



# DIALOGUE

Volume 1 • No. 2 2008 | September

## FROM THE EDITOR

# The Québec Commission: *Ethics, Democratic Values, and the Surveillance Society*

### IN THIS ISSUE

- 1 *From the Editor*  
The Quebec Commission:  
Ethics, Democratic Values,  
and the Surveillance Society
- 3 *Feature Article*  
A Fair Trade? Canadian  
Ethics Commission Helps  
Recast the "Privacy vs.  
Security" Dilemma
- 6 *HIDE Spotlight*  
Focus Group on Digital  
Identities
- 8 *Partner Profiles*  
Cesagen and Zuyd University
- 7 *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.



The groundswell of insecurity, obsession for the elimination of risk, security, as well as implementation of intrusive surveillance methods, are toxic to democracy.<sup>1</sup> With that declaration, the Québec Commission de l'éthique de la science et de la technologie opened the final paragraph of its position statement, *In Search of Balance: An Ethical Look at New Surveillance and Monitoring Technologies for Security Purposes*. The Commission was established in the fall of 2001 by the Conseil de la science et de la technologie at the behest of the Québec Minister of Research, Science, and Technology. Its mission is to inform, sensitize, gather opinions, foster reflection, and organize debates "on the ethical issues raised by developments in science and technology" and to propose "orientations to guide stakeholders in their decision-making."<sup>2</sup> The Commission has also issued other position statements on ethical issues raised by scientific and technological developments.<sup>3</sup>

This issue of *Dialogue* provides two reviews of the Commission's position statement. In this column, I describe the contents of the position statement and the new technologies the Commission examined; summarize the statement's main themes; and outline the ethical framework the

Commission adopted in assessing the new technologies. In the feature article, Jacob Moses provides a more in-depth analysis of the Commission's key findings and of the Commission's framing of values.

“Governments no longer gather information only about certain risk segments of the population. Global networks of digital databases make anyone a possible object of surveillance.”

### A Look Inside

The 73-page position statement contains three chapters and two appendices. Chapter 1 defines the concept of security; examines the sense of insecurity reflected in media coverage of certain events and public opinion polls; asserts that modern societies have become risk societies;

CONTINUES ON PAGE 2

**Table 1. New Surveillance and Monitoring Technologies**

Biometric system	A technological application that "allows a person to be automatically identified, or to verify a person's eligibility to be given certain rights or services (namely access) based on the recognition of physical attributes (fingerprints, retinal patterns, hand geometry), traces (DNA, blood, odors), or behaviors (signature, gait)." (p. 21)
Video surveillance	Use of cameras for remote monitoring of public or private areas. Images taken from monitoring equipment can be viewed on a screen. This is an old technology with new technological advances in miniaturization and concealment as well as in image digitization which "allows for facial recognition of filmed individuals and comparison with other previously collected biometric data." (p. 28)
Radio frequency identification tag	An electronic tag with a miniature antenna that can be activated by a specific reader that translates the analogue information into digital data for processing by a computer. Data from an RFID tag can be transferred to a reader by way of four different frequencies: low frequency (100–500 kHz), high frequency (10–15 MHz), ultrahigh frequency (850–1000 MHz), and microwave (2.4–5.8 GHz). RFID technology collects a variety of data about individuals and tracks them as they move through public places.

asks whether risk societies foster the rise of surveillance societies; and identifies the key values and ethical issues raised by the deployment of new surveillance and monitoring technologies. The chapter also describes the current regulatory regimes in Canada and Québec regarding information privacy. In Chapter 2 the Commission focuses on three new surveillance and monitoring technologies: biometric systems; video surveillance (also known as closed circuit television, or CCTV); and radio frequency identification

(RFID). The ethical and privacy issues raised by the deployment of these technologies are addressed in Chapter 3. Appendix 1 reprints the *Rules for Use of Surveillance Cameras with Recording in Public Places by Public Bodies* developed by the Commission d'accès à l'information du Québec. The *Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities* issued by the Office of the Privacy Commissioner of Canada are reprinted in Appendix 2.

