



DIALOGUE

Volume 2 • No. 6 | 2009 September

POLICY FORUM REPORT

Policy Forum on Privacy as Contextual Integrity

IN THIS ISSUE

- 1 *Policy Forum Report*
Policy Forum on Privacy as Contextual Integrity
- 3 *Workshop Report*
Data Sharing and Biometrics: Asian and International Contexts
- 7 *News and Notes*
- 8 *Partner Profiles*
The Hastings Center

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 Karen J. Maschke, The Hastings Center

One of the HIDE project's areas of focus is the theme of privacy as contextual integrity. Various privacy contexts and the implications for data protection were discussed at a policy forum meeting The Hastings Center hosted on July 5–6, 2009, in Prague, Czech Republic. 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 concept of privacy pervades 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."¹ 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."² Moreover, many commentators contend that privacy joins autonomy, security, freedom, transparency, justice, and equality as

“According to Nissenbaum, when information collection and sharing norms are respected, contextual integrity is maintained; when they are not, it is violated.”

a central value of liberal democratic societies.³

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

CONTINUES ON PAGE 2



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.”⁴ 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, and law enforcement and national security agencies are also collecting vast amounts of information about individuals to be stored, analyzed, and shared. And in addition to collecting traditional information about people—such as their names, birthdates, race, gender, and places of residence—governments and private

“A key theme of the meeting is that the threat to privacy posed by biometric technologies is not about the technology per se, but about how it’s applied.”

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.⁵ 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.”⁶ 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.”⁷

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.”⁸ 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.”⁹ Yet neither the concept of “privacy as contextual integrity” nor the more encompassing framework of “privacy as fair information principles” may 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.”¹⁰

Key Issues and Questions for Further Inquiry

Several speakers and participants noted that privacy is not only about the physical dimension, but also about the exercise of power over individuals and their bodies. Antoinette Rouvroy suggested that 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.

Another key theme of the meeting is that 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 databases, and the use of databases 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? Several participants pointed out that Europe is further ahead of the United States in thinking about how data and the flow of information should be regulated. For instance, keynote speaker Harold Edgar emphasized that the U.S. privacy structure is not well formulated; is segmented by subject area (e.g., education, medicine, etc.); and is characterized by a patchwork of state and federal statutes, regulations, and judicial case law.

In his presentation on biobanks for research, Mats Hansson supported an expansive view of individual autonomy so that people could give broad consent for research with their biospecimens and associated data. Yet Hugh Whittall and others pointed out that 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 United Kingdom,



WORKSHOP REPORT

Data Sharing and Biometrics: Asian and International Contexts

By Lisbeth Witthøfft Nielsen, National University of Singapore

In July, HIDE Partner Centre for Biomedical Ethics (CBmE) of the National University of Singapore hosted the problem-solving workshop, “International Data Sharing and Biometric Identification—the Ethical Issues in an Asian and International Context,” in Singapore City, Singapore. The one-and-a-half day workshop was the first of two HIDE problem-solving workshops that aim to identify meaningful steps toward resolution of complex problems. The workshops take an analytical approach by creating a forum for experts from different disciplines in which speakers and participants are asked to explain their own perspectives and to engage in a dialogue, rather than a debate.

This first problem-solving workshop had two goals: to identify and discuss the ethical and legal challenges the privacy framework adopted by the Asia-Pacific Economic Cooperation (APEC Privacy Framework) poses for the EU Data Protection Directive, and to identify and discuss the potential value conflicts relating to key concepts such as privacy, security, and identity in an Asian as well as an international context. With these goals in mind, the workshop sessions were organized around four main themes: 1) international data sharing; 2) privacy vis-à-vis security; 3) privacy and the right to an identity; and 4) rights and ethics with regard to personal data and the human body.

In the opening lecture, Ruth

Chadwick addressed issues around standardization, harmonization, and ethics in international data sharing. She outlined three models for harmonization of ethics: the human rights model, the necessary conditions model, and the cultural dialogue model. Chadwick contended that harmonization with respect to ethical issues around privacy protection should be seen as an ongoing process of dialogue where existing values can also be challenged. During the rest of the workshop, the speakers and participants identified five cross-cutting themes and offered suggestions for small-step solutions.

