial, iris, voice recognition, and hand geometry technologies. The market for these products is undergoing a sea change as companies move from developing the technology to utilizing it for real world security purposes. Making these systems convenient to adopt and use is the key to future market growth. According to the International Biometric Group, the worldwide biometric identification market has already increased from US\$1.2 billion in 2004 to US\$4.6 billion next year, and will continue to grow to approximately US\$5.7 billion in 2010, with a compound annual growth rate of 40% (Figure 1).

These overall figures represent expansion in several sectors of the market. Fingerprint identification systems will comprise 44% of the total market by 2009, making this the most popular kind of biometric technology available. According to the market research firm Frost & Sullivan, the demand for fingerprint sensors could grow by an astounding factor of 100, from US\$41 million in revenue on 4.3 million units sold in 2004 to US\$1.8 billion in revenue on 545 million units sold in 2011. The market for fin-

gerprint readers is also expected to grow with a compound annual growth rate of 35.3% from US\$344 million in 2004 to US\$1.56 billion in 2009 (See Figure 2). But fingerprint identification technology is not the only market sector that is flourishing. The use of positioned facial and iris recognition technology is on the rise, and multibiometric systems—which combine different kinds of identification methods in the same device, or “biometric terminal”—are expected to emerge as a force in the market in the next few years.

The impact of these technologies is becoming more diffuse. Technology that was once affordable only for large corporations and government entities is now available to individuals in a number of ways. For example, the automated fingerprint identification system (AFIS) is a system of computerized fingerprint records originally developed by the U.S. Federal Bureau of Investigation to electronically store fingerprints of criminal suspects and convicted offenders. But today, computerized fingerprint systems like AFIS are used for many purposes: to control physical access to places and buildings; to protect computer network terminals and portable storage devices such as laptops, personal digital assistants (PDAs), smart phones, USB keys, and portable hard disk drives; and to enable the collection of information such as personnel, inventory, and product quality data within a company. Incorporating fingerprint systems into these activities was made possible by the development in the last few years of sensor fingerprint technologies that can be embedded in notebook computers and mobile devices such as PDAs and smart phones. Many models of these devices now take advantage of this technology. Notebook computers with biometric sensors went from 10% of the total market in 2005 to 15% in 2006, and their number is estimated to multiply by a factor of 15 by 2011, for a total of 228 million notebooks with biometric sensors for sale. This growth is enabled by

CONTINUES ON PAGE 6

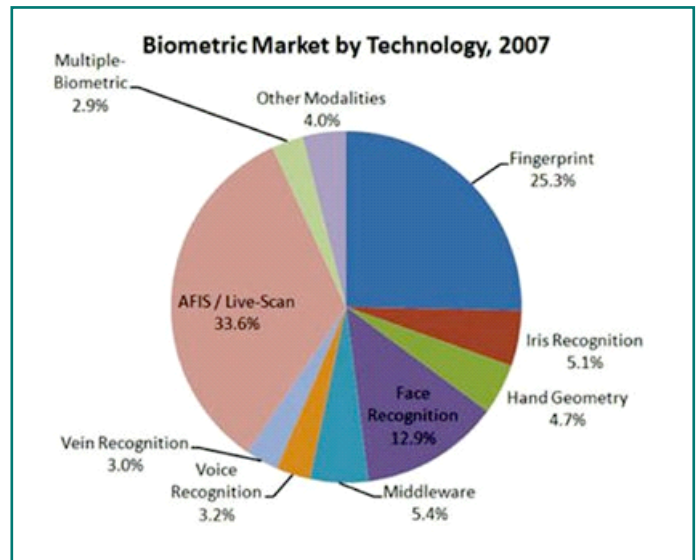


Figure 2.

the falling cost of manufacturing fingerprint sensors as part of portable information devices. The additional cost for doing so was around US\$50 in 2005, but today, the price is less than US\$5.

Vendors must shift their thinking to reflect these trends. Focusing on complex technological solutions and high security requirements worked in a highly specialized market, but this view is no longer appropriate and can only hamper progress. The biometric market’s future lies in applications that are convenient and cheap for mainstream consumers.

The European Commission’s Biometric-Related Projects

By Valerio Cusimano, *Eutelis Italia SRL*

In recent years the European Community has tried to improve its methods and systems for ensuring the safety of its citizens in the face of terrorist and other security threats. One approach to accomplishing this goal is the European Commission’s Preparatory Action on Security Research (PASR), which has funded several projects that are of interest to HIDE partners (see Table 1). The missions of these projects included:

- protecting networked systems,
- protecting against terrorism (including bioterrorism and incidents with biological, chemical, and other substances),
- enhancing crisis management,
- promoting interoperability and integrated systems, and
- improving situation awareness.

