



POLICY FORUM ON PRIVACY AS CONTEXTUAL INTEGRITY

**PF COORDINATOR:
THE HASTINGS CENTER**

DATE: 5-6 JUNE 2009

PLACE: PRAGUE

.....H.Y<c]XU:bbDFU[i Y7cb[fYgg7YbdfY

CONTENTS:

.....

..... d%

% "6UM[fci bX8cWa Ybh d"

&" "6UM[fci bXFYUX]b[gZcf=bficXi VbfmubXQ Yfj]Mk G/gg]cbgž d+

..... f]XUž) ž by8\$\$

' "' "6UM[fci bXFYUX]b[gZcfK cf_g]cdG/gg]cbgž d,

..... GUh fXUž) ž by"

("' "6UM[fci bXEi Ygf]cbgZcfK cf_g]cdG/gg]cbHkc d%\$

..... Dc]MkOd]cbgZcf Dfj UMMfchVM]cbžGUh fXUž) ž by"

) "' FYZfYbWg7]YX d&



THE
HASTINGS
CENTER

HIDE Policy Forum on Privacy as Contextual Integrity

June 5 - 6, 2009

The Holiday Inn Prague Congress Centre

Prague, Czech Republic

AGENDA

Friday, June 5

1:30 – 1:40

Opening Session of Policy Forum: Welcome and Introductions

- *Thomas H. Murray, PhD, The Hastings Center*
- *Emilio Mordini, MD, DPhil, Center for Science, Society and Citizenship*

1:40 – 2:10

Introductory Comments

- *Maurizio Salvi, PhD, Bureau of Policy Advisors of the President of the European Commission and Secretary of the European Group of Ethics*
- *Pēteris Zilgalvis, JD, Head of Unit Governance and Ethics, Directorate Research, European Commission*

2:10 – 2:15

Framing Themes: Democracy, Security, Surveillance, Public/Private Spheres

Introductory Comments

Thomas H. Murray, PhD, The Hastings Center

2:15 – 3:15

Keynote Presentation and Discussion

Harold Edgar, LLB

Julius Silver Professor in Law, Science, and Technology

Columbia Law School

3:15 – 4:30

Roundtable Discussion: Perspectives on Privacy

Jiří Maštalka, expert of the International Department, The Office for Personal Data Protection, Czech Republic

Paul Ivory, Program Manager, Irish Council for Bioethics

Antoinette Rouvroy, PhD, Information Technology and Law Research Centre

Moderator: Karen Maschke, PhD, The Hastings Center

4:30

Reception

Saturday, June 6

9:00 – 9:30

Introduction to Forum Theme, Overview of Format, and Introductions

Thomas Murray, PhD, The Hastings Center

Session One: When Biometrics Meets Bioethics

- 9:30 – 10:00 **Health Research & Medical Databanks**
Mats Hansson, PhD, Centre for Bioethics at Karolinska Institute & Uppsala University
- 10:00 – 10:30 **Moderated Discussion**
Moderator: Thomas Murray
- 10:30 – 10:45 Coffee/Tea Break
- 10:45 – 11:15 **DNA Databanks for Law Enforcement/National Security**
Hugh Whittall, Director, Nuffield Council on Bioethics
- 11:15 – 12:00 **Moderated Discussion**
Moderator: Karen Maschke
- 12:00 – 1:15 Lunch

Session Two: Policy Options for Privacy Protection

- 1:15 – 3:45 Moderated Working Session/Discussion
(break 2:45 – 3:00) *Moderator: Thomas Murray*

Reports and recommendations for discussion:

- Rand Europe. *Review of the European Data Protection Directive*, 2009.
- Home Office (UK). *Keeping the Right People on the DNA Database. Science and Public Protection*, 2009.
- House of Lords, Select Committee on the Constitution, *Surveillance: Citizens and the State*, 2nd Report of Session 2008-09, Volume 1.
- House of Commons, Home Affairs Committee. *A Surveillance Society?* Fifth Report of Session 2007-2008, Volume 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*, Quebec, Canada, 2008.
- Nuffield Council, *The Forensic Use of Bioinformation: Ethical Issues*, 2007.

- 3:45 – 4:00 **Policy Forum Follow-up Activities**
Online Tools, Other Resources, and Wiki Policy Paper
- 4:00 **Adjourn**

HIDE Policy Forum: Privacy as Contextual Integrity

Background Document

Karen J. Maschke, PhD and Jacob Moses

The Hastings Center

1. Introduction

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. Privacy has been defined as

- "the right to be let alone,"¹
- an extension of one's personality or personhood,²
- four related torts: intrusion, private facts, false light, and appropriation,³
- the right to control access to bodies and information,⁴
- "the condition of not having undocumented personal knowledge about one possessed by others,"⁵
- "the state of possessing control over a realm of intimate decisions, which includes decisions about intimate access, intimate information, and intimate actions,"⁶
- whatever "is not, according to a reasonable person in normal circumstances, the legitimate concern of others."⁷

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."⁸ 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 well-being."⁹ Moreover, many commentators contend that privacy joins autonomy, security, freedom, transparency, justice and equality as a central value of liberal democratic societies.¹⁰

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."¹¹ 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.