Identifying Ethical Issues from a Privacy or Dignity Perspective

Workshop participants pointed out the challenge of trying to interpret the concept of privacy in relation to implementation of the EU Data Protection Directive and the APEC framework. There was an extended discussion about whether the concept of dignity would be more useful when examining the ethical issues related to biometric technologies applied for security purposes. Another question raised was whether privacy is to be interpreted as a right within the context of the EU Directive on Data Protection. In this context

Emilio Mordini argued that a legal framework that interprets privacy protection more as a right to privacy defined in terms of human dignity will present a higher level of protection in a data-sharing context. From the various discussions it became

“Continuous dialogue is important to help identify and understand cultural and regional differences in the way basic concepts such as privacy are addressed.”

clear that more attention should be given to considerations about what privacy protection policies should entail and what data need to be protected from whom. Malcolm Crompton argued that there is a need for addressing issues normally associated with privacy protection in a more positive light, taking improved security and improved privacy as the goals. He argued in favor of dropping the word “privacy” and instead using terms such as dignity, control, and trust. Workshop participants generally agreed that privacy is too complex a notion to use as an ethical foundation for an evaluation of the values at stake. The idea of dignity as a foundation for evaluation was not present-

CONTINUES ON PAGE 5

Policy Forum Speakers

- Harold Edgar
Columbia Law School
- Mats Hansson
Uppsala University
- Paul Ivory
Irish Council for Bioethics
- Jirí Maštálka
*Office for Personal Data Protection,
Czech Republic*
- Thomas H. Murray
The Hastings Center
- Antoinette Rouvroy
Université de Namur
- Maurizio Salvi
*Bureau of Policy Advisors of the President
of the European Commission*
- Hugh Whittall
Nuffield Council on Bioethics
- Pēteris Zilgalvis
European Commission

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, participants noted that governance mechanisms should 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 of biometric applications is justifiable. When considering privacy concerns and biometric technologies, it may be useful to consider whether privacy and biometrics are agent-related, interest-related, or whether they are agent-neutral (i.e., protect others, family members, or a power structure in society).

When considering privacy in the context of national security, participants asked, is it appropriate to conceptualize privacy as a fundamental right or as a value? They also wondered whether, when developing privacy and data protection policies, it is important to distinguish between biometrics used for security purposes and biometrics used for other purposes.

And finally, several pointed out that in the national security context, the veil of secrecy makes it difficult to evaluate the legitimacy and proportionality of data collection, and that government secrecy may undermine the values that are central to the proper functioning of liberal, democratic societies.

Background readings and other materials are available at http://www.hideproject.org/events/pf-contextual_integrity.html

1. Moore AD. Toward informational privacy rights. *San Diego Law Review* 2007;44:816.
2. Moore, p. 818.
3. 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: Government du Québec, 2008).
4. Solove DJ. *The Digital Person: Technology and Privacy in the Information Age* (New York: New York University Press, 2004), 2.
5. Nissenbaum H. Privacy as contextual identity. *Washington Law Review* 2004;79(1):101-139, p. 120.
6. Nissenbaum H. Protecting privacy in an information age: The problem of privacy in public, 2000, <http://www.nyu.edu/projects/nissenbaum/papers/privacy.pdf>.
7. Nissenbaum, 2004, p. 120.
8. Nissenbaum, 2000, p. 20.
9. *Ibid.*, p. 22.
10. Solove DJ. "I've got nothing to hide" and other misunderstandings of privacy. *San Diego Law Review* 2007;44:745.

ed as a *solution* to the problem, but as a concept that might be more useful.

Identity Interpreted as Individuality or Uniqueness

How one is to understand the notion of identity was specifically addressed by the presentations in the third session. Using an ethical rationalist approach (that of Alan Gewirth) Roger Brownsword argued that from a perspective of purposive agency, one can construct an idea of generic rights, but that a right to identity cannot be justified as a generic right. This led to a discussion on whether identity should be interpreted in terms of rights. Alastair Campbell argued from the idea of a right to a nonreduced identity or a right to a complexity of identities. In this context Eric Yap highlighted the fact that technology is not necessarily a threat—it can also enrich individu-

ality, and one should keep in mind that genetic features already make the individual unique. Although the participants disagreed on whether the notion of identity should be interpreted in terms of rights, it was clear from the discussion that more attention should be paid to the issue of identity and how this relates to protection of privacy in the context of biometrics.