One important project was the Integrated Surveillance

of Crowded Areas for Public Security, or ISCAPS. This was a two-year project whose aim was to promote technological surveillance research. ISCAPS activities included researching threatening scenarios and operational requirements, utilizing key technologies (sensors, information processing and threat detection, communications, system configuration, and security), designing open system architecture, integrating components, and validating and demonstrating the results. ISCAPS employed a combination of sensors—visible camera, infrared camera, biometrics, and tags—to increase the quality of identification and tracking of persons, goods, and vehicles.

Another technology research project was People Real-Time Observation in Buildings: Assessment of New Technologies in Support of Surveillance and Intervention Operations, or PROBANT. This project was designed to focus on the development, integration, and validation of technologies, enabling operators in crisis intervention and surveillance situations to observe individuals located inside buildings and trace them in real time. Its aim was to improve the capability of security officers—police officers in particular—to visualize, locate, and identify human beings hidden behind walls and to follow their movements. Measurements of biometric values were incorporated into surveillance technologies to help determine if observed individuals are alive, nervous, sleeping, etc. The surveillance systems were also designed to allow for sophisticated data analysis techniques and remote control. The technologies validated by PROBANT serve to guard against terrorism by detecting and identifying threats in cases like kidnapping and hijacking where hostages are at stake. They allow law enforcement and other security officers to gather the information necessary to plan and exe-

Table 1. The European Commission’s PASR Projects at a Glance

<i>Project</i>	<i>Date</i>	<i>Aims</i>
ISCAPS	2005-2007	<ul style="list-style-type: none"> • To reinforce security for European citizens • To downsize the terrorist threat by reducing the risk of malicious events
PROBANT	2006-2008	<ul style="list-style-type: none"> • To improve the quality of information derived from raw data • To improve user-interface features, allowing operators to rapidly understand images and make decisions with confidence • To provide more reliable techniques for using biometric data to profile and label moving people and to establish if a hidden person is alive
ESSTRT	2004-2006	<ul style="list-style-type: none"> • To identify key security technologies that should be developed • To determine how new technologies can improve security • To determine the potential for combining these with nontechnological means to confront threats • To outline net cost and benefit estimates of using various technologies
STRABORSEC	2004-2006	<ul style="list-style-type: none"> • To consolidate the list of technologies identified for border security • To determine interoperability and standardization needs associated with these technologies • To inventory existing specification standards and associated assessment standards when in place • To identify what assessment standards are missing for existing specification standards • To identify what standards and assessments must be developed, including descriptions of scope and business justification for each • To propose priorities and a time frame for the implementation of these standards

cute a safe and effective rescue operation. These technologies may also be used—in accordance with national laws on penal procedure—in investigative operations related to terrorist networks.

Enhancing European border security requires not only an understanding of the terrorist and weapon threats to Europe and the unstable situations that produce them, but also a better interoperability of technologies deployed at Europe's borders. For this purpose, the European Security: High Level Study on Threats, Responses and Relevant Technologies, or ESSTRT, project aimed to analyze the characteristics of different targets in order to understand any particular vulnerabilities.

Another way to enhance border security is to enhance the standards of biometric technologies using information gathered by the border security group of the European Security Research Advisory Board and other European research projects. This work was the mission of the Standards for Border Security Enhancement, or STABORSEC project, which aimed to identify and assess standards—including mechanisms for conformity and evaluation—to guarantee effective interoperability of border security technology. STABORSEC produced a detailed, prioritized inventory of the standardization efforts that must be deployed to cover interoperability needs.

All the work accomplished by these projects has been very important for security purposes. However, the ethical aspects of these security systems and technologies have not been fully explored. The HIDE project recognizes that new surveillance technologies require attention to ethical and privacy concerns that cannot be addressed in the context of a particular technology. Rather, these concerns must be framed by a broad, comprehensive perspective that takes into consideration the social impact of these technologies and the opportunities to minimize their undesirable consequences for individuals and society.

Biometric Technologies: The View from Poland

By **Agnieszka Bicz and Wieslaw Bicz, Optel Ltd**

As is the case in other east European countries, the scale of the development and use of biometric technologies in Poland is relatively limited. There are a few domestic firms—not much more than ten—that are selling and installing biometric devices. These firms mostly cater to larger companies, hospitals, factories, banks, or governmental offices, and the devices they sell are manufactured outside of Poland by large international companies.

However, one new biometric technology was developed in Poland: finger recognition with ultrasound. Optel has developed a holographic camera which visualizes fingers that has a device that collects acoustic waves scattered by the finger. This technology is considered by many specialists as most promising from the point of robustness, liveness recognition, and achievable resolution.

