Privacy and Biometric ID Systems:

An Approach Using Fair Information Practices for Developing Countries

Robert Gellman

Abstract

Biometric identification systems that are in place or under consideration in many countries present significant privacy consequences principally relating to information privacy or data protection. This paper discusses personal privacy in the context of the adoption of biometric identification systems.

While defining privacy is challenging, Fair Information Practices offer familiar and generally accepted privacy principles used in many countries around the world. The principles of Fair Information Practices can be implemented in a variety of ways to meet the needs of any given activity, culture, or nation. Related factors that should be considered include security threats, the existence of identity theft, and the surveillance consequences of centralization of data from an identification system or from transaction records.

The paper suggests ways to use the elements of Fair Information Practices in a biometric identification system to achieve a balanced outcome that protects privacy to an adequate degree. Using Privacy Impact Assessments to consider privacy consequences before making decisions can also assist in achieving a result that minimizes data processing activities that affect the privacy of individuals.

Center for Global Development
1800 Massachusetts Ave NW
Third Floor
Washington DC 20036
202-416-4000
www.cgdev.org

Robert Gellman. "Privacy and Biometric ID Systems: An Approach Using Fair Information Practices for Developing Countries." CGD Policy Paper 028. Washington DC: Center for Global Development.

http://www.cgdev.org/publication/privacy-and-biometrics
CGD is grateful for contributions from the UK Department for International Development, the Norwegian Ministry of Foreign Affairs, the Swedish Ministry of Foreign Affairs, and the William and Flora Hewlett Foundation in support of this work.

Center for Global Development

CGD Policy Paper 028
August 2013

Contents

This report was written by Robert Gellman under a contract with the Center for Global Development. The report reflects the views of the author. The author gratefully acknowledges the assistance of Julia Clark, Alan Gelb, and Latanya Sweeney in the preparation of this report and helpful comments from Colin Bennett and Beth Schwanke.

Foreword

Identification programs involving the use of biometric technology are expanding rapidly in developing countries. A recent survey includes 160 cases with total coverage of over 1 billion people. Some respond to specific needs, such as health insurance, the delivery of social transfers or creation of clean voter rolls, while others aim to create national, multi-purpose, ID platforms. More countries are adopting data protection laws, but the introduction of these programs has not always been matched by a corresponding focus on their implications for privacy, even though many of these programs are supported by donor countries where the privacy of personal data is recognized as a major concern. Nevertheless, as shown by debate in India and some other countries, privacy issues will become more salient as the volume of personal information held in digital form increases.

This paper by Robert Gellman was commissioned as part of CGD's research to better understand and use new technology for development. It recognizes that there is no unique concept of privacy and also that there may be tradeoffs between privacy and other objectives that may be viewed differently in different situations. Approaching the issue from the perspective of Fair Information Practices, it offers guidelines on how the privacy implications of a biometric identification project can be assessed. These concerns are relevant both for countries planning to strengthen their identification systems and for donors considering whether to support them or to use enhanced identification technology in their own projects.

Alan Gelb
Senior Fellow
Center for Global Development

Introduction

Society has looked for solutions to the problem of identifying individuals for hundreds of years, using available technologies to meet the need.[1] The current struggles over the adoption and use of identification technologies are nothing new.

What may be new today is that the privacy consequences of identification systems receive more attention than in the past. This is appropriate because modern information technology offers the ability to collect and link vast amounts of data from multiple sources, to communicate data over great distance, to store and retrieve data from anywhere around the globe, to remember data indefinitely, to allow data collected for one purpose to be readily repurposed for other activities (including activities by sponsors or users of an identification system and activities by third parties and criminals), and to do all of these things at a low cost and often without the knowledge, approval, or participation of the data subject. All of these technological capabilities can affect privacy positively, negatively, or neutrally. Every personal identification system should consider the privacy consequences of the system in advance of adoption and throughout its life cycle.

The backdrop for this paper is the spread of biometric identification technology both for developmental uses and for security in poorer countries. The adoption of biometrics has not always been accompanied by an adequate discussion of privacy. A recent Center for Global Development paper considers the importance of identification and sets out the facts and the trends of biometric identification adoption.[2] That paper surveys 160 cases where biometric identification has been used for various purposes in developing countries. Biometric information collection for identification purposes is already robust and will expand over time.