The technologies the Commission examined are listed in Table 1. Most of them are not new. For instance, fingerprinting has been used since the early 1900s; video cameras and RFID have been around for more than a half century. Moreover, there is nothing new about government entities (national, subnational, and local) collecting personal information about their citizens, tourists, guest workers, and immigrants. What is new is the extent to which these technologies are being used in mass surveillance for security purposes—sometimes surreptitiously and sometimes without individuals' consent—and the ability to share and data-mine massive amounts of personal information

through the use of global, interconnected databanks.

To fulfill their obligation to protect their citizens from harm, governments need information about potential and actual threats to the safety of the populace. As the Commission notes, "Providing security for a territory, a country, city, or home is a constant challenge which involves accurate threat assessment and the implementation of effective protection systems."<sup>4</sup> Drawing from the literature on security, risk, and surveillance, the Commission identified two mutually influential dimensions of the concept of security: an objective dimension that involves assessing the actual level of security or absence of threats and dangers, and a subjective dimension that "refers to how people feel about their own safety."<sup>5</sup> There has been a growing sense of insecurity in Canada and elsewhere since the September 11, 2001, attacks on the World Trade Center in New York City and the US Pentagon in Washington, DC. Even before the events of 9/11, however, modern Western societies were already obsessed with eliminating risk. Governments have increasingly developed action plans, policies, and laws to protect citizens from perceived threats to their security, including methods of collecting information to make risk assessments and to effectively direct resources to prevent and respond to crimes or terrorist attacks. What's changed in recent years is that governments no longer gather information only about certain risk segments of the population. Instead, the general public is now "under surveillance in order to target actions against individuals considered at risk, or who present a risk to others."<sup>6</sup> Moreover, global networks of digital databases containing personal information obtained from biometric systems, video surveillance, and RFID tags make it possible for anyone to become the object of surveillance.

The normative framework the Commission used in examining these technologies is presented in Table 2. As the title of the position statement

**Table 2. Key Democratic Values and Ethical Issues**

**Democratic values**

- Autonomy
- Security
- Freedom
- Privacy
- Transparency
- Justice
- Equality

**Ethical issues**

- Relevance, effectiveness and reliability
- Proportionality of response to insecurity
- Social acceptability
- Consent
- Respect for the end purpose
- Protection of personal information

CONTINUES ON PAGE 4



# A Fair Trade?

## Canadian Ethics Commission Helps Recast the “Privacy vs. Security” Dilemma

By Jacob Moses, The Hastings Center

Responding to many of the same trends in national security surveillance as the HIDE project, the Québec Commission de l'éthique de la science et de la technologie's recent position statement outlines key ethical issues raised by the collection of information through biometric scanning, video surveillance, and radio frequency identification (RFID).<sup>1</sup> While some issues the Commission addresses are particular to the Canadian context (especially the discussion of privacy laws and public opinion polls), the ethical framework is highly germane to the wider international conversations about privacy, security, and surveillance. In this article, I summarize some of the Commission's key findings and recommendations as well as discuss the Commission's framing of values, which has perhaps the greatest relevance to the HIDE project.

### Down with “Big Brother”

The position statement begins with a general sociological discussion of surveillance, security, risk, and fear. The Commission argues that Canada is becoming a “surveillance society” because, like many other developed nations it is a “risk society” that believes that the more information it gathers, the better it will be able to avoid security risks. One of the difficulties in measuring these risks, however, is that a large component of security is subjective. Fear generated from infrequent but high impact events like acts of terrorism can dramatically raise citizens' sense of inse-

curity. The commission worries that exaggerated responses to risks could produce overreaching surveillance societies.

