



# DIALOGUE

Volume 1 • No. 4 2009 | March

## POLICY FORUM REPORT

# HIDE Policy Forum on Outsourcing of Systems for Detection, Identification, and Authentication

### IN THIS ISSUE

- 1 *Policy Forum Report*  
HIDE Policy Forum on Outsourcing of Systems for Detection, Identification, and Authentication
- 3 *Feature Article*  
From Pallets to People?  
*RFID and Technology Design*
- 9 *News and Notes*
- 10 *Partner Profiles*  
Eutelis Italia and Optel Ltd

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 Victor M. Lee, IBG

**O**n 6 February 2009, International Biometric Group (IBG) hosted the first HIDE Policy Forum, titled “Outsourcing of Systems for Detection, Identification, and Authentication.” Forum participants weighed the benefits and costs of the trend toward outsourcing biometric systems and personal detection technologies. They also examined the privacy, data protection, and other ethical concerns that surface as a result.

### General Themes

Governments and corporations are increasingly willing to outsource their functions, processes, and procurement activities to parties in other countries. In his presentation, “Ethical Dimensions of Outsourcing,” Victor M. Lee began with a broad definition of outsourcing—the procurement of goods or services under contract with an outside supplier—that he then began to break down. Outsourcing may be divided geographically into onshore outsourcing (also called “domestic outsourcing”) or offshore outsourcing. Onshore outsourcing refers to outsourcing conducted entirely within a single country. Offshore outsourcing refers to outsourcing that transcends national borders or jurisdictions. He noted that

outsourcing can be divided into two categories: business process outsourcing and technology services outsourcing. Business process outsourcing is the outsourcing of operational func-

“Ethical considerations about outsourcing include whether data protection practices should be standardized across the European Union.”

tions and responsibilities to third-party providers. Technology services outsourcing refers to the research, development, manufacture, production, provisioning, and/or support of hardware and software systems by a third-party provider.

Lee pointed out that public-sector entities increasingly rely on the often faster-moving and more cost-efficient private sector to handle what were once core government responsibilities, such as security operations and

CONTINUES ON PAGE 2



## IBG Policy Forum Participants

- Valeria Balestrieri  
*CSSC*
- Bojana Bellamy  
*Accenture*
- Wieslaw Bicz  
*Optel*
- Kirsten Bock  
*Independent Centre for Privacy Protection*
- Alastair Campbell  
*National University of Singapore*
- Antonella Caretta  
*Garante per la Protezione Dei Dati Personali (Italian DPA)*
- Antonio Casseli  
*Garante per la Protezione Dei Dati Personali (Italian DPA)*
- Simon Dobrisek  
*Uni-LJ*
- Katja Jacobsen  
*CESAGEN*
- John Leach  
*IAAC*
- Victor Lee  
*IBG*
- Karen Maschke  
*The Hastings Center*
- Paul McCarthy  
*CESAGEN*
- Lokke Moerel  
*De Brauw*
- Ariane Mole  
*Bird & Bird*
- Emilio Mordini  
*CSSC*
- Tom Murray  
*The Hastings Center*
- Lisbeth Nielsen  
*National University of Singapore*
- Alexander Nouak  
*Fraunhofer*
- Karolina Owczynik  
*Zuyd University*
- Alain Pannetrat  
*CNIL*
- Carole Pelligrino  
*SAGEM*
- Chris Pounder  
*Amberhawk*
- Rafaella Puggioni  
*John Cabot University*
- Max Snijder  
*EBF*
- Michael Thieme  
*IBG*
- David Wright  
*Trilateral Research & Consulting*

identity management. Security concerns could both encourage and deter outsourcing. Governments and companies might be wary of outsourcing if they were concerned about data handling by contractors outside of their jurisdiction. Private sector outsourcers, he noted, could take (mis)calculated risks with sensitive data that would be unthinkable for the public sector. However, outsourcing could benefit those governments and companies that would have lower-quality products and outcomes if they provided needed services or supplies themselves. Also, through outsourcing contracts to trusted providers and/or allies, governments or companies might save time and money that could be spent on complementary security enhancements that build upon existing in-house expertise.