The broad purpose of this paper is to discuss personal privacy in the context of the adoption of biometric identification systems. This paper does not support or oppose identification technologies in general or biometrics in particular. The value of processes for reliably identifying individuals is a given. Identification systems also affect privacy in a variety of ways, some protective of privacy, and some not. For example, an identification system can make it easier or more difficult for one individual to assume the identity of another.

---

[1] For a review of identification issues in the thirteenth through seventeenth centuries, see Valentin Groebner, Who Are You? Identification, Deception, and Surveillance in Early Modern Europe (2007), http://www.zonebooks.org/titles/GROE_WHO.html. Governments, law enforcement, banks, churches, and others all faced the same problems that we do today in determining who an individual is, but they did not have fingerprints, photographs, or administrative states to issue credentials. They used the facilities, processes, and technologies that they had, however imperfect. Groebner describes the use of portraits, seals, coats of arms, badges, descriptions, registers, lists, and official signs to identify and authenticate an individual. In Italy, governments commissioned painters including Giottino, Botticelli, and Andrea del Sarto to engrave for circulation images of bankrupts on the run, delinquents, and traitors. Groebner expressly states that the notion of the Middle Ages as a simpler period that did not suffer from problems of mistaken identities is wrong.

2 Alan Gelb & Julia Clark, Identification for Development: The Biometrics Revolution (2013) (Working Paper 315) (Center for Global Development), http://www.cgdev.org/content/publications/detail/1426862.

This paper seeks to assist those evaluating the privacy consequences of biometric identification systems by offering a workable framework for understanding privacy, by considering generally existing approaches to legal and other protections for privacy, by reviewing selected privacy issues with an eye toward biometrics, and by suggesting standards, processes, and best practices that will better address privacy. The intended audience includes those who fund biometric identification systems (governments and international donors), those who design and build the systems, and those who operate them.

The paper begins with a discussion of definitional issues for privacy and suggests that data protection or information privacy is best understood using Fair Information Practices. The paper proceeds with a discussion of background issues relevant to the privacy of identification systems. Next, it shows how the principles of Fair Information Practices might apply to the design or operation of a biometric identification system. The paper considers the contribution of Privacy by Design. Finally, the paper suggests ways to use a Privacy Impact Assessment during the development and implementation of a biometric information system.

Biometrics rely on unique physical attributes. Fingerprints are the most classic biometric, with face, iris, voice, hand geometry, and other systems in use and more in development. Some systems measure behavioral activity (e.g., speech or gait) rather than physical attributes. Combinations of biometrics are also in use and under development. Discussion of the specifics of biometric technology is available elsewhere.[3] Biometric technology continues to advance, new biometric measures are under development, and existing technological restrictions may disappear. A biometric identifier may work today only under ideal conditions with bright lights, close proximity, and a cooperative data subject. In the future, however, a later generation of the same technology is likely to allow the capture of the same biometric identifier in low light, without the data subject's consent, and while that data subject is walking down a public street at some distance from the sensor.[4] When evaluating the privacy consequences of identification technology, it does not seem appropriate to assume that privacy protections afforded by current technological limits will continue to protect privacy in the future. Technology will change, but the need to address privacy will not.

However, it is worth mentioning characteristics of biometric identifiers that may be most relevant to this report. First, biometrics establish a verifiable link between a human being and a credential such as an ID card or database record (individual authentication). Second, biometrics can provide the capability for a one-to-many comparison against a biometric

---

[3] See, e.g., National Institute of Standards and Technology, The Biometrics Resource Center, http://www.nist.gov/itl/csd/biometrics/index.cfm. Biometrics are the subject of numerous articles, reports, conferences, and websites.

[4] For example, in testimony in 2012, Electronic Frontier Foundation Staff Attorney Jennifer Lynch refers to technology that allows real-time facial acquisition and recognition at 1000 meters. Testimony before the Senate Judiciary Subcommittee on Privacy, Technology, and the Law, 112th Congress, 2d. Sess. (2012), at text accompanying note 31, http://judiciary.senate.gov/pdf/12-7-18LynchTestimony.pdf.

database in attempt to establish the identity of an unknown individual or to determine if an individual is already enrolled in the system. The de-duplication feature is not available in other identification systems. Third, these two characteristics of biometrics – verifying identity and de-duplication – have different implications for privacy and security and call for independent evaluation. Fourth, biometrics use one or more identifiers that may be difficult to change in the event that an ID card or a database record is compromised. In contrast, a personal identification number (PIN), numeric identifier, or token can be more easily cancelled and reissued. Fifth, biometrics may increase the reliability of an ID system, and so encourage its wider use across different applications. These and other characteristics of biometrics should be part of any evaluation of an identification system from a privacy perspective.