Some fears of privacy advocates also may be overstated. Although more footnote than all-out critique, the position statement helpfully qualifies the ubiquitous and rhetorically rich—though conceptually problematic—Orwellian image of “Big Brother.” This image of state surveillance is often used as unexamined cliché, and the Commission worries that citing Big Brother suggests the primary danger of surveillance technologies is that they will bring about a throwback to totalitarianism, where nefarious systems will be designed to expunge democratic rights. In overstating their case, the Commission worries that critics miss the *actual* rise of “Small Brothers” — small-scale private and public surveillance programs enacted with the goal of enhancing security. The efforts of good-intentioned but perhaps short-sighted surveillance actors could paradoxically lead to a more gradual erosion of fundamental rights. If ignored, Small Brothers that do “not necessarily follow proper guidelines and sound practices, could fall completely beyond the control of the state.”<sup>2</sup>

The Big Brother metaphor also

suggests a sort of technological determinism that ignores the social and political context driving the development and application of surveillance and monitoring technologies. The language of Orwell hints that these technologies are intrinsically poisonous and will inevitably lead to dystopia.

“ The use of [new surveillance and monitoring technologies] must never lose sight of its primary objective: to protect democratic societies against the risk of compromise to its fundamental values. ”

In urging a balanced view of the pitfalls, but also of the possibilities of surveillance and monitoring technologies to serve society, the Commission lays out recommendations that it hopes can help society avoid both Big and Small Brothers.

### Ethical Considerations

Carving out a middle ground, the Commission recommends several ways to facilitate the responsible use of surveillance and monitoring technologies. The Commission identified six ethical issues through which to assess applications of and policies for these technologies.

CONTINUES ON PAGE 5

indicates, the Commission sought to find a proper balance between the competing democratic values of security and freedom, with the goal of promoting both values simultaneously.<sup>7</sup> This is always a difficult challenge because an emphasis on security may compromise “the very rights and liberties that constitute the founding principles of democracy.”<sup>8</sup> After outlining the normative framework to use in assessing deployment of the surveillance and monitoring technologies, the Commission made six recommendations directed to several government agencies (Table 3).

First, there should be a dialogue among citizens, the government, and the industry to develop guidelines for biometric systems, video surveillance, and RFID. The Commission noted that such guidelines should take into account ethical concerns with respect to fundamental democratic values. Second, a consultative approach should be developed to advise the government about its deployment of new surveillance and monitoring technologies, with particular emphasis

on focusing on ethical concerns about the relevance, effectiveness, and reliability of the technologies. Third, the public consultation process should follow the model developed by the *Commissaire à la santé et au bien-être*. Fourth, the results of the public consultation should be readily available so as to raise the general public’s awareness about the ethical issues associated with the new surveillance and monitoring technologies. In its fifth recommendation, the Commission said there should be additional attempts to inform the public about a) the legal issues surrounding the use of new surveillance and monitoring technologies and the consequences for the values of autonomy, freedom, security, and privacy and b) the means for public participation in the decision-making, implementation, and follow-up processes. Finally, the Commission suggested implementing mechanisms to compensate individuals wrongfully associated with illicit activities and to correct the mistake. In addition to these recommendations, the Commission

said that the *Bureau de la sécurité privée*, which regulates the private security industry in Québec, should include in its training for licensed agencies “a compulsory ethics component based on the ethical issues raised in this Position statement.”<sup>9</sup>

Whether the Commission’s recommendations will be implemented in Québec or elsewhere in Canada remains to be seen. And it’s unclear what impact the position statement will have in the United States or Europe. Finally, more could be said about using a balancing approach in assessing the use of new surveillance and monitoring technologies. Several commentators have challenged the idea of balancing security and liberty and in doing so attempt to develop a fuller critique of security.<sup>10</sup> Through focus groups, policy forums, ethics briefs, and policy papers, HIDE partners and other stakeholders will be examining these and other issues the Commission raised in its position statement. Stay tuned.

—Karen J. Maschke  
The Hastings Center

**Table 3. Commission Recommendations**

**Recommendation 1**

- Promote a dialogue among citizens, the government, and the industry towards the adoption of guidelines regarding the use of biometric systems, video surveillance, and RFID.
- Take into account ethical concerns with respect to fundamental democratic values when setting guidelines.

**Recommendation 2**

- Use a consultative approach to advise the government about deployment of new surveillance and monitoring technologies, with particular emphasis on areas that raise ethical issues using the criteria of relevance, effectiveness, and reliability.