Finally, Lee offered five ethical considerations for reflection and debate:

- the merits of extending diplomatic protection to outsourcers;
- the desirability of expanding legal jurisdictions to include extraterritorial outsourcers;
- the feasibility of limiting types of “outsourcable” data;
- the need to resolve discrepancies in data protection practices across the European Union;
- and the proper role (regarding oversight, etc.) of public sector entities toward their outsourcers.

John Leach, an information society specialist, focused on the challenge of maintaining public confidence while at the same time permitting personal detection systems to be used for national purposes like national security assurance, border enforcement, and maintaining public order. Leach noted that the public often feels more vulnerable when the government—already viewed as intrusive—outsources the handling of personal data. He also pointed out that there are issues beyond privacy concerns. Threats from inappropriately processed data include profiling and

discrimination, erroneous treatment and compensation due to incorrect data, and data misuse leading to malicious treatment. However, he insisted that protecting personal information and developing systems to collect and process personal data need not be at odds if there was a properly constructed governance framework to provide standard privacy protections and ensure transparency of outsourcing policies and practices. Privacy protections include defining and delimiting system purposes, defining roles and role boundaries, monitoring activities, proactively reporting breaches to affected citizens, providing effective recovery and restitution for those affected, and providing regular performance updates, especially when outsourcers are involved. As for transparency, Leach encouraged the dissemination of written standard protections and education of the public as to the risks involved and safeguards in place.

In his presentation on “Biometrics and e-Identity,” Max Snijder explained how biometric tools contain sensitive data because they help to establish and verify root identity. He also noted that concerns over biometric data were not wholly unfounded, as the possibilities of biometric spoofing and biometric data theft were realistic. Compromised biometrics, Snijder said, could lead not only to spoofing and manipulation, but also to tracking, surveillance, societal labeling, and social engineering. He pointed out that biometric implementations can be arranged so that they are privacy-sensitive and advocated using and processing templates instead of actual facial images so that raw biometric image data never leave biometric data systems.

### The EU Framework and Member State Policies

In his presentation, “Outsourcing and the EU Data Protection Directive,” Chris Pounder stressed the importance of accurately and clearly defining the roles, responsibilities, and obligations of those

CONTINUES ON PAGE 4



## FEATURE ARTICLE

# From Pallets to People? *RFID and Technology Design*

By Jacob Moses, The Hastings Center

*Design is a plan for arranging elements in such a way as best to accomplish a particular purpose.*

—Charles Eames (1907–1978)

For designers like Eames, the process of creating useful objects is as important as the objects themselves: it is a design dictum that process drives product. Thus, it seems reasonable that when trying to understand an emerging technology, we should consider not only the technology itself, but also the design process, values, and constraints that shaped the technology's creation. Doing this is especially relevant when the technology is designed and developed for a particular set of purposes, but its use then expands beyond the original scope, as is the case for radio frequency identification (RFID).

Typical RFID systems are composed of three components: a chip, a receiver, and a database. The chip, which is attached to or embedded in an object, contains data that is transmitted in a radio signal. A receiver—which in some systems can be over 600 feet away from the chip—decodes the signal. The information is then stored in a database, which may interact with other systems to retrieve related data.

Radio waves have been used to identify objects at least since World War II, and the first patent for RFID technology dates back to 1973. However, it was not until the late 1990s that RFID technology was developed for commercial applica-

tions such as electronic devices on toll roads. RFID's greatest boost came in the early 2000s when businesses began using it to more quickly and intelligently track packages through the labyrinthine global supply-chain.<sup>1</sup> RFID chips can transmit information about goods wirelessly to a receiver outside the container, thus obviating the need to physically open and inspect the contents of the container.

As technical standards that facilitate the use of generic readers have emerged, the use of RFID has expanded and manufacturing costs have dropped. Yet privacy concerns are on the rise—especially concerns about governments' use of the technology for the surveillance and tracking of citizens and noncitizens alike. For example, when embedded in a pair of shoes, a chip that helped track movement of the shoes from the factory to the store could also be used to monitor the movement of the wearer walking on the street. Thus, while the prospect of RFID-tagging everything from shampoo bottles to prescription drugs and creating an "Internet of things" might be useful in some contexts,<sup>2</sup> using RFID in identity documents like passports is controversial because pallets and people differ in more than one morally relevant way.

