

# DELIVERABLE D4.1a

## Report on The Policy Forum on Privacy as



# HIDE PROJECT

Project funded by the European Commission-FP7

Contract: 217762

Co-ordination and Support Action (CSA)

Start date of the project: 1 Feb 2008

Duration 36 months

1° Reporting Period

Deliverable:	D4.2a
Title:	Policy Forum on Privacy as Contextual Integrity - Report
Due date:	30-07-2009
Actual submission date	30-07-2009
Lead contractor for this deliverable:	The Hastings Center
Contact:	<b><i>maschkek@thehastingscenter.org</i></b>
Dissemination Level:	PU



This work was supported in part by the European Commission under contract FP7-217762 HIDE. HOMELAND SECURITY, BIOMETRIC IDENTIFICATION, & PERSONAL DETECTION ETHICS.

## BACKGROUND

Homeland Security, Biometric Identification & Personal Detection Ethics (HIDE) is a project promoted by the European Commission and coordinated by the Centre for Science, Society and Citizenship, an independent research centre based in Rome, Italy. HIDE's mission is to set up a platform devoted to ethical and privacy issues of biometrics and personal detection technologies which addresses transnational (European) and international problems. HIDE aims to become the preeminent catalyst for innovative policy solutions to emerging ethical problems in the area of surveillance technologies, especially where collaboration among national and international agencies, communities, businesses, and non-governmental organizations (NGOs) is crucial. HIDE promotes creative problem solving and provides for concrete tools for a successful dialogue.

One of HIDE's areas of focus is the theme of privacy as contextual integrity. The concept of privacy is pervasive in debates about biometric identification. But what are we talking about when we talk about privacy? If we're talking about the *meaning* of privacy, there is no single definition of the concept. If we're talking about the *value* of privacy, the fact that aspects of privacy have been found in every society systematically examined suggests that privacy "is a cultural universal necessary for the proper functioning of human beings."<sup>1</sup> One can claim with great confidence, says the philosopher Adam Moore, "that privacy is valuable for beings like us. The ability to regulate access to our bodies, capacities and powers, as well as sensitive personal information, is an essential part of human flourishing and wellbeing."<sup>2</sup> Moreover, many commentators contend that privacy joins autonomy, security, freedom, transparency, justice and equality as a central value of liberal democratic societies.<sup>3</sup>

But what value does privacy have for democratic societies in the current "age of information." Do we need to reconceptualize privacy when hundreds, perhaps thousands, of companies are constructing gigantic databases of peoples' psychological profiles and amassing data about their race, gender, income, hobbies, and purchases? As the legal scholar Daniel Solove notes, companies are assembling and analyzing shards of data from our daily existence to "investigate backgrounds, check credit, market products, and make a wide variety of decisions affecting our lives."<sup>4</sup> Yet credit card companies, Internet retailers, and food stores are not the only ones creating massive databases of personal information. Biomedical and health services researchers, government service providers, as well as law enforcement and national security agencies are also collecting vast amounts of information about individuals to be stored, analyzed, and shared. Moreover, in addition to collecting traditional information about people – such as their names, birthdates, race, gender, and place of residence – governments and private entities are increasingly collecting various types of "bioinformation" like fingerprints, iris and facial images, and DNA.

Privacy and data protection laws that govern the collection and use of personal information are based on the framework of "fair information principles." Although there are slight variations in how these principles have been articulated, legislation and regulations typically reflect the approach recommended in 1980 by the Organization of Economic Co-Operation and Development (OECD): collection limitation, data quality, purpose specification, use limitation, security, openness, individual participation, and accountability. Thus, the collection, use, and sharing of personal information based on fair information principles means that information is not "up for grabs"; instead, there are norms governing how much information is collected, what type of information is collected, and who has access to that information.<sup>5</sup> According to philosopher Helen Nissenbaum, when norms of information

collection and sharing are respected, “contextual integrity is maintained.” When those norms are not respected, “contextual integrity has been violated.”<sup>6</sup> Thus, for Nissenbaum, “contextual integrity ties adequate protection for privacy to norms of specific contexts, demanding that information gathering and dissemination be appropriate to that context and obey the governing norms of distribution within it.”<sup>7</sup>