Whether you know it or not, your bioinformation may be in an electronic database that is interconnected to databases in Europe, the US and elsewhere that contain other personal information about you. Maybe the source of your bioinformation is a fingerprint you gave to the military when you served in one of the armed forces, or a hand print you gave to an employer to get access to the company’s computer network. If you’ve been to London or New York City, video cameras recorded your face and physical movements when you walked throughout those cities and when you entered and exited subway stations, parks, and buildings. Maybe your iris image or fingerprint is stored in a computer chip embedded in a biometric smart card that you use for quick identify verification at special airport security lanes. Or maybe your genetic information obtained from a DNA sample you gave to researchers is in a genetic database that researchers from around the world will have access to. And if you were ever near or at a crime scene, the police might have collected traces of your DNA and stored the information in a forensic DNA bank.

Not only is the amount of traditional and bioinformation being collected staggering, so is the constant transmission of information within and across national borders. Moreover, information no longer flows from a single source or flows from that source in a one-directional or multi-directional manner. Today, information flows from multiple data providers in a complex, globally interconnected network of data sharing.

Public opinion polls in the US and Europe indicate that people are concerned about who is collecting information about them and what they are doing with it. Many people have concerns about being harmed by the disclosure and use of their personal information. They worry that their “identity” will be stolen and used by others to obtain money from their bank accounts and to purchase items with their credit cards; that companies are buying and selling their personal information to develop and sell products; and that law enforcement and other government agencies are collecting personal information to track and monitor peoples’ activities for political or nefarious purposes. Thus, many countries have enacted data protection laws that govern the collection and use of personal information. Member states of the European Union (EU) enacted national laws in response to requirements of the 1995 EU Data Protection Directive.¹² Unlike in Europe and elsewhere, the US does not have a comprehensive national privacy law or a national privacy commissioner empowered to implement and enforce the law. Instead, the US

has several federal privacy laws that cover various issues (such as education, credit, and telecommunications, etc.) and a patchwork of state privacy laws.

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 (Box 1). 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.¹³ 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.”¹⁴ 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.”¹⁵

Box 1. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data¹⁶

- **Collection Limitation.** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data quality principle.** Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
- **Purpose specification.** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- **Use limitation principle.** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
 - with the consent of the data subject; or
 - by the authority of law.
- **Security safeguards principle.** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
- **Openness principle.** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of

personal data, and the main purposes of their use, as well as the identity about usual residence of the data controller.

- **Individual participation principle.** An individual should have the right:
 - to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
 - to have communicated to him, data relating to him
 - within a reasonable time;
 - at a charge, if any, that is not excessive;
 - in a reasonable manner; and
 - in a form that is readily intelligible to him;
 - to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
 - to challenge data relating to him and, if the challenge is successful, to have the data erased; rectified, completed or amended.
- **Accountability principle.** A data controller should be accountable for complying with measures which give effect to the principles stated above.

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.”¹⁷ 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.”¹⁸ 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.”¹⁹

When secrecy is a hallmark of security, who ensures that the norms of information gathering and sharing – i.e, contextual integrity – in the security context are maintained? Put another way, who governs information collection, analysis, and flow in the security context? In addition to these questions, the face-to-face meeting of the HIDE Forum on Privacy as Contextual Integrity will address several others: Are the concerns that people raise about their personal information really privacy concerns, or are they concerns about something else? Why are people concerned about the collection and sharing of medical and health data in the research context? Why are they concerned about law enforcement agencies collecting DNA samples to combat crime if “they have nothing to hide?”²⁰ What is the impact on privacy interests and democratic values when

government information gathering becomes a form of surveillance? Do national privacy and data protection laws and policies adequately protect privacy and other democratic values, particularly when they include exceptions for security purposes?

2. Background Readings for Introductory and Overview Sessions, Friday, 5 June 2009

2.1. Framing Themes: Democracy, Security, Surveillance, Public/Private Spheres

Froomkin, M. "The Death of Privacy," *Stanford Law Review*, Vol. 52, 2000, pp. 1461-1543.
<http://osaka.law.miami.edu/~froomkin/articles/privacy-deathof.pdf>

Hansson, Mats G., *The Private Sphere: An Emotional Territory and Its Agent*, Dordrecht: Springer, 2007. Partial Introduction available at:
<http://books.google.com/books?id=rXj17LFDUfcC>

Liberatore A, "Balancing Security and Democracy, and the Role of Expertise: Biometrics Politics in the European Union," *European Journal on Criminal Policy and Research*, Vol. 13, No. 1-2, 2007, pp. 109-137.
<http://www.springerlink.com/content/h2876230167p9t85/>

Marx, Gary T., "Murky Conceptual Waters: The Public and the Private," *Ethics and Information Technology*, Vol. 3, No. 3, 2001, pp. 157-169.
<http://web.mit.edu/gtmarx/www/murkypublicandprivate.html>

Mordini E., "Nothing to Hide: Biometrics, Privacy and Private Sphere," in *Biometrics and Identity Management*, ed. Schouten, B., N. C. Juul, A. Drygajlo and M. Tistarelli, New York: Springer, 2008.
<http://www.springerlink.com/content/q318640j4v1112n3/>