### Same Chips, Different Purposes

Civil society groups, privacy advocates, and others worry that governments designing identification systems that use RFID are neglecting privacy issues. One interesting charge is that the "Gen 2" RFID chips used in personal identification documents

“There is international consensus that when developing applications of RFID, privacy considerations should be part of the design process from the start, rather than relegated to the end.”

like passports borrow directly from industry without consideration of the different context for identity management. As one opponent has argued, "the Gen 2 chip was designed to track things, not identify people."<sup>3</sup> Other commentators have pointed out that "it shouldn't surprise you that a system designed to be manufactured as cheaply as possible is also designed with no security constraints whatsoever."<sup>4</sup> The implication is that it's not only data that is encoded in the RFID chip, but also the interests and intentions of its designers.

In the context of supply-chain management, standards that allow any RFID tag to be read by any read-

CONTINUES ON PAGE 5

involved in protecting individuals' personal data. Drawing upon Articles 15, 16, 17, and 26 of the EC Data Protection Directive, he noted that outsourcing is typically a data processor activity, and that the data controller is responsible for selecting and vetting the data processor. Pounder rejected the notion that software or technology provisioning is a form of outsourcing and contended that only those delivering services who actually handled personal data (e.g., support, testing, etc.) should be defined as data processors. He also noted that data controllers should be liable for the use of biometrics or personal data and that they should undertake privacy impact assessments. In addition, data controllers should improve their understanding of the technologies involved in order to convince data subjects why the processing of their personal data is in their best interest.

Antonio Caselli and Antonella Canetta described Garante per la Protezione Dei Dati Personali, the Italian data protection authority (DPA), and its views on outsourcing. The Italian DPA is an independent, government-recognized entity whose authority derives from the 2003 Italian Personal Data Protection code. As a collegiate body consisting of four members, the Italian DPA is responsible for developing privacy awareness, verifying compliance with the data protection code, conducting inspections and database reviews, and evaluating citizen complaints and reports. Caselli and Canetta mentioned that one of the critical roles for the Italian DPA was to form a bridge between data controllers/data processors and the citizenry. They noted that one goal of the Italian DPA is to build trust with the citizenry regarding the processing and sharing of their personal information. To do this, the organization can apply administrative sanctions and report to judicial authorities instances involving violations of the data protection code. The Italian DPA advocates transparency of database management and the implementation of safeguards that vary as a function of the sensitivity of

the data in question. Technologies cannot be approved on a blanket basis, but must demonstrate both proportionality and specificity in function and purpose. They emphasized, however, that the Italian DPA is not against technology. Rather, the organization seeks to understand technologies like biometrics and to determine how such technologies can be used productively and even to enhance personal security. Such advance analysis is conducted in part under the "prior checking" activities of Article 20 of the EC Data Protection Directive.

In her presentation on "Biometric Systems, Outsourcing, and Data Privacy," Ariane Mole discussed the French perspective and possible changes at the EU level of data protection policies. In France, biometric data can only be processed with prior authorization from the French data protection authority (CNIL). CNIL assesses how the outsourcing is performed, including examining existing security measures. Similarly, outsourcing of French personal data outside of the European Union also requires prior authorization from CNIL. Alain Pannetrat, who also provided information about CNIL, noted that biometric data processed under access control needs are rarely considered to be permissible when outsourced domestically. He said that offshore outsourcing to a non-EU compatible country was also unheard of, except in cases of border control. Pannetrat distinguished biometric data from other types of data, indicating that the former was especially sensitive given its irrevocability and ability to be linked across disparate databases. Additionally, he mentioned users' allegedly limited confidence, awareness, and understanding of biometric technologies. These factors have led CNIL to take a very strict approach to biometric data

protection, especially with respect to outsourcing.

Pannetrat noted that CNIL is not insensitive to the need for biometrics in outsourced access control. Thus, it is open to compromise regarding which biometrics are always kept under local control (users empowered with control over their own biometric data or traceless biometrics used with local databases), while the rest of the process may be outsourced.

### Certification and Service Provider Perspectives

In her presentation on "Privacy Friendly Outsourcing," Kirsten Bock described the work of the Independent Centre for Privacy Protection (ICPP), a data protection

“Instead of asking whether biometrics or personal data collection meet data protection requirements, the real question is whether such data should be processed for national security purposes at all.”

authority in Germany. Bock focused mostly on the ICPP's EuroPriSe project, an effort in which ICPP issues a "trust mark" or "privacy seal" for outsourced products or services that meet its privacy and data protection standards. This concept provoked much discussion, and Bock acknowledged that because countries like Spain and Italy have different approaches, ICPP certification would need to be done on a country-by-country basis. She confirmed that large companies would not be eligible to receive a single seal that could be applied across the European Union and noted that the seal was only voluntary and thus shouldn't be a market barrier to entry for non-EU companies ineligible for the seal.