Painting the Background: What is Privacy?

The Challenge of Defining Privacy

It can be difficult to discuss privacy in a global context because the word *privacy* has no universal definition. Indeed, there is no precise equivalent to the English word *privacy* in some languages.[5] Even a discussion limited to the English language has major definitional problems.

Privacy scholar and former data protection commissioner David Flaherty describes privacy as a "broad, all-encompassing concept that envelops a whole host of human concerns about various forms of intrusive behavior, including wiretapping, surreptitious physical surveillance, and mail interceptions."[6] As broad as Flaherty's description is, it may not be broad enough to suit some people and some concerns. Professor James Whitman makes the point thusly: "[h]onest advocates of privacy protections are forced to admit that the concept of privacy is embarrassingly difficult to define."[7]

Official statements about privacy are often murky. The U.S. Supreme Court interprets the US Constitution as protecting as a privacy matter both information privacy and a broader range of interests often described as *personal autonomy*, but much uncertainty remains about the scope of the constitutional privacy interest.[8] Many other countries also recognize a constitutional privacy right,[9] but the specific meaning may not be clear. The Universal Declaration of Human Rights, adopted by the United Nations in 1948, is one of multiple

---

5 See, e.g., John Mole, Mind Your Manners: Managing Business Cultures in the New Global Europe 250 (2003), http://www.saigontre.com/FDFiles/MindYourManners.pdf.

6 David H. Flaherty, Protecting Privacy in Surveillance Societies xiii (1989).

7 James Q. Whitman, The Two Western Cultures of Privacy: Dignity Versus Liberty, 113 Yale Law Journal 1151, 1153 (2004), http://www.yalelawjournal.org/the-yale-law-journal/article/the-two-western-cultures-of-privacy:-dignity-versus-liberty/.

8 See, e.g., Whalen v. Roe, 429 U.S. 589 (1977), http://www.law.cornell.edu/supct/html/historics/USSC_CR_0429_0589_ZS.html.

9 Electronic Privacy Information Center, Privacy & Human Rights: An International Survey of Privacy Laws and Developments 2006 1 (2007).

international documents that identifies privacy as a human right, but the scope of that right is far from clear.[10]

Cultural, religious, and other factors contribute to the difficulty of defining privacy. A few examples make the point. Sweden and other Scandinavian countries have broadly applicable privacy laws, but the tax returns of individuals are public.[11] In the United States, where there are no broad privacy laws, a specific law expressly prohibits the federal government from disclosing tax returns.[12] In some Muslim communities, women typically appear in public wearing garments covering the body from head to feet. In France and some other European countries, nude sunbathing is common. Americans may be equally dismayed by both of these opposite practices.

In addition, different professions also have different approaches to privacy. Physicians, attorneys, accountants, and clergy are professionals with differing ethical codes addressing privacy. National legal regimes may influence these codes in different ways.

The point should be clear. The definition of privacy in any jurisdiction must take into account the cultural, historical, legal, religious, and other local factors. One size may not fit all countries, regions, or cultures when it comes to privacy or to some elements of privacy. In addition, views of privacy change as time passes and technology advances. However, different perspectives are not a barrier to evaluating privacy but a challenge.[13]

One of the few examples of a multi-national privacy policy is the European Union.[14] The Europeans usually use the narrower term *data protection*, and the legal instrument adopted by the European Union is a *data protection* directive.[15] The term *data protection* solves some language and definitional issues. A generally equivalent term often used in the United States and in some other places is *information privacy*.

---

[10] Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/810, at Art.12 (1948), http://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=eng. ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.").

[11] See Jeffrey Stinson, *How much do you make? It'd be no secret in Scandinavia*, USA Today, June 18, 2008, http://usatoday30.usatoday.com/news/world/2008-06-18-salaries_N.htm.

[12] 26 U.S.C. § 2603, http://www.law.cornell.edu/uscode/text/26/6103.