Nissenbaum H. "Protecting Privacy in the Information Age: The Problem of Privacy in Public," *Law & Philosophy*, Vol. 17, No. 7, 1998, pp. 559-596.
<http://www.nyu.edu/projects/nissenbaum/papers/privacy.pdf>

Solove D. J., "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy," *San Diego Law Review* Vol. 44, 2007, pp. 745.
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565

Surveillance Studies Network, *A Report on the Surveillance Society*, 2006.
http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf

2.2 Disciplinary and Philosophical Perspectives on Privacy

Cohen, J. E., "Privacy, Visibility, Transparency, and Exposure," *University of Chicago Law Review* Vol. 75, No. 1, 2008, pp. 181-201.

http://lawreview.uchicago.edu/issues/archive/v75/75_1/Cohen.pdf

deHert, P., "Biometrics: Legal Issues and Implications," Background paper for the Institute of Prospective Technological Studies, DG JRC, Sevilla: European Commission, 2005.

http://cybersecurity.jrc.ec.europa.eu/docs/LIBE%20Biometrics%20March%2005/LegalImplications_Paul_de_Hert.pdf

Rouvroy, A., "Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence." *Studies in Ethics, Law, and Technology*, Vol. 2, No. 1, 2008.

<http://www.bepress.com/selt/vol2/iss1/art3/>

Solove, D. "Conceptualizing Privacy," *California Law Review*, Vo. 90, 2002, pp. 1087-1155.

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=313103

Westin, A. F., "Social and Political Dimensions of Privacy," *Journal of Social Issues*, Vol 59, No. 2, 2003, pp. 431-453.

<http://www3.interscience.wiley.com/journal/118833375/abstract>

3. Background Readings for Workshop Sessions, Saturday, 6 June 2009

3.1 Privacy and Health Research/Medical Databanks

Electronic Privacy Information Center. Medical Privacy (US Perspectives).

<http://epic.org/privacy/medical/>

Singapore Bioethics Advisory Committee, *Personal Information in Biomedical Research*, 2007.

<http://www.bioethics-singapore.org/uploadhtml/20745%20PMPI%20Report.html>

Parliamentary Office of Science and Technology, "Data Protection & Medical Research," *postnote* No. 235, London, 2005.

<http://www.parliament.uk/documents/upload/postpn235.pdf>

3.2 Privacy and DNA Databanks for Law Enforcement/National Security

Nuffield Council, *The Forensic Use of Bioinformation*, London: Nuffield Council, 2007.

<http://www.nuffieldbioethics.org/go/ourwork/bioinformationuse/introduction>

The National DNA Database. *Annual Report 2004-2005*, London: Home Office, 2006.

http://www.homeoffice.gov.uk/documents/NDNAD_AR_04_051.pdf

EU Court of Human Rights, Case 30562/04 *S and Marper v. the United Kingdom* [2008] ECHR 1518.

<http://www.bailii.org/eu/cases/ECHR/2008/1581.html>

UK Human Genetics Commission, *A Citizens' Inquiry into the Forensic Use of DNA and the National DNA Database*, 2008.

http://www.hgc.gov.uk/Client/news_item.asp?NewsId=101 (includes "Introduction by the HGC Working Group," "Citizens' Report," "Summary of Conclusions," "Contractor's Report," "Evaluation Report," and "Consultation Questions")

3.3 Policy Options for Privacy Protection

House of Lords, Select Committee on the Constitution, *Surveillance: Citizens and the State*, 2nd Report of Session 2008–09, Volume I: Report, HL Paper 18-1, London, 2009.

<http://www.parliament.the-stationery-office.com/pa/ld200809/ldselect/ldconst/18/1802.htm>

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.

<http://www.ethique.gouv.qc.ca/In-Search-of-Balance-An-Ethical.html>

House of Commons, Home Affairs Committee, *A Surveillance Society?* Fifth Report of Session 2007-2008, Volume 1, 2008.

<http://www.parliament.the-stationery-office.co.uk/pa/cm200708/cmselect/cmhaff/58/58i.pdf>

Institute for Prospective Technological Studies, *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview. A Report to the European Parliament Committee on Citizens, Freedoms and Rights, Justice and Home Affairs (LIBE)*, 2003.

<http://cybersecurity.jrc.ec.europa.eu/docs/LIBE%20STUDY/20823-ExeSummEN.pdf>

American Bar Association, Standing Committee on Law and National Security, "The Cantigny Principles on Technology, Terrorism, and Privacy," *National Security Law Report*, Vol. 27, No. 1, pp. 14-16, 2005.

http://www.abanet.org/natsecurity/nslr/2005/NSL_Report_2005_02.pdf

The National Research Council, Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, *Protecting Individual Privacy in the Struggle against Terrorists. A Framework for Program Assessment*.

http://books.nap.edu/catalog.php?record_id=12452#toc

UK Home Office, *Keeping the Right People on the DNA Database: Science and Public Protection*, 2009.

http://www.nio.gov.uk/consultation_paper_-_keeping_the_right_people_on_the_dna_database.pdf

Rand Europe, *Review of the European Data Protection Directive*, 2009.

http://www.rand.org/pubs/technical_reports/TR710/

4. Background Questions for Workshop Session Two: Policy Options for Privacy Protection, Saturday, 6 June 2009

Karen J. Maschke, PhD

The Hastings Center

The format will be a moderated working session/discussion. In addition to the material provided here, please review as much as possible the background documents listed below.