Transparency, Public Perceptions of Privacy, and Democratic Decision-Making

This theme arose in the second session in relation to the discussion on preventive and reactive policing. Several participants emphasized that just because the public may express different notions about the meaning of privacy doesn't mean that privacy is no longer considered a value that needs protection. Participants also emphasized the importance of transparency and public involvement in political decisions regarding security measures that involve the collection and sharing of personal data. Several of the participants argued that it is far from feasible to reach an agreement internationally on "the right thing to do" in terms of international data sharing and regulations on biometrics, as one has to take into account that there are many interests (e.g., political, financial, and public) involved in the policy-making process. There was general agreement of the need for more debate on the various interests at stake in the policy-making process, as well as for more attention on public perceptions of privacy and how this intersects with public policy.

Finding Common Ground for Identification of the Human Interests at Stake

A general theme throughout the workshop was how best to find a common ground for identifying the human interests at stake in relation to data-sharing—and, more specifically, in relation to biometric identification. Bénédicte Havelange and others argued for developing a framework that addresses data protection in rela-

tion to collecting and sharing biometric data, since biometric data differs from other types of data in that it directly involves the body. Central to this context are the differences in the human-rights-based approach of the EU Data Protection Directive and the pragmatic approach of the APEC Privacy Framework. There was general agreement that in terms of working toward harmonizing data protection policies, a multiple-track approach is needed that can take into account the underlying differences in interpretations of concepts such as privacy, dignity, and identity. Emilio Mordini argued that judging from the discussion during the workshop, it is unlikely that a common ground for identification of human interests with regard to issues of privacy protection can be found in either the notion of dignity or personality. As an alternative, he suggested liberty as a key notion that might be used as a common starting point for evaluating questions regarding security and privacy.

Dialogue as a Model for Progress Toward Harmonization

The workshop confirmed that dialogue is important to help identify and understand cultural and regional differences in the way basic concepts such as privacy are addressed. Both Ruth Chadwick's opening lecture and Bénédicte Havelange's presentation in the first session addressed issues around harmonization. It was clear from the discussion that workshop participants agreed on the need for more harmonization. There was also agreement that ethics and the further development of legal frameworks in an international context should work hand-in-hand to ensure that process of harmonizing and standardizing data-sharing does not compromise the protection of personal data.

Another point on which all agreed was that larger ethical and legal challenges regarding international data-sharing stem from differences in interpreting the concept of privacy. Several speakers emphasized that

Workshop Speakers

- Abu Bakar Bin Munir
University of Malaya, Malaysia
- Roger Brownsword
King's College
- Ruth Chadwick
Cesagen
- Malcolm Crompton
Information Integrity Solutions P/L
- Vinayak Godse
Data Security Council of India
- Michael Hardin
U.S. Department of Homeland Security
- Jim Harper
Cato Institute
- Bénédicte Havelange
Office of the European Data Protection Supervisor (EDPS), Belgium
- Colin Minihan
Department of the Prime Minister and Cabinet, Australia
- Terence Sim
National University of Singapore
- Tom Sorell
University of Birmingham
- David Zhang
Hong Kong Polytechnic University
- Eric Yap
DSO National Laboratories and Ministry of Defense, Singapore

some of the values associated with privacy in a Western context are not as important in some Asian countries, and Malcolm Crompton pointed out that the concept has different meanings across languages. In addition, Vinayak Godse and Abu Bakar Bin Munir noted that cultural and social contexts shape values associated with privacy, and that sharing personal data may not necessarily be seen as a problem in some Asian countries.

Alastair Campbell, referring to the many disciplines represented at the workshop, stressed the importance of

dialogue in an area that is not only ethically and politically sensitive, but that also entails discussing data and data-sharing in different ways depending on the discipline from which the issues are approached.