Conceptualizing privacy from the perspective of contextual integrity has intuitive appeal. As Nissenbaum notes, “people do not object to providing to doctors . . . the details of their physical condition, discussing their children’s problems with their children’s teachers” or “divulging financial information to loan officers at banks.”<sup>8</sup> And “even if information is quite personal or intimate,” she says, “people generally do not sense their privacy has been violated when the information requested is judged relevant to, or appropriate for, a particular setting or relationship.”<sup>9</sup> Yet both the concept of “privacy as contextual integrity” and the more encompassing framework of “privacy as fair information principles” may not be adequate norms for privacy protection when governments collect and share personal information for security purposes. Indeed, it’s difficult to know if governments adhere to fair information principles or contextual integrity in the security context because secrecy is often a hallmark of security. Moreover, as Solove points out, “far too often, the balancing of privacy interests against security interests takes place in a manner that severely shortchanges the privacy interest while inflating the security interests.”<sup>10</sup>

## **HASTINGS CENTER POLICY FORUM ACTIVITIES**

The Hastings Center initiated the Policy Forum on Privacy as Contextual Integrity by conducting extensive research on the topics of informational privacy and electronic data sharing. Based on this research, a background document that included an essay, a bibliography, and a list of questions was developed and posted on the HIDE website prior to the face-to-face meeting, which was held 5-6 July 2009 in Prague, Czech Republic. The agenda for the face-to-face meeting was developed in close cooperation with Emilio Mordini, the leader of the HIDE project. International experts from national data protection organizations, academia, government agencies, bioethics commissions, think tanks, and vendor organizations participated in the face-to-face meeting.

The following individuals were speakers at the face-to-face meeting:

- *Pēteris Zilgalvis, JD, Head of Unit Governance and Ethics, Directorate Research, European Commission: Privacy Related Research Issues under the Science in Society Programme*
- *Maurizio Salvi, PhD, Bureau of Policy Advisors of the President of the European Commission and Secretary of the European Group of Ethics: Relevance of EU Policies to Data Sharing*
- *Harold Edgar, LLB, Julius Silver Professor in Law, Science, and Technology, Columbia Law School, USA: Privacy in the US Context*
- *Jiří Maštálka, expert of the International Department, The Office for Personal Data Protection, Czech Republic: Privacy and Data Protection in the Czech Republic*
- *Paul Ivory, Program Manager, Irish Council for Bioethics: Biometrics: Enhancing Security or Invading Privacy? Opinion*
- *Antoinette Rouvroy, PhD, Information Technology and Law Research*

*Centre: Epistemological and Political Dimensions of Privacy*

- *Thomas H. Murray, PhD, The Hastings Center: Privacy as Contextual Integrity*
- *Mats Hansson, PhD, Centre for Bioethics at Karolinska Institute & Uppsala University: Health Research and Medical Databanks*
- *Hugh Whittall, Director, Nuffield Council on Bioethics: DNA Databanks for Law Enforcement/National Security*

In addition to the speakers, the other participants at the meeting included:

- Jean Claude Ameisen, French National Ethics Committee
- Valeria Balestrieri, CSSC
- Wieslaw Bicz, Optel
- Alastair Campbell, Centre for Biomedical Ethics, National University of Singapore
- Nicolas Delvaux, Sagem
- Simon Dobrišek, University of Ljubljana
- Wendy Drozenova, Bioethical Commission, Czech Republic
- Eugenijus Gefenas, Vilnius University
- Katja Jacobsen, CESAGEN
- Josef Kure, Masaryk University
- Karen Maschke, The Hastings Center
- Jacob Moses, The Hastings Center
- Emilio Mordini, CSSC
- Linda Nielsen, EGE
- Lisbeth W. Nielsen, Centre for Biomedical Ethics, National University of Singapore
- Karolina Owczynnik, Zuyd University (INM)
- Jan Pague, Charles University, Prague
- Antoinette Rouvroy, FNRS – CRID – University of Namur
- Michael Thieme, IBG
- Anne Cambon Thomsen, INSERM
- Renata Veselska, Masaryk University

The Policy Forum's activities after the face-to-face meeting shifted to the on-line environment. A summary of the meeting, links to the background readings, and the participation list was posted on the Policy Forum website. Future activities will include enhancing the Policy Forum's online forum, as well as networking with privacy, data protection, and other key stakeholders who could not attend the face-to-face meeting. The Policy Forum will inform stakeholders about international activities, policies, and reports related to biometrics, privacy and data protection and regularly encourage stakeholders to participate in HIDE's online forums.