The questions listed here will serve as an introductory framework for the session. A more detailed set of questions and comments will be presented at the session.

- What are the privacy concerns that each report addresses? Are the concerns consistent across each report, or is there variation in how the concerns are raised and defined?
- Are there important issues the reports fail to address?
- Is “data protection” and “privacy protection” the same thing?
- Is the balancing approach neutral, or do attempts to “strike a balance” weigh some values and interests more favorably than others?
- What are the privacy concerns in the context of government collection and use of information? Is privacy the issue, or something else?
- What barriers might impede implementation of recommendations that are specific to the UK?
- What barriers might impede implementation of the recommendations for changes to the EU Data Protection Directive?
- Assuming there should be public trust in governments’ intentions regarding the collection and sharing of data, is public trust alone enough to justify the government’s intentions?
- If law enforcement and national security activities are exempt from statutory/regulatory data protection policies, what principles govern the collection and use of personal information in these contexts? Are adequate mechanisms in place to ensure that restrictions on liberty, autonomy, privacy, informed consent and equality are justifiable?

4.1 Nuffield Council on Bioethics. *The Forensic use of Bioinformation, 2007.*

Report's Key Themes and Observations

- Stresses that government needs to find a balance between protecting people from crime and protecting “certain ethical values, such as liberty, autonomy, privacy, informed consent and equality.”
- In trying to find balance, principle of proportionality should be used: “Any interference with legally enforceable human rights must be justified as being *proportionate* to the need to detect and prosecute offenders, and there must be evidence that the interference will be effective.”
- Emphasizes need to ascertain “best practice” within policing to maximize the crime control potential of bioinformation.
- Need for transparency and ethical oversight concerning research use of the DNA profiles and stored samples.

Recommendations

- It is proportionate for the police to take fingerprints and DNA without the need for consent from people arrested on suspicion of involvement in any recordable offence, but not minor non-recordable offences.
- Fingerprints, biological samples and DNA profiles should be retained indefinitely only for those convicted of a recordable offence.
- The DNA of people charged with serious violent or sexual offences could be kept for up to five years even if they are not convicted.
- People who provide the DNA voluntarily should be able to have the DNA removed from the NDNA database at any time without having to give a reason.
- Volunteers’ DNA should not be stored beyond the conclusion of the relevant case.
- At this time the establishment of a population-wide forensic DNA database cannot be justified. However, the possibility of establishing one should be subject to review as technology develops.
- Familial searching should not be used unless it is justified in each specific case.
- Public guidelines and safeguards for the use of familial searching should be developed.
- Ethnic inferences should not be sought, and where they are used they should be treated with great caution.
- Research proposals should be subjected to close ethical review and details about information about research use of the database should be published regularly.
- There should be a statutory basis for the regulation of forensic databases.
- When considering requests for the removal from storage of fingerprints and DNA taken from minors, there should be a presumption in favor of the removal and destruction of all records, samples and DNA profiles. In deciding whether or not the presumption should be rebutted, account should be taken of factors such as:

- the seriousness of the offence;
- previous arrests;
- the outcome of the arrest;
- the likelihood of this individual re-offending;
- the danger to the public; and any other special circumstances.

4.2 UK House of Commons, Home Affairs Committee, A Surveillance Society? Fifth Report of Session 2007 - 2008, Volume 1.

Report's Key Themes and Observations

- Rejects "crude characterizations of our society as a surveillance society in which all collections and means of collection information about citizens are networked and centralized in the service of the state."
- Points out, however, that "the potential for surveillance of citizens in public spaces and private communications has increased to the extent that ours could be described as a surveillance society unless trust in the Government's intentions in relation to data and data sharing is preserved. The Home Office in particular and Government in general must take every possible step to maintain and build on this trust: our Report provides a starting point."
- Although there are risks of surveillance, there also are benefits: to the consumer, to the patient and public health, to the citizen and society (e.g. delivery of better public services).
- Emphasis on public trust and balancing of risks and benefits.

Recommendations

- Information Commissioner should provide Parliament with an annual report on surveillance; Government should produce a response to the report and provide to Parliament.
- Parliament should hold an annual debate on the issue of surveillance.
- In general the Government should move to curb the drive to collect more personal information and establish larger databases.
- Need more standards, transparency, data minimization, and accountability regarding use of CCTV.
- Several actions recommended regarding the National Identity Scheme, including that the Home Office should explain the intended function of the Scheme for law enforcement purposes and explicitly state that the National Identity Register will not be used as a matter of routine to monitor individuals' activities
- Several actions recommended regarding the National DNA Database, including that the Home office, the National Policing Improvement Agency, and the police should work together to develop and observe a regulatory framework which protects individuals from unnecessary invasions of privacy and loss or unauthorized use of their genetic material and information gleaned from it.

- Several actions recommended regarding the Regulation of Investigatory Powers Act (RIPA), including that in its review of RIPA codes of practice the Home Office should take steps to raise public awareness of how and why communications data might be collected and used and undertake a public consultation on the levels of authorization which should be required for various surveillance activities and the purposes which would justify different levels of intrusion.