The workshop revealed that the greatest challenge in trying to harmonize differing data protection frameworks lies in finding a way to foster fruitful dialogue on the issues that pertain to protecting people's personal information. Whether this can happen by encouraging more dialogue about what privacy means, by turn-

ing to other contexts in which privacy is discussed, or by turning to different concepts when interpreting existing legal rights was left as an open question.

This short workshop report is based on the more exhaustive report of the workshop, outlined session for session. The full workshop report, including all the material from the workshop (abstracts, Powerpoint presentation slides, short biographies for speakers etc.), is available at <http://www.hideproject.org/events/workshops.html>.

HIDE Past Events

- **17–18 September 2009**
HIDE Workshop on Restrictions in the Implementation of EU Data Protection Directive for Public Interest, Security and Defense, Ljubljana, Slovenia
- **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
- **5–6 June 2009**
Policy Forum on Privacy as Contextual Integrity, Prague, Czech Republic
- **4 March 2009**
Policy Forum on Body Issues, Brussels, Belgium
- **6 February 2009**
Policy Forum on Outsourcing of Systems for Detection, Identification, and Authentication, London, UK
- **31 October 2008**
Embedded Technology Focus Group, Maastricht, the Netherlands
- **15 September 2008**
System Interoperability Focus Group, London, UK
- **9 September 2008**
Technology Convergence Focus Group, Paris, France

HIDE Upcoming Events

- **16 October 2009**
Focus Group Meeting on Privacy Enhancing Technologies, Manchester, UK
- **7 December 2009**
Focus Group Meeting on System Interoperability, London, UK
- **29 January 2010**
Focus Group Meeting on Embedded Technology, Maastricht, the Netherlands

For more details, visit www.hideproject.org.

Other Upcoming Events

- **4–6 November, 2009**
31st International Conference of Data Protection and Privacy Commissioners, Madrid, Spain

Recent Publications

- European Data Protection Supervisor. Area of freedom, security and justice: EDPS calls for strong emphasis on fundamental rights in future Stockholm Programme. Press release. 13 July 2009.
<http://europa.eu/rapid/pressReleasesAction.do?reference=EDPS/09/8&format=HTML&aged=0&language=EN&guiLanguage=en>
- Information and Privacy Commissioner, Ontario, Canada, and European Biometrics Group. The relevance of untraceable biometrics and biometric encryption: A discussion of biometrics for authentication purposes. August 2009.
<http://www.ipc.on.ca/images/Resources/untraceable-be.pdf>
- Irish Council for Bioethics. Biometrics: Enhancing security or invading privacy? Proceedings of the Irish Council for Bioethics Conference, 26 November 2008, Dublin. 2009.
http://www.bioethics.ie/uploads/docs/Biometrics_Conference_Final.pdf
- Nissenbaum H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Palo Alto, CA: Stanford University Press, 2009.

PARTNER PROFILES

THE HASTINGS CENTER



The Hastings Center is an independent, nonpartisan, and non-profit bioethics research institute founded in 1969. Its mission is to address fundamental ethical issues in the areas of health, medicine, and the environment as they affect individuals, communities, and societies. To achieve this mission, the Center has established four goals: to pursue interdisciplinary research and education that includes both theory and practice; to engage a broad audience of thoughtful people in the Center's work; to collaborate with policy-makers to identify and analyze the ethical dimensions of their work; and to strengthen the international dimensions of the Center's work.

Much of the Center's research addresses bioethics issues in three broad areas: care and decision-making at the end of life, public health priorities, and new and emerging technologies. The Center draws on a worldwide network of experts, including an elected association of leading researchers influential in bioethics called Hastings Center Fellows. Research is carried out by interdisciplinary teams that convene to frame and examine issues that inform professional practice, public conversation, and social policy.

The *Hastings Center Report* and *IRB: Ethics & Human Research* bring the best scholarship and commentary in bioethics to members and other readers worldwide. Center research scholars direct research projects, write and speak on a variety of topics, serve as consultants, and assist members of the press. Intellectual life at the Center is enhanced by a visiting scholars program and a research library. Research grants, charitable contributions, and income from a modest reserve fund support the Center's work.

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