[13] For a list of national privacy laws, see http://www.informationshield.com/intprivacylaws.html.

[14] The Asian Pacific Economic Cooperation (APEC) sponsors another multi-national privacy effort at promoting Cross Border Privacy Rules in order to reduce barriers to information flows, enhance consumer privacy, and promote interoperability across regional data privacy regimes. APEC *Privacy Framework* (2005), http://publications.apec.org/publication-detail.php?pub_id=390.

[15] Council Directive 95/46, On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Art. 5, 1995 O.J. (L 281) 31, 39, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML [hereinafter cited as "*EU Data Protection Directive*].

Both *data protection* and *information privacy* refer to the collection, maintenance, use, and disclosure of *personal data*.[16] While the broad concepts of *data protection* and *information privacy* are similar enough for present purposes, *data protection* and *information privacy* can vary significantly when implemented in national and regional laws.

For *personal data*, the term *processing* includes collection, maintenance, use, and disclosure of *personal data* and provides additional specificity.[17] The terms *personal data* and *personally identifiable information* (PII) are interchangeable here.

For the purposes of this report, *data protection* as it relates to the processing of PII is the principal privacy concern under discussion. There may be privacy or other objections beyond the narrower focus on the processing of personal information. For example, in some cultures, some might object to the taking of a photograph or to the collection some types of body information. Those are broader *privacy* concerns, and those objections could be factors in some countries when making a choice about the type of biometric identifier to use. If so, a palm print might be more acceptable for local cultural or religious reasons.

However, once collected, the biometric, whether photo or palm print, becomes *personal data* that falls primarily under *data protection* as a concern. Defining the borders between privacy and data protection is not crucial here, but awareness of the differences is useful to keep in mind, as is the possibility that data collection methods may give rise to a different set of concerns than data usage.

Sidebar on Terminology

Privacy is a broad term that relates to general concerns about surveillance, processing of personal data, intrusive activities, personal autonomy, relationships, and more.

Personal data or *personally identifiable information* (PII) is information about any identified or identifiable natural person.

Processing of personal information includes the collection, maintenance, use, and disclosure of the information.

Data protection or *information privacy* is the subset of privacy issues about the processing of personal information.

Data controller means the person who determines the purposes and means of processing of personal data.

Data subject means an individual whose personal data is being processed.

[16] *EU Data Protection Directive*, Art. 2(a).

[17] The Directive defines *processing of personal data* to mean "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." *EU Data Protection Directive*, Art. 2(b).

Two additional comments about data protection are appropriate at this stage. First, for any given activity involving PII, data protection is not a binary attribute that is either present or absent. Data protection cannot be assessed on a one-dimensional scale. Personal data is not either *protected* or *not protected* for privacy. As will become clear in the next section, data protection involves a set of attributes, concerns, and standards whose implementation can vary without necessarily violating basic principles. Data protection calls for weighing and balancing choices, procedures, and values to achieve a result acceptable in a society.

For example, many tend to view health data as worthy of the highest level of privacy protection. Yet if health records are strictly controlled and only used for the treatment of a data subject, it may be difficult or impossible to conduct many types of health research. Public health activities and fiscal controls over health spending might also suffer. The challenge is to find a way to balance the possibly conflicting objectives of data protection and health research, public health, and other goals, including security, law enforcement, oversight of health professionals, and management. The use of biometric identification, like identification based on other types of PII, requires the balancing of data protection along with other concerns.

Second, national data protection laws are no longer found only in technologically advanced nations. A 2012 review found that 89 countries now have data protection laws, with 81 countries providing comprehensive coverage of both private and public sectors.[18] Thus, in many countries, existing legal frameworks may already contain privacy principles that provide rules or guidance applicable to biometric identification systems. However, the extent to which existing national data protection laws are adequately followed or enforced is debatable in many countries. Also, privacy and civil liberties concerns may not receive the attention in some countries that they do in others. Thus, notwithstanding the spread of data protection laws around the world, this paper may have value for anyone seeking a better understanding of the fundamentals of privacy.

Fair Information Practices

Narrowing the focus of privacy to *data protection* here is a step, but it does not resolve all definitional challenges. If, as stated above, we cannot measure data protection on a one-dimensional scale, then how can we measure it? We need to identify the elements of *data protection* so that can we can apply them when evaluating privacy in general and data protection in biometric identification systems in particular.