## **KEY ISSUES RAISED AND QUESTIONS FOR FURTHER INQUIRY**

Privacy means different things to different people. The concept has been defined as the right to be let alone; the right to control access to one's body and information; and the realm of intimate decisions about the self and one's control over that realm. Privacy is not only about the physical dimension, but also about the exercise of power over individuals and their bodies. One way to conceptualize privacy is to define it as something very basic, constituent in our

biology, in how our brain works. We need privacy as a negative right – something based on the notions of individual and democratic liberties.

The threat to privacy posed by biometric technologies is not about the technology per se, but about how it's applied. When their personal information is collected, stored, and shared, people are concerned about function creep, large data bases, and the use of data bases for profiling purposes. But is privacy the same thing as data protection? What is it we are trying to protect when we talk about data protection?

Europe is further ahead of the US in thinking about how data and the flow of information should be regulated. In the US, the privacy structure is not well formulated. It is segmented by subject area (e.g., education, medicine, etc.) and characterized by a patchwork of state and federal statutes, regulations, and judicial case law.

In the context of biobanks for research, an expansive view of individual autonomy would permit people to give broad consent for research with their biospecimens and associated data. Yet in the context of law enforcement, there should be limitations on the collection, use and storage of DNA samples and greater transparency regarding law enforcement DNA databases. Claims about the need for DNA samples for law enforcement purposes should be evidence-based, which ties in with the need for proportionality. In the UK, for example, having a larger DNA database hasn't actually led to a justifiable improvement in hits that lead to matches and then to convictions.

There is constant tension between the needs of law enforcement and national security and the right to privacy. For example, there are legitimate circumstances when homeland security and law enforcement officials cannot obtain informed consent to collect and use personal information. However, governance mechanisms need to be in place to ensure that the public knows what data are being collected and for what purposes, particularly when biometric technologies are used to collect, store, and share bioinformation like fingerprints and DNA samples. Proportionality is a key imperative to ensure that the use biometric applications is justifiable. When considering privacy concerns and biometric technologies, it may be useful to consider whether privacy and biometrics is agent-related, interest-related, or whether it is agent-neutral (protects others, family members, or a structure of power in society).

When considering privacy in the context of national security, is security a value, or is it a fundamental right? Is it important to distinguish between biometrics for security purposes and other ones? In the context of national security, the veil of secrecy makes it difficult to evaluate the legitimacy and proportionality of data collection. Yet, government secrecy may undermine the values that are central to the proper functioning of liberal, democratic societies.

---

<sup>1</sup> Moore, Adam D. Toward informational privacy rights, *San Diego Law Review* 2007;44, p. 816.

<sup>2</sup> Moore, p. 818.

<sup>3</sup> 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*, Quebec, Canada, 2008.

<sup>4</sup> Solove Daniel J. *The Digital Person: Technology and Privacy in the Information Age*. New York and London: New York University Press, p. 2.

<sup>5</sup> Nissenbaum Helen. Protecting privacy in an information age: the problem of privacy in public. *Law & Philosophy* 1999;17:559-596.

---

<sup>6</sup> Nissenbaum Helen, “Privacy as contextual identity,” *Washington Law Review*, 2004;79(1).

<sup>7</sup> Nissenbaum, 1999.

<sup>8</sup> Nissenbaum, 1999.

<sup>9</sup> Nissenbaum, 1999.

<sup>10</sup> Solove Daniel J. “I’ve Got Nothing to Hide” and other misunderstandings of privacy. *San Diego Law Review* 2007;44:745, p. 772.