Bock highlighted two major categories of outsourcing risk: 1) loss of data, data theft, or identity theft; and 2) financial responsibility, legal liability

er are a very clever bit of technical design. However, the elegant beauty of interoperability risks becoming a tangled privacy mess when the same technology is applied to the direct and indirect identification and tracking of people. Technical documents produced early in the development of Gen 2 RFID chips suggest that the designers conceived of the technology as “decoupled” from “any security and cryptographic technique.”<sup>5</sup>

Subsequent efforts to embed electronic product code RFIDs in identity documents illustrate that, even when implemented, many privacy protection schemes have troublesome vulnerabilities. Researchers have found, for example, that RFID chips in a driver’s license can be read “in the field” even when embedded in a protective case designed to block signal transmission. Moreover, the few security measures designed into the Gen 2 chips were not properly enabled, and individuals who have an RFID document are probably unaware of either the privacy risks or how to use the privacy-protecting features that have been tacked on to reduce them.

Beyond the concrete technical vulnerabilities that can arise from a technology designed for one purpose but used for a different one, there may also be symbolic harms from the use of that technology. For example, is there something troubling about governments using a technology originally designed to track objects and animals to identify people within its borders?

### Trying to Stay Neutral

Guidelines with input from nearly every developed nation and best practices from the communications industry recommend that when developing applications of RFID, privacy considerations should be integrated into the design process from the start, rather than relegated to the end. Yet this approach was arguably not followed in the case of U.S. electronic identification documents.<sup>6</sup> Integrating privacy considerations into technology design may, however, be in tension with a dominant princi-

ple in technology assessment. “Technology neutrality” states that “in and of itself [RFID] does not impose threats to privacy.” Rather, the principle suggests that we focus primarily on how technological tools are used by human actors. But if the international consensus is correct and we should care about the principles and purposes built into the design process, why should we ignore these matters when it comes to actually assessing a technology?

One reason is that we may fear the result will be to broadly condemn the technology itself. This concern may be well-founded, as it can excuse bad actors who use a technology irresponsibly. We should not conclude simply that a technology like RFID will itself necessarily bring about particular outcomes. For example, China’s effort to track its citizens with RFID cards encoded with their names, addresses, work histories, educational backgrounds, religions, ethnicities, police records, and medical insurance status is problematic only when evaluated in the context of the country’s political, social, and economic structure. At the same time, relevant design features—such as the fact that users are unable to read the content of the information contained in the chip or know when their signal is being read by others—might enable particularly invasive programs that differ both quantitatively and qualitatively from what can be done with paper-based identity documents.

### Better Design

Keeping policy agnostic of the particulars of a technology is not meritless, but it can also obscure foreseeable vulnerabilities. Once privacy concerns are better integrated into design and policy processes, some may well wonder whether in the end RFID identity cards remain beneficial. In fact, the United States Department of Homeland Security Emerging Applications and Technology Subcommittee found that “for . . . applications related to human beings, RFID appears to offer little benefit when compared to the consequences

it brings for privacy and data integrity. Instead, it increases risks to personal privacy and security, with no commensurate benefit for performance or national security.”<sup>7</sup>

Looking at the design assumptions and construction alone cannot answer the question of whether or how we ought to embed RFID in identity documents. However, examining the complex interaction between a technology’s intended use and its actual use can help illuminate some ways to help shape its responsible use, especially when it raises ethical concerns. Perhaps if we think like designers, we can design more ethical products and policy.

1. The history of RFID technology. *RFID Journal*, <http://www.rfidjournal.com/article/view/1338/1/129>.

2. International Telecommunication Union. *The Internet of Things*. Geneva, Switzerland: ITU, 2005.

3. Cope S, The impact of implementation: A review of the REAL ID Act and the Western Hemisphere Travel Initiative. Testimony before the Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, 29 April 2008.

4. Halperin R. TFI perspective on RFID as an Aml enabling technology. In: *FIDIS: Future of Identity in the Information Society*. Chapter D7.7: RFID, Profiling, and Aml. Ed. Hildebrandt M and Meints M, August 2006, <http://www.fidis.net/resources/deliverables/profiling/d770/doc/28/>.