---

[18] Graham Greenleaf, *The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?* (2012) (Edinburgh School of Law Research Paper Series No 2012/12), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960299. The article also documents the influence of EU data protection standards (including FIPs) in shaping the laws of non-EU Member States. See also Graham Greenleaf, *Global data privacy laws: 89 countries, and accelerating*, (2012) Special supplement to 115 Privacy Laws & Business International Report (2012), available at http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=57970.

The most commonly used set of data protection principles for this purpose is Fair Information Practices (FIPs).[19] Information privacy law and policy in many countries relies on FIPs as core principles. The international policy convergence around FIPs is broad and deep, and the agreement has remained substantially consistent for several decades.[20] The EU's Data Protection Directive and the many national laws in EU Member States and in other counties based directly or indirectly on the Directive are implementations of FIPs.

FIPs originated in the 1970s with a report from a predecessor of the federal Department of Health and Human Services in the United States.[21] A few years later, the Organisation for Economic Cooperation and Development (OECD) revised the original statement of FIPs.[22] The OECD's version became the most influential statement of the principles.[23]

The eight principles set out by the OECD are:

Collection Limitation Principle: 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 Principle: 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 [the Purpose Specification Principle] except: a) with the consent of the data subject; or b) by the authority of law.

[19] For a short and general history of FIPs, see Robert Gellman, *FAIR INFORMATION PRACTICES: A Basic History* (2012) (Version 1.91), http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

[20] See generally Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (1992).

[21] U.S. Dep't of Health, Educ. & Welfare, Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems (1973), http://epic.org/privacy/hew1973report/default.html.

[22] Org. for Econ. Cooperation and Dev., *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

[23] The Asian Pacific Privacy Framework, an alternative international approach to privacy, has much in common with the OECD FIPs principles, *available at* http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx.

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 and usual residence of the data controller.

Individual Participation Principle: An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) 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; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) 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.

These FIPs principles can be organized in a variety of ways. Different formulations of FIPs often show significant variances in the number and organization of principles. This is true even when the content of different versions is substantially the same.[24] For example, the OECD version of FIPs treats access and correction rights under as a single principle, but access and correction can be stated as independent rights. Similarly (as will be seen later), purpose specification and use limitation are sometimes merged rather than treated separately.

The high-level FIPs principles include few implementation details. The consequence is that applying FIPs in a particular context cannot be accomplished through a mechanical application of rules. Implementing FIPs requires judgment and customization. This operational flexibility is helpful because it allows the principles to adapt to different activities, data, contexts, and societies. However, it also allows comparable systems with significantly divergent privacy policies to claims compliance with FIPs. No central authority determines if any given activity complies with FIPs principles, although governmental supervisory authorities for privacy may engage in a comparable activity under the terms of a national privacy law.

---

[24] The Canadian Standard Association Model Code for the Protection of Personal Information as enacted into Canada's Personal Information Protection and Electronic Documents Act essentially restates FIPs in ten principles rather than eight. S.C. 2000, c. 5, Schedule 1 (Can.), available at http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-2.html.

Notwithstanding their broad acceptance and use, FIPs has some critics. The critics include some who are more supportive of privacy protections[25] and some who are less supportive.[26] Debates over the adequacy of privacy standards are perpetual. FIPs nevertheless remain the most commonly used standard for information privacy.

One conclusion that flows from FIPs is that information privacy is not merely a matter of consent or choice. It is not sufficient for an individual to have an opportunity to affirmatively consent (opt-in) or to negatively consent (opt-out) to an activity that uses PII. All elements of FIPs matter in evaluating information privacy. A single choice about participation does not and cannot address all the data protection interests and concerns that arise.

In the case of an identification system, allowing a choice about participation does not mean that those who elect to have an identifier waive all data protection concerns. The interests reflected in FIPs remain important regardless of the choice offered. Of course, individual preference may override a standard implementation of FIPs principles. For example, an individual can consent to a disclosure of his or her PII that a law or standard otherwise prohibits. However, there are limits to choice. For example, no one should be asked to opt-out of having adequate security protections for their PII.

In the era of Facebook, Google, and cell phones, how do privacy concerns about an identification system compare?