4.3 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, 2008.*

Report's Key Themes and Observations

- Focus on New Surveillance and Monitoring Technologies (NSMT's): biometric systems, video surveillance, and RFID.
- Believes that "risk societies," which are obsessed with "risks, threats and danger," and likely to embrace NSMT's as a way to gather information in an attempt to control risks
- Worries not about rise of "Big Brother," but about rise of many "Small Brothers" - resulting in privately conducted surveillance "which does not necessarily follow proper guidelines and sound practices [and] could fall completely beyond the control of the state."
- Emphasizes value of individual autonomy, as well as other fundamental democratic values: security, freedom, privacy, transparency, justice, and equality.

Recommendations

- 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.
- Guidelines should take into account ethical concerns with respect to fundamental democratic values.
- Use a consultative approach to advise the Government about its deployment of new surveillance and monitoring technologies, with particularly emphasis on areas that raise ethical issues using the criteria of relevance, effectiveness and reliability.
- Use the 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 the technologies.
- Make the results of the public consultation publicly available to sensitive the general public about the ethical issues associated with the new surveillance and monitoring technologies.

- Inform the public about 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 about the means for public participation in the decision-making, implementation and follow-up processes involved.
- Implement a compensation and correction mechanism for cases where the use of NSMT is prejudicial to individuals by wrongfully associating them with illicit activities.

4.4 UK House of Lords, Select Committee on the Constitution, Surveillance: Citizens and the State, 2nd Report of Session 2008-09, Volume 1.

Report's Key Themes and Observations

- Emphasis on the constitutional principles that should govern the use of surveillance in the UK: the Sovereignty of the Crown in Parliament; the Rule of Law, encompassing the rights of the individual; the Union State; representative government; and membership of the Commonwealth, the European Union, and other international organisations.
- Recognition that central to the success of evolving constitutional democracy is public commitment to the fundamental principles that underpin the constitutional tenets. In particular, there is a widespread belief in the importance of individual freedom and the need for executive accountability and restraint.
- Asserts that a commitment to the freedom of the individual as paramount, and that this is a precondition of the functioning of the existing constitutional framework and that privacy and the principle of restraint in the use of surveillance and data collection powers are central to individual freedom.

Recommendations (Chapter 9)

- We regard privacy and the application of executive and legislative restraint to the use of surveillance and data collection powers as necessary conditions for the exercise of individual freedom and liberty. Privacy and executive and legislative restraint should be taken into account at all times by the executive, government agencies, and public bodies. (paragraph 144)

Recommendations relating to the commissioners

- Before introducing any new surveillance measure, the Government should endeavour to establish its likely effect on public trust and the consequences for public compliance. This task could be undertaken by an independent review body or non-governmental organisation, possibly in conjunction with the Information Commissioner's Office. (paragraph 110)
- The Government should consider expanding the remit of the Information Commissioner to include responsibility for monitoring the effects of government

- and private surveillance practices on the rights of the public at large under Article 8 of the European Convention on Human Rights. (paragraph 137)
- We regret that the Government have often failed to consult the Information Commissioner at an early stage of policy development with privacy implications. We recommend that the Government instruct departments to consult the Information Commissioner at the earliest stages of policy development and that the Government should set out in the explanatory notes to bills how and when they consulted the Information Commissioner, and with what result. (paragraph 231)
 - We welcome the Government's decision to provide a statutory basis for the Information Commissioner to carry out inspections without consent of public sector organisations which process personal information systems, but regret the decision not to legislate for a comparable power with respect to private sector organisations. We recommend that the Government reconsider this matter. Organisations which refuse to allow the Commissioner to carry out inspections are likely to be those with something to hide. In addition, the protection of citizens' data may in the absence of legislation be vitiated given the growing exchange of personal data between the public and private sectors. (paragraph 238)
 - We welcome the new powers for the Information Commissioner to levy fines on data controllers for deliberately or recklessly breaching the data protection principles and we recommend that the Government bring these powers into force as soon as possible. The maximum level of penalties should mirror that available to comparable regulators, and should not be disproportionate. This must be subject to an appropriate appeals procedure. (paragraph 243)
 - We recommend that the Chief Surveillance Commissioner and the Interception of Communications Commissioner should introduce more flexibility to their inspection regimes, so that they can promptly investigate cases where there is widespread concern that powers under the Regulation of Investigatory Powers Act 2000 have been used disproportionately or unnecessarily, and that they seek appropriate advice from the Information Commissioner. (paragraph 257)
 - We recommend that the Investigatory Powers Tribunal publicise its role, and make its existence and powers more widely known to the general public. (paragraph 259)
 - We recommend that the Government amend the provisions of the Data Protection Act 1998 so as to make it mandatory for government departments to produce an independent, publicly available, full and detailed Privacy Impact Assessment (PIA) prior to the adoption of any new surveillance, data collection or processing scheme, including new arrangements for data sharing. The Information Commissioner, or other independent authorities, should have a role in scrutinising and approving these PIAs. We also recommend that the Government—after public consultation—consider introducing a similar system for the private sector. (paragraph 307)