5. Brock DL. *The Electronic Product Code (EPC), A Naming Scheme for Physical Objects*. Cambridge, MA: Massachusetts Institute of Technology, 2001.

6. Meingast M, King J, Mulligan DK. Embedded RFID and everyday things: A case study of the security and privacy risks of the U.S. e-passport. Conference paper, IEEE International Conference on RFID, March 2007, <http://www.truststc.org/pubs/157.html>.

7. DHS Emerging Applications and Technology Subcommittee. *The Use of RFID for Human Identification*. Washington, DC: DHS, 2006.

ty for damages, and loss of face or image. To help address these problems, Bock proposed an approach consisting of several elements: data minimization, transparency, process control, clear descriptions of roles and responsibilities, clear contracts between data controllers and data processors, implementation of data subject rights, and controls and audits. On the first three elements, Bock often agreed with the Italian DPA. She similarly insisted that data subjects should generally maintain ownership and control over their personal data and that they should also be entitled to damages caused by abuse, misprocessing, or mishandling of personal data.

Bojana Bellamy's presentation emphasized the outsourcer and system integrator's perspective regarding outsourcing and data protection. Bellamy pointed out that complex data flows, multiple delivery locations, and varying national rules and attitudes on data protection made protecting data privacy incredibly complex in today's world. She expressed concern that many of her company's clients expect service providers to protect data and thus to assume liability for security breaches. This view is at odds with prior presenters' remarks that data controllers—not data processors—are ultimately liable and responsible for the protection of personal data. Indeed, Bellamy insisted that her company's clients remained the final controller of personal data and that

the company's role is solely to process data and comply with data security regulations and client instructions. Risks, she suggested, should be shared between the controller and the processor. Bellamy described her company's Client Data Protection Program (CDPP), which provides for policies, standards, and procedures; program structure and oversight responsibility; delegation of authority; education and awareness; monitoring and auditing; enforcement and discipline; response and prevention; and program effectiveness assessment. The company's approach to handling data privacy includes developing a "compliance culture" and incorporating contractual requirements and security policies into various project-level "control points."

### Concluding Themes

In the final presentation, Lokke Moerel noted that the private IT sector has embraced outsourcing for some time. Yet public-to-private outsourcing introduces some new questions, especially as more personal data are being exchanged across borders. In addition to the issues surrounding the sensitivity of personal data and biometric data and the high-profile failures in data protection, Moerel raised the problem of conflicting laws across EU member states and between the European Union and the United States. She also noted that the balance had shifted from data protection toward security and said that she thought the wrong questions

were being asked. Instead of wondering whether biometrics or personal data collection meet data protection requirements, the real question should be whether such data should be processed for national security purposes in the first place. The issue is whether national security laws pass data protection tests. To help effect real limitations and practical compliance, Moerel suggested a contractual regime in which binding corporate rules are developed for both data controllers and processors. These binding corporate rules would in turn be linked to a global privacy policy to help unify the European Union through efforts such as the EC Working Party 29's efforts to coordinate data protection authorities. Moerel proposed that privacy protections would only be fully achieved when:

- there is full harmonization of EU security requirements;
- additional Working Party 29 guidance has been created for binding corporate rules for processors;
- Working Party 29 has provided biometric guidance for governments;
- model clauses have been developed between processors;
- data breach notification requirements have been codified;
- and countries with unacceptable state control powers have been publicly identified.

## HIDE Past Events

- **9 September 2009**  
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

- **6 February 2009**  
Policy Forum on Outsourcing of Systems for Detection, Identification, and Authentication, London, UK

- **4 March 2009**  
Policy Forum on Body Issues, Brussels, Belgium

## HIDE Upcoming Events

- **5–6 June 2009**  
Policy Forum on Privacy as Contextual Integrity, Prague, Czech Republic

- **2–3 July 2009**  
HIDE workshop on International Data Sharing and Biometric Identification—The Ethical Issues in an Asian and International Context, Singapore City, Singapore

For more details, visit [www.hideproject.org](http://www.hideproject.org).