**Recommendation 3**

- Use the consultation model developed by the *Commissaire à la santé et au bien-être* to organize a public consultation process that highlights the ethical issues involving the use of surveillance and monitoring technologies.

**Recommendation 4**

- Make the results of the public consultation publicly available to sensitize the general public about the ethical issues associated with the new surveillance and monitoring technologies.

**Recommendation 5**

- Inform the public about a) the legal issues surrounding the use of new surveillance and monitoring technologies and the consequences for the values of autonomy, freedom, security, and privacy and b) the means for public participation in the decision-making, implementation, and follow-up processes involved.

**Recommendation 6**

- Implement a compensation and correction mechanism for cases in which the use of new surveillance and monitoring technologies wrongfully associates individuals with illicit activities.

**Acknowledgments**

Thanks to Benjamin Gould for his research assistance in preparing this piece.

1. Commission de l'éthique de la science et de la technologie. *In Search of Balance: An Ethical Look at New Surveillance and Monitoring Technologies for Security Purposes*. Québec, Canada, February 8, 2008, p. 53. <http://www.ethique.gouv.qc.ca/In-Search-of-Balance-An-Ethical.html>.
2. Commission de l'éthique, Mission Statement, <http://www.ethique.gouv.qc.ca/Mission-and-mandate.html>.
3. Commission de l'éthique, *Informing, Reflecting, Proposing. 2001–2007 Activity Report and Future Prospects*. [http://www.ethique.gouv.qc.ca/IMG/pdf\\_CEST2001-2007Activity-Web.pdf](http://www.ethique.gouv.qc.ca/IMG/pdf_CEST2001-2007Activity-Web.pdf).
4. Commission de l'éthique 2008, *In Search of Balance*, p. xix.
5. *Ibid.*, p. 3.
6. *Ibid.*, p. 10.
7. *Ibid.*, p. 37.
8. *Ibid.*, p. xxiii.
9. *Ibid.*, p. 52.
10. Ashworth A. *The Criminal Process: An Evaluative Study*. Oxford, UK: Oxford University Press, 1998; Dworkin R. The threat to patriotism. *New York Review of Books*, February 28, 2004, 44-49; Neocleous M. Security, liberty and the myth of balance; towards a critique of security politics. *Contemporary Political Theory* 2007;6:131-149.

■ **Relevance, effectiveness, and reliability.** The Commission worries that the widespread use of surveillance and monitoring technologies could reverse the burden of proof regarding perceived and real threats to security. For example, innocent suspects identified by an unreliable surveillance technology could become victims of unwarranted reliance on the technology. To some extent, we have seen this in the explosion of forensic DNA testing for law enforcement purposes. Although incredibly powerful as an identifier, this technology and its application will always be imperfect. In a precautionary appeal, the Commission urges that surveillance advocates be the ones charged with demonstrating that a surveillance technology is safe and effective; targets of surveillance should not bear the burden of showing it to be unreliable and ineffective.

■ **Proportionality of response to actual risk.** The Commission worries that knee-jerk reactions to dramatic breaches of safety or security like terrorist attacks could result in an exaggerated response. Thus, the technical reliability, proportionality of response to insecurity, and degree of intrusiveness should be examined for each and every deployment of surveillance and monitoring technologies.

■ **Social acceptability and public consent.** The public—particularly those who will be placed under surveillance—should be asked what it thinks about the use of surveillance and monitoring technologies. Moreover, public participation should be encouraged, and deliberations should be transparent. Because individual consent is not feasible and in some cases is contradictory to the primary goals of surveillance technology, the Commission finds that group consent is sufficient provided that the public is informed of how individual information will be used, the policies are transparent, and there are mechanisms in place to file grievances.

■ **Limit scope to respect the end purpose.** To respond to the “functional

creep” that occurs when information is gathered for one purpose and later used for another, the Commission urges both private and public policies that respect the initial ends of the original deployment of the technology—otherwise justification of data collection to the public will be disingenuous. Adopting shorter data retention periods is one recommendation to guard against this creep.