Poland adopted biometric passports in 2006. A biometric chip encodes the personal information obtained from a paper document as well as facial mapping information

directly onto a page in the Polish passport. The introduction of the biometric passport is the only significant biometric action of the Polish government since the introduction in 2001 of the Automatic Fingerprint Identification System (AFIS) for law enforcement purposes. However, it is expected that when the European Union (EU) fully implements biometric border checks (expected to be operational by 2015), the government's next biometric action will be to install biometric devices on its borders with Russia, Belarus, and Ukraine, as well as at international airports and harbors. It can also be assumed that in response to new developments in biometric technologies and EU requirements, Polish government agencies, police, and other institutions will increasingly adopt biometric technologies for a variety of purposes.

There are two scientific institutions in Poland that play a significant role in the development of biometric technologies:

- The Department of Identification Systems and Laser Devices of The Institute of Mathematical Machines (IMM) in Warsaw not only works on biometrics, but also develops access control devices based on finger recognition modules (from Sony), organizes scientific conferences, and publishes papers and books about biometrics.
- NASK Biometric Laboratories was established with the cooperation of the Institute of Control and Computation Engineering at the Warsaw University of Technology. NASK investigates novel biometric identification techniques, develops biometric systems, and integrates them with existing security setups.

Many other universities or scientific institutes have some people who are working on biometric projects or are interested in activities in this area. Some colleges have included courses or lectures about biometrics in their curricula. The scientists working on biometrics in Poland are trying to develop novel biometric recognition methods or to improve existing ones. However, due to the lack of financing and absence of domestic companies with a strong commercial background in biometrics, these activities have only a small chance of bringing significant results. Nonetheless, these institutions have published several articles about their work in international scientific journals. In addition, one book about biometrics has been published in Poland (*Krzysztof Slot, Wybrane zagadnienia biometrii*, ISBN: 978-83-206-1673-6, WKŁ), and another book originally written in English was translated into Polish (*Biometria—originally Guide to Biometrics—by Ruud M. Bolle, Jonathan H. Connel, Sarath Pankanti, Nalini K. Ratha, and Andrew W. Senior*). Finally, a few conference proceedings and collections of smaller papers about biometrics were published by the IMM and other institutions. Whether the public is interested in biometrics is difficult to gauge since there has so far been no public discussion about the social or ethical aspects of biometric technologies.

PARTNER PROFILES

CENTRE FOR SCIENCE, SOCIETY, AND CITIZENSHIP



Founded in 2002, CSSC is a non-partisan research organization registered as a private research center by the Italian Ministry of University and Research. The Centre's mission is to attempt to clarify the human (social, cultural, and ethical) factors which shape techno-

logical innovation. It focuses on bringing science policies closer to citizens by promoting public awareness of science, technology, and innovation and by encouraging open dialogue among citizens and the main actors in the field. The Centre places particular importance on the ethical dimensions of new and emerging technologies and to challenges posed by the political and ethical tension between individual liberty and the common good. By taking an interdisciplinary approach, CSSC has explored the social, cultural and ethical implications of emerging technologies in biomedicine; disaster prevention and first response; homeland security; and eInclusion, a European Union project that was designed to contribute to the development of evidence-based electronic inclusion and accessibility policies at the EU and Member State levels. Conferences the Centre has organized include Ethical Implications of Scientific Research on Bioweapons and Prevention of Bioterrorism (European Commission, 2004); Ethical and Social Implications of Biometric Identification Technology (European Commission, 2005); Ethical, Social and Policy Implications of New Epidemics (European Commission, 2006); and Identity, Security and Democracy (NATO Advanced Research Workshop, 2006). CSSC's track record of researching, partnering and networking has made it a leading European institution in the area of science and society.

SAGEM SÉCURITÉ



Sagem Sécurité is the world leader in biometric technologies and in a wide range of other products, including Point-of-Sales terminals, smart cards, cryptography, unmanned aerial vehicles (UAVs), Control and Command rooms, and night vision cameras. The company is a 100% subsidiary of Safran, an international high-technology group with four core businesses: aerospace propulsion, defense and security, aerospace equipment, and communications. Safran has 56,000 employees in over 30 countries with annual revenues exceeding €11 billion. The Safran group comprises a number of companies with prestigious brand names and holds alone or in partnership global or European leadership positions in all of its markets. In 2006, Sagem Sécurité sales were €1.4 billion. Sagem's expertise comes from its capacity to master fundamental technologies and its systems integration ability to coordinate and integrate them into complex operational systems. Sagem will bring to the HIDE project its experience in several countries around the world involving digital identity management. It has deployed identity cards or voting cards to Nigeria, Lebanon, United Arab Emirates, Mexico, Colombia, and the Philippines. Sagem will bring additional expertise to the project involving privacy enhancing technologies like cryptography, which it has deployed in the new release of the French bankcard and in secure communication mode for governmental and military services.

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, Belgium

Sagem Sécurité
Paris, France

The Hastings Center
Garrison, NY

University of Ljubljana
Ljubljana, Slovenia

Zuyd University
Herleen, The Netherlands