## Recent Publications

- EU Court of Human Rights. *S and Marper v. the United Kingdom*.  
<http://www.bailii.org/eu/cases/ECHR/2008/1581.html>

- European Parliament to phase in biometric passports by 2012. *European Biometrics Forum*, 29 January 2009.  
[http://www.eubiometricsforum.com/index.php?option=com\\_content&task=view&id=791&Itemid=95](http://www.eubiometricsforum.com/index.php?option=com_content&task=view&id=791&Itemid=95)

- Marks P. Face-blurring technology raises privacy questions. *New Scientist*, 31 January 2009.  
<http://www.newscientist.com/article/mg20126936.600-face-blurring-technology-raises-privacy-questions.html?full=true&print=true>

- Relaunch issue: Revisiting video surveillance. *Surveillance & Society* 2009;6(1).  
<http://www.surveillance-and-society.org/ojs/index.php/journal/issue/view/Relaunch/showToc>

- House of Lords, Select Committee on the Constitution. *Second Report of Session 2008–09. Surveillance: Citizens and the State. Volume 1: Report*. UK Parliament, February 2009.  
[http://www.hideproject.org/downloads/House\\_of\\_Lords-Part1\\_Borders\\_Citizenship\\_Immigration\\_Bill.pdf](http://www.hideproject.org/downloads/House_of_Lords-Part1_Borders_Citizenship_Immigration_Bill.pdf)

- House of Lords, Select Committee on the Constitution. *Second Report of Session 2008–09. Surveillance: Citizens and the State. Volume 2: Evidence*. UK Parliament, February 2009.  
[http://www.hideproject.org/downloads/House\\_of\\_Lords-Surveillance\\_Citizens\\_and\\_the\\_State.pdf](http://www.hideproject.org/downloads/House_of_Lords-Surveillance_Citizens_and_the_State.pdf)

- Response to the House of Lords Constitution Committee Surveillance Society report. UK Information Commissioner's Office, 6 February 2009.  
[http://www.ico.gov.uk/upload/documents/pressreleases/2009/hol\\_surveillance\\_report\\_statement.pdf](http://www.ico.gov.uk/upload/documents/pressreleases/2009/hol_surveillance_report_statement.pdf)

## PARTNER PROFILES

### EUTELIS ITALIA SRL



Eutelis Italia is a telecommunications and media consulting firm that specializes in providing national and international consulting services to telecommunications and value-added services providers, network operators and providers, equipment manufacturers, telecommunications users, and public authorities. Additional services include consulting in the areas of regulatory framework, smartcard applications, human resources, and start-up financing. Eutelis also provides strategic consulting services for technical and economic product and services development concepts, as well as competitive, market, and efficiency analyses. In addition, Eutelis can assist in the implementation of strategic concepts by developing market entry strategies, marketing concepts, and business concepts, and by providing project management, product placement, and development and realization planning, as well as expert opinions, studies, and workshops. All of these services are carried out on an individual basis and are customized to suit each client's needs. Eutelis' consulting services for service and network providers consist of developing concepts for new services combined with diversified consulting experience ranging from technical solutions to market research and entry concepts, business and marketing planning, and project management for service introduction. Eutelis is experienced in helping new service providers of voice, mobile, Internet, and broadband service providers develop, implement, and operate new services, networks, and companies.

### OPTEL LTD



Optel's roots go back to 1985, when Wieslaw Bicz, the company's President and CEO, brought a group of specialists together to investigate the feasibility of developing a fingerprint scanning and recognition device using ultrasound as the scanning medium. This project led to the development of a fully operational proof of concept prototype in 1992, which represented the first successful use of ultrasound in a fingerprint scanning application. Through its early years, Optel's efforts were focused almost exclusively on the biometric finger-scanning project. However, over the last ten years, Optel began working on a number of other innovative products involving such diverse technologies as ultrasound and acoustical emissions, analysis, and processing, as well as acoustical and holographic imaging techniques. The company has 20 employees, most of whom are experienced engineers who specialize in physics, electronics, mechanics, informatics, and acoustics. Optel's primary goal is to develop new and innovative hardware and software technologies for various product applications, with a focus on product developments possessing mass-market potential. Optel's innovative developments have resulted in the granting of several patents in the United States and elsewhere for applications in the field of biometrics, nondestructive testing, and medical diagnostics.

## 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, USA

**University of Ljubljana**  
Ljubljana, Slovenia

**Zuyd University**  
Heerlen, the Netherlands