■ **Protect privacy.** The Commission found that it was necessary to discuss the privacy dimension of each technology individually, as the meaning of privacy itself can vary considerably between different types of surveillance. For example, video surveillance challenges what can be seen as a sort of *public* privacy, where the understanding that “everyone is entitled to expect to be able to move about in public without being the object of constant surveillance.”<sup>3</sup> On the other hand, biometrics can be seen as inherently more violative of *personal* privacy, and respecting confidentiality will be much more important. Some concerns, such as data access and sharing, are common to all of the technologies the Commission examined. The Commission calls for a broad, public conversation on privacy.

### Uncompromised Values

As the HIDE project aims to critically investigate the values involved in personal detection technologies, the approach of the Commission may be of particular interest to HIDE partners. The position statement sets out the values the Commission argues should be used in creating and evaluating surveillance policy. Autonomy—the ability for individual self-determination—is frequently argued to be the central value needing protection, whether the discussion is about medical ethics or surveillance technologies. Indeed, the Commission holds respect for indi-

vidual autonomy to be a democratic ideal.<sup>4</sup>

Frequently, surveillance is framed as a direct challenge to autonomy—and, more specifically, privacy. The debates that follow question whether a particular loss of privacy is legal, and whether the associated sacrifices in autonomy are justifiable.

In a recent issue of *Scientific American*, technology commentator Esther Dyson writes “[privacy] concerns are typically presented as trade-offs: privacy versus effective medical care, privacy versus free advertising-driven content, privacy versus security.” Troubled by this trend, Dyson continues, “Those debates are well worn, but they are now returning to the fore in a way they did not when specialists, insiders and die-hard privacy advocates were the only ones

“ If the question is “Do you want security or privacy?” it seems the answer is simply “yes.” The Commission’s privacy statement makes an important contribution to the discussion. ”

paying attention.”<sup>5</sup> While popular, there are good reasons to challenge the trade-offs Dyson identifies. For instance, the Commission applies a lesson learned in the medical ethics context: autonomy does not stand alone and cannot carry the day. Instead of pitting security against autonomy, the report places the value of security next to freedom, privacy, transparency, justice, and equality as necessary prerequisites for individual autonomy in a liberal democracy. It’s easy to see that without a basic level of security from the state, a person’s autonomy (and its associated rights) would be eclipsed by primal concerns for her survival. This is a crude picture of why a state’s police power is justifiable. The Commission suggests that surveillance, particularly that conducted by government, should be

CONTINUES ON PAGE 6

advanced insofar as it *promotes* autonomy and its constituent values. “The use of [new surveillance and monitoring technologies] must never lose sight of its primary objective: to protect democratic societies against the risk of compromise to its fundamental values.”<sup>6</sup>

The language of values may not be new in the debate, but the balance of values the position statement clearly articulates and challenges governments to strike is one that does not call for citizens to forfeit core values of democracy in the name of safety and security. An example of the type of balancing the Commission rejects comes from a consultant for the US Office of the Director of National Intelligence (the office that controls the country’s \$50 billion intelligence budget): “We have a saying in this business: ‘Privacy and security are a zero-sum game.’” In this view, citizens must give up privacy in order to enhance security. But this relationship is hardly watertight.

There are many ways to increase security that do not call for private information. Locks and keys, for example, can increase one’s security, but they don’t involve much sacrifice of privacy. Furthermore, the preliminary findings presented in McCarthy and Jacobsen’s article in the September 2008 issue of *Dialogue* suggests that some technologies for surveillance and monitoring purposes can actually enhance privacy. Naturally, many technologies that would be most useful to security professionals would require access to private information. Critiquing the idea of a zero-sum game merely allows us to acknowledge that there are an awful lot of things we can do to increase security that do not involve privacy, and many compromises of privacy that will not necessarily result in boosted security.

The Commission’s position statement does not suggest that we jettison the language of security and privacy; the two are deeply connected and deeply important. But when these are the only two values considered—and when they are considered

to be in direct opposition—the debate quickly reaches an impasse both philosophically and politically. Critics of surveillance and monitoring technologies worry that supporters ignore the value of fundamental democratic rights, and supporters are afraid that the critics underestimate very real threats to security.