- We believe that the Information Commissioner should have a greater role in advising Parliament in respect of surveillance and data issues. We therefore recommend that the Government should be required, by statute, to consult the Information Commissioner on bills or statutory instruments which involve surveillance or data processing powers. The Information Commissioner could then report any matters of concern to Parliament. (paragraph 370)
- We recommend that the Government, in conjunction with the Information Commissioner, undertake a review of the law governing citizens' consent to use of their personal data. (paragraph 397)
- We share the Information Commissioner's disappointment that the Government have not made a specific commitment to working with the Information Commissioner's Office to raise public awareness. We recommend that the Government reconsider this matter and commit to a plan of action agreed with the Information Commissioner. (paragraph 436)

Recommendations relating to the National DNA Database

- We believe that DNA profiles should only be retained on the National DNA Database (NDNAD) where it can be shown that such retention is justified or deserved. We expect the Government to comply fully, and as soon as possible, with the judgment of the European Court of Human Rights in the case of *S. and Marper v. the United Kingdom*, and to ensure that the DNA profiles of people arrested for, or charged with, a recordable offence but not subsequently convicted are not retained on the NDNAD for an unlimited period of time. (paragraph 197)
- Whilst a universal National DNA Database would be more logical than the current arrangements, we think that it would be undesirable both in principle on the grounds of civil liberties, and in practice on the grounds of cost. (paragraph 200)
- We recommend that the law enforcement authorities should improve the transparency of consent procedures and forms in respect of the National DNA Database (NDNAD). We believe that the DNA profiles of volunteers should as a matter of law be removed from the NDNAD at the close of an inquiry unless the volunteer consents to its retention. (paragraph 208)
- We are concerned that the National DNA Database (NDNAD) is not governed by a single statute. We recommend that the Government introduce a bill to replace the existing regulatory framework, providing an opportunity to reassess the rules on the length of time for which DNA profiles are retained, and to provide regulatory oversight of the NDNAD. (paragraph 212)

Recommendations relating to CCTV

- We recommend that the Home Office commission an independent appraisal of the existing research evidence on the effectiveness of CCTV in preventing, detecting and investigating crime. (paragraph 82)

- We recommend that the Government should propose a statutory regime for the use of CCTV by both the public and private sectors, introduce codes of practice that are legally binding on all CCTV schemes and establish a system of complaints and remedies. This system should be overseen by the Office of Surveillance Commissioners in conjunction with the Information Commissioner's Office. (paragraph 219)

Recommendations for legislation and the legislative process

- We welcome the UK Computing Research Committee's suggestion that the encryption of personal data should be mandatory in some circumstances. Organisations should avoid connecting to the internet computers which contain large amounts of personal information. We recommend that the Government introduce appropriate regulations. (paragraph 117)
- We recommend that the Government undertake a review of the administrative procedures set out in the Regulation of Investigatory Powers Act 2000 so as to resolve the contrasting views expressed by the Association of Chief Police Officers (ACPO) and the Office of Surveillance Commissioners about the effectiveness of the current legal framework and the system of authorisations. (paragraph 159)
- We recommend that the Government consultation on proposed changes to the Regulation of Investigatory Powers Act 2000 should consider whether local authorities, rather than the police, are the appropriate bodies to exercise such powers. If it is concluded that they are the appropriate bodies, we believe that such powers should only be available for the investigation of serious criminal offences which would attract a custodial sentence of at least two years. We recommend that the Government take steps to ensure that these powers are only exercised where strictly necessary, and in an appropriate and proportionate manner. (paragraph 177)
- We are concerned that three different offices overseeing the operation of the Regulation of Investigatory Powers Act 2000 (RIPA) may result in inefficiencies and disjointed inspection. We recommend that the Government examine the feasibility of rationalising the inspection system and the activities of the three RIPA Commissioners. (paragraph 252)
- We are concerned that primary legislation in the fields of surveillance and data processing all too often does not contain sufficient detail and specificity to allow Parliament to scrutinise the proposed measures effectively. We support the conclusion of the Joint Committee on Human Rights that the Government's powers should be set out in primary legislation, and we urge the Government to ensure that this happens in future. We will keep this matter under close review in the course of our bill scrutiny activities. (paragraph 357)
- We urge the Government to give high priority to post-legislative scrutiny of key statutes involving surveillance and data processing powers, including those passed more than three years ago. The statutes should be considered as part of a

whole, rather than in isolation. This post-legislative role could be carried out effectively by a new Joint Committee on surveillance and data powers. (paragraph 379)

Other specific actions for the Government

- We recommend that the Government should instruct government agencies and private organisations involved in surveillance and data use on how the rights contained in Article 8 of the European Convention on Human Rights are to be implemented. The Government should provide clear and publicly available guidance as to the legal meanings of necessity and proportionality. We recommend that a complaints procedure be established by the Government and that, where appropriate, legal aid should be made available for Article 8 claims. (paragraph 134)
- We recommend that the Government consider introducing a system of judicial oversight for surveillance carried out by public authorities, and that individuals who have been made the subject of surveillance be informed of that surveillance, when completed, where no investigation might be prejudiced as a result. We recommend that compensation should be available to those subject to unlawful surveillance by the police, intelligence services, or other public bodies acting under the powers conferred by the Regulation of Investigatory Powers Act 2000. (paragraph 163)
- We recommend that the Government's development of identification systems should give priority to citizen-oriented considerations. (paragraph 268)
- We agree with the recommendation of the Joint Committee on Human Rights that the role of data protection minister should be enhanced and its profile elevated, and are disappointed that the Government's response has not grasped the main point about the need for more effective central leadership. The Government should report to the House through this Committee on the feasibility of having Ministry of Justice (MoJ) lawyers working in other departments and reporting to the MoJ on departmental policies with data protection implications, and of certification of legislative compatibility with the Human Rights Act 1998. This should be in conjunction with the current system of certification of compatibility by the Minister in charge of each bill going through Parliament. (paragraph 290)
- We support the recommendations made in the Thomas-Walport Data Sharing Review Report for changes in organisational cultures, leadership, accountability, transparency, training and awareness, and welcome the Government's acceptance of them. We urge the Government to report on their progress to Parliament. (paragraph 292)
- We recommend that the Government devote more resources to the training of individuals exercising statutory surveillance powers under the Regulation of Investigatory Powers Act 2000, with a view to improving the standard of practice and respect for privacy. We recommend that the principles of necessity and

- proportionality are publicly described and that the application of these principles to surveillance should be consistent across government. (paragraph 323)
- We believe that encryption has a vital role to play in ensuring the security of data, and that the Government should insist upon its use as appropriate throughout the public and private sectors. (paragraph 331)
 - In the interests of strengthening the protection of personal data, we urge the Government to make the Manual of Protective Security subject to regular and rigorous peer review. (paragraph 342)
 - In the light of the potential threat to public confidence and individual privacy, we recommend that the Government should improve the safeguards and restrictions placed on surveillance and data handling. (paragraph 345)
 - We recommend that the Government review their procurement processes so as to incorporate design solutions that include privacy-enhancing technologies in new or planned data gathering and processing systems. (paragraph 349)
 - We recommend that the Government bring together relevant research councils, polling organisations and government research and statistics bodies to examine ways of improving the independent gathering of public opinion on a range of issues related to surveillance and data processing. (paragraph 400)
 - We recommend that the Government and local authorities should help citizens to understand the privacy and other implications for themselves and for society that may result from the use of surveillance and data processing. Government should involve schools, learned and other societies, and voluntary organisations in public discussion of the risks and benefits of surveillance and data processing. (paragraph 427)
 - We recommend that the Government should undertake an analysis of public consultations and their effectiveness, and should explore opportunities for applying versions of the Citizens' Inquiry technique to surveillance and data processing initiatives involving databases. (paragraph 432)
 - We recommend that the Government improve the design of the Information Charter, and report regularly to Parliament on the measures taken to publicise the Charter and on their monitoring of the public response to it. (paragraph 440)
 - We support the Government's acceptance of the Council for Science and Technology's recommendations for public dialogue and engagement in terms that commit them to the further development of techniques, governance structures, and relationships both within government and with external bodies. We recommend that the Government report to Parliament on the formal requirements which they are placing on departments and agencies to ensure that this commitment extends to policies and practices involving surveillance and data processing. (paragraph 445)
 - We believe that the Government should involve non-governmental organisations in the development and implementation of surveillance and data processing policies with significant implications for the citizen. (paragraph 451)

Recommendations relating to Parliament

- We welcome the Government's plans for better data handling. We recommend that the Government's report on progress on data handling and security be scrutinised by parliamentary committees. (paragraph 337)
- We encourage the Merits of Statutory Instruments Committee to apply the tests of necessity and proportionality to all secondary legislation which extends surveillance and data processing powers, and to alert the House in the normal way where there are any doubts about the appropriateness of the instruments. (paragraph 365)
- We recommend that a Joint Committee on the surveillance and data powers of the state be established, with the ability to draw upon outside research. Any legislation or proposed legislation which would expand surveillance or data processing powers should be scrutinised by this Committee. (paragraph 376)

Recommendation relating to all public and private sector organisations

- As surveillance is potentially a threat to privacy, we recommend that before public or private sector organisations adopt any new surveillance or personal data processing system, they should first consider the likely effect on individual privacy. (paragraph 103)

4.5 UK Home Office. Keeping the Right People on the DNA Database. Science and Public Protection, 2009.

Report's Key Themes and Observations

- The European Court of Human Rights determined in December 2008 that the "blanket policy in England and Wales of retaining indefinitely the fingerprints and DNA of all people who have been arrested but not convicted was in breach of Article 8 of the European Convention on Human Rights."
- However, the Court indicated that it agreed "with the Government that the retention of fingerprint and DNA data 'pursues the legitimate purpose of the detection, and therefore, prevention of crime'."
- The Court's judgment "clearly allows a retention policy provided it is not 'blanket and indiscriminate'. The focus here is "therefore on the details of retention, recognizing the important distinctions made in the judgement between cellular samples, which contain an individual's actual DNA, the DNA profiles on the database which simply describe for identification purposes certain non coding parts of the individual's DNA, and finally fingerprints.