If the question is “Do you want security or privacy?” it seems the answer is simply “yes.” The Commission’s policy statement makes an important contribution to the discussion by showing that responsible, balanced policies will not force decision-makers or citizens to choose a victor in the false dilemma of security versus privacy.

1. Commission de l’éthique de la science et de la technologie, *In Search of Balance: An Ethical Look at New Surveillance and Monitoring Technologies for Security Purposes*. Québec, Canada, February 8, 2008. <http://www.ethique.gouv.qc.ca/In-Search-of-Balance-An-Ethical.html>.
2. *Ibid.*, p. 12.
3. *Ibid.*, p. 47.
4. *Ibid.*, p. 13.
5. Dyson E. Reflections on privacy 2.0. *Scientific American* 2008;299(3):50-55.
6. Commission de l’éthique 2008, p. xx.
7. Wright L. The spymaster. *The New Yorker*, January 12, 2008, p. 52.
8. McCarthy P, Jacobsen KL. Privacy enhancing technologies. *Dialogue: The Newsletter of HIDE* 2008;1(1):3-4.

## HIDE SPOTLIGHT

### Focus Group on Digital Identities in Embedded Systems and Ambient Intelligence

31 October 2008, Maastricht, the Netherlands

In the first of three focus group meetings organized by HIDE partner Zuyd University, invited experts will inspire and provoke discussions on the social and ethical aspects of identification in embedded systems and ambient intelligence. 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. Embedded software, ubiquitous computing, ambient technology, smart objects, and the emergence of “the Internet of Things” are terms denoting a particular aspect or view of this emerging technological future.

Due to developments in radio frequency identification (RFID), miniaturization, wireless and sensor technologies, and near field communication (NFC), people will be moving through and interacting with their physical environment in new ways. Objects themselves will interact and communicate by sending information about themselves, their users, or their environments to electronic networks and databases.

On the positive side, huge gains in convenience, efficiency, and safety are predicted to result from the use of these technologies. From a more bleak perspective, their use could lead to widespread tracking of people and the subsequent loss of individual privacy. In particular, and most relevant to the HIDE project, the information on peoples’ behaviors generated by these systems will likely be an invaluable and highly tempting resource for law enforcement purposes. As a consequence, end-users, consumers, and citizens may be included in the pool of criminal suspects, which would render them vulnerable in unforeseen ways. Thus, it is increasingly recognized that in order to realize the potential value of these technologies and avoid the public’s rejection of them, transparent and preferably end-user controlled identity management systems have to be included from the beginning. ■

*To participate or for more information, please contact Dr. Irma van der Ploeg, [i.vdploeg@hszuyd.nl](mailto:i.vdploeg@hszuyd.nl). The number of focus group participants will be limited.*

## HIDE Past Events

- 9 September 2008  
Technology Convergence Focus Group, Paris, France
- 15 September 2008  
System Interoperability Focus Group, London, UK

## HIDE Upcoming Events

- 31 October 2008  
Embedded Technology Focus Group, Maastricht, Netherlands
- 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
- 2–3 July 2009  
Problem Solving Workshop on Transatlantic and International Data Sharing and the APEC Privacy Framework, Singapore City, Singapore

## HIDE News

- HIDE partner Dr. Irma van der Ploeg, head of the Infonomics and New Media Research Center of Zuyd University, has recently been awarded a Starting Grant for Independent Researchers by the European Research Council. This will fund a five-year research project entitled Social and Ethical Aspects of Digital Identities: Towards a Value Sensitive Identity Management (DiglDeas). The project aims to increase understanding and awareness of the social and ethical aspects of digital identity management (IDM) and to contribute to the quality and social and ethical acceptability of technological developments. With a series of interdisciplinary studies focusing on different application areas of IDM, more fine-grained knowledge of the ways IDM is implicated in contemporary transformations of identity will be produced by a team of three PhD students and a postdoctoral researcher. More information can be obtained from the project coordinator at [i.vdploeg@hszuyd.nl](mailto:i.vdploeg@hszuyd.nl).