Recommendations

- Sample, profile, and fingerprint retention policies based on age of suspects; nature of crime; whether individuals arrested, convicted, or provided DNA voluntarily.

- Enhance existing governance and accountability of NDNAD.

4.6 Rand Europe. Review of the European Data Protection Directive, 2009.

Report's Key Themes and Observations

- "It is thus clear that the Directive as it is currently being interpreted, implemented and enforced in the Member States does not fully meet its stated objectives of protecting data subject's right to privacy with respect to their personal data or of enabling the free flow of such personal data within the European Union, even without fully considering the similar need that exists between reliable parties outside the Union."
- "The world has now moved on to a networked society where personal data is continuously collected, enriched, amended, exchanged and reused. It is clear that this new social environment needs well-adjusted data protection regulations to address the far greater risks of abuse. This leads to the question: is the current Directive, with its roots in a largely static and less globalised environment, still sufficiently flexible to handle the challenges of today?"
- "One of the crucial characteristics of the Directive is that it is tied to the concept of personal data, and not to the notion of privacy. Indeed, the provisions of the Directive can apply to acts of data processing which are not considered to be privacy sensitive in their own right. The Directive, therefore, serves a number of purposes, privacy protection being only one. Its rules fulfil a range of functions in practice, including encouraging freedom of expression, preventing discrimination and improving efficiency."
- One of the minor weaknesses of the Directive is "the growing dichotomy between data protection in the first (internal market) and the third pillar (law enforcement and judicial co-operation). While the Directive only covers the first pillar, the consensus seemed to be that a common vision on data protection was needed across pillars. The possible disappearance of the pillar distinction in the future is one reason behind this thinking. More importantly, the existence of special rules that substantially exempt third pillar activities from data protection principles undermines the status of these principles as an important part of the European interpretation of fundamental rights. While some concessions certainly need to be made in the light of third pillar efforts, the current approach to data protection in the third pillar is seen as being too ad hoc and lacking restrictions."

Challenges

"Within the contexts of rapid technological change and globalization, a set of distinct challenges were identified:

- Defining privacy - when is privacy affected by personal data processing and when is it not, and how strong should the link between data protection regulations and privacy protection be?
- Risk assessment - can we predict how risky it is to provide our personal data to an entity or organisation?
- The rights of the individual in relation to the benefit of society - under what circumstances can personal privacy become secondary to the needs of society, considering the fundamental importance of privacy protection for the development of a democratic society as a whole?
- Transparency - personal data is everywhere, particularly online, and through technological developments such as ambient intelligence and cloud computing could become increasingly difficult to track and control. How can we be sure how and where it is being used?
- Exercising choice - many services are only provided after sufficient personal data is released, but if important services are denied when we are unwilling to supply that data, do we still have a real choice?
- Assigning accountability -who is ultimately held responsible and where do we go to seek redress?"

Recommendations

- Emphasis on "getting the most out of the current system" rather than complete overhaul of the Directive.
- Emphasis on a results oriented approach with suggestions for new or revised process-based protection and enforcement strategies, including the development of a regulatory architecture.

5. References Cited

1. Warren S. and L. Brandeis, "The Right to Privacy," *Harvard Law Review*, Vol. 4, 1890, pp. 193-220.
2. Pound, R., "Interests in Personality," *Harvard Law Review*, Vol. 28, 1915, p. 343; Freund, P. A., "Privacy: One Concept or Many?" *Privacy (Nomos XIII)*, ed. J. R. Pennock and J. W. Chapman, Palo Alto, CA: Atherton Press, 1971.
3. Prosser D. W., "Privacy," *California Law Review*, Vol. 48, 1960, pp. 383, 389.
4. Moore, A. D., "Toward Informational Privacy Rights," *San Diego Law Review* Vol. 44, 2007, p. 809.
5. Parent W. A., "Privacy, Morality, and the Law," *Philosophy and Public Affairs*, Vol. 12, 1983, p. 269.
6. Innes J., *Privacy, Intimacy, and Isolation*, New York: Oxford University Press, 1992.
7. DeCew, J. W., *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, Ithica, NY: Cornell University Press, 1997.
8. Moore, A. D., "Privacy, Its Meaning and Value," *American Philosophical Quarterly*, Vol. 40, No. 3, 2003, p. 816.
9. Moore, p. 818
10. 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.
11. Solove D. J., *The Digital Person: Technology and Privacy in the Information Age*, New York and London: New York University Press, 2004, p. 2.
12. Official Journal of the European Communities, Council, No L. 28, 23 November 1995, p. 31.
13. Nissenbaum H., "Protecting Privacy in an Information Age: The Problem of Privacy in Public," *Law & Philosophy* Vol. 17, 1998, pp. 559-596.
14. Nissenbaum, 1999
15. Nissenbaum H., "Privacy as Contextual Identity," *Washington Law Review*, Vol. 79, No. 1, 2004.
16. OECD Guidelines, reprinted the Privacy Rights Clearinghouse, 2004, <http://www.privacyrights.org/ar/fairinfo.htm#2>
17. Nissenbaum, 1999
18. Nissenbaum, 1999
19. Solove D. J., "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy," *San Diego Law Review* Vol. 44, 2007, p. 772.
20. Solove, 2007