## Other News

- The Privacy Commissioner of Canada recently awarded two research grants that have relevance for the HIDE project: Camera Surveillance in Canada: Current Trends (Queen's University) and Privacy Games: The Vancouver Olympics, Privacy and Surveillance (University of Alberta). The projects are expected to be completed in 2009.
- The Surveillance Project has launched The New Transparency: Surveillance and Social Sorting, a project funded by the Social Sciences and Humanities Research Council of Canada through a Major Collaborative Research Initiative (MCRI). The project will examine the history, key characteristics, and consequences of surveillance and social processes that make visible the identities of individuals, the workings of institutions, and the flow of information in unprecedented ways. <http://www.surveillanceproject.org/projects/the-new-transparency>

## Recent Publications

- American Civil Liberties Union. Expert findings on surveillance cameras: What criminologists and others studying cameras have found. [http://www.aclu.org/images/asset\\_upload\\_file708\\_35775.pdf](http://www.aclu.org/images/asset_upload_file708_35775.pdf)
- D'emilio F. Italy opts to have fingerprints on national identity cards. <http://www.news.com.au/couriermail/story/0,23739,24033442-954,00.html>
- Kuppasamy B. Malaysia: Genetic fingerprinting bill under flak. <http://www.ipsnews.net/print.asp?idnews=43837>
- Nakashima E. Citizens' US border crossings tracked. Data from checkpoints to be kept for 15 years. <http://www.washingtonpost.com/wp-dyn/content/article/2008/08/19/AR2008081902811.html>
- Ozer, NA. Rights "chipped" away: RFID and identification documents. *Stanford Technology Law Review* 2008. <http://stlr.stanford.edu/pdf/Ozer-RightsChippedAway.pdf>
- UK Information Commissioner's Office. CCTV Code of Practice. Revised edition. [http://www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specialist\\_guides/ico\\_cctvfinal\\_2301.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf)

## PARTNER PROFILES

### CENTRE FOR THE ECONOMIC AND SOCIAL ASPECTS OF GENOMICS (CESAGEN)



Cesagen is a multidisciplinary center in which staff from the social sciences and humanities work closely with staff from the natural and medical sciences to address the social, economic, and policy aspects of developments in genomics. Established in October 2002 as a collaboration between Lancaster and Cardiff Universities, Cesagen is part of the Genomics Network funded by the Economic and Social Research Council (ESRC). Cesagen has had critical inputs into work on public engagement in the UK with UK Biobank and other governmental initiatives in genomics, as well as strong links with ethics and policy research in Europe. Recent work has examined convergent areas of technology and policy with genomics and health incorporating work on databases, nanotechnologies, and biometrics. Completed projects include Biometric Identification Technology Ethics (BITE); Ethical, Legal, and Social Aspects of Human Genetic Databases: a European Comparison (ELSAGEN); and The Institutionalization of Ethics in Science Policy, Practices, and Impact (INES). Cesagen will continue to work closely with life scientists, clinicians, policy actors, and other key stakeholders in partnership and mutual engagement in addressing the complexities and uncertainties that the genomic era brings.

### ZUYD UNIVERSITY—INFONOMICS AND NEW MEDIA RESEARCH CENTRE



The Infonomics and New Media Research Centre (INM) is an independent and interdisciplinary research unit based at Zuyd University, the Netherlands. Its mission is to develop knowledge, stimulate debate, and increase awareness of societal and normative aspects of information technology; stimulate knowledge valorization and transfer to professional fields; and contribute to user-centered and value-sensitive design. The Centre's primary research focuses on digitization processes in society in general, and social and ethical aspects of digital identities in particular. Centre faculty work with a broad range of national and international partners, among which are knowledge institutions, universities, private enterprises, public services, and government agencies. With the recently awarded Starting Grant for Independent Researchers by the European Research Council, the Centre will develop a five-year research project entitled Social and Ethical Aspects of Digital Identities: Towards a Value Sensitive Identity Management (DigIDeas).

## 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**  
Herleen, the Netherlands