Multiple factors may affect an individual's assessment of the privacy consequences of an identification system versus the assessment of an Internet or cell phone activity. Many individuals are likely to perceive meaningful differences between an identification system and commercially operated PII-intensive activities on the Internet or otherwise.

The extent to which the collection and use of PII occurs routinely in modern life varies considerably around the world. Both governments and the private sector collect and use PII much more extensively in some countries than in other countries. As technology expands throughout the world, however, this could easily change. Cell phones in particular are PII intensive. The basic operation of a cell phone requires constant tracking of the phone's location. Other information stored in a phone, including address books, calendars, photographs, and files, can be at risk for secondary use either with or without the user's

---

[25] See, e.g., Gary Marx, *An Ethics For The New Surveillance*, 14 The Information Society 171 (1998), available at http://web.mit.edu/gtmarx/www/ncolin5.html (arguing that FIPs need to be broadened to take account of new technologies for collecting personal information); Roger Clarke, Research Use of Personal Data (2002), http://www.anu.edu.au/people/Roger.Clarke/DV/NSCF02.html (arguing for broader protections for privacy and for more anonymity, and pseudonymity).

[26] FIPs may have become a form of generic trademark for privacy principles rather than an indicator of any affiliation with the original standards. Thus, some statements identified as FIPs have been lacking in all of the classic elements. In 2000, for example, the FTC offered a version that included only notice, choice, access and correction, and security. Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace* (May 2000), http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

knowledge and approval. Are the privacy consequences of an identification system (biometric or otherwise) operated by the government much worse or much different from those we face in a world filled with cell phone and social networks?

First, an identification system may be required either as a matter of law or as a matter of practice. If an individual needs a particular identifier in order to vote or receive a government benefit, then there is no real choice. However, whether an individual posts information on a social network and what information the individual chooses to post is a matter of choice. Cell phones present fewer practical choices. Options include not accepting privacy-invasive applications or turning off the phone to keep location unknown to the phone system.

Second, many individuals will perceive a significant difference if the government or the private sector operates a personal data collection activity. A government can put an individual in prison, for example. Official identification requirements can affect the right to vote or receive government benefits. With a private identification service, an individual would not necessarily be sharing information with the government, and the individual may have an option about which identification provider to use.[27] Choice in identification providers may be less likely with a government service, especially a national service. Conversely, in some jurisdictions only the government may be subject to a privacy law or to due process obligations.

Third, it may matter if an activity is identifiable to an individual rather than anonymous or pseudonymous. An identification system is likely to create information that is fully identifiable to an individual. It is possible for an identity system to operate in part on an anonymous basis. For example, if an individual must be 21 years old to purchase liquor, an identification system could allow age verification without revealing or recording identity. However, it is fair to assume that a formal identification system will result in individually identifiable information much of the time. In contrast, Internet activities can sometimes be anonymous or pseudonymous, especially if a user seeks to protect his or her identity.

Fourth, it may matter if the terms of an identification activity are established by law or if they are set by private companies. Changing a law is a complex and lengthy activity, and individuals generally must accept the terms of any existing law. However, privately established terms can be adjusted more readily. Individuals may not have the ability to

---

[27] The National Strategy for Trusted Identities in Cyberspace (NSTIC) is a US initiative to improve the privacy, security, and convenience of online transactions. It calls, among other things, for "multiple accredited identity providers, both private and public, and choices among multiple credentials." See US Department of Commerce,

National Institute of Standards and Technology, *Recommendations for Establishing an Identity Ecosystem Governance Structure* (2012), http://www.nist.gov/nstic/2012-nstic-governance-recs.pdf. See also http://www.nist.gov/nstic/index.html.

change terms on their own, but companies sometimes react when customers object to privacy invasive policies. The most important option for individuals using a private service may be that they can decide not to use the service or they can switch to a different service with more acceptable terms.

Fifth, private activities using PII may have attributes that are likely to be absent from government identification systems. Many websites and cell phone applications rely on personal information from users in order to generate revenue from marketing activities. The need for advertising or other revenues may lead to the creation of detailed profiles about individuals in order to target ads to users. The accumulation of details of an Internet user's activities – such as the collection and maintenance of all search requests made on a website – may be broadly comparable to the details that might result from a centralized identification database that collects detailed transaction information. However, it seems less likely that commercial exploitation of PII will result with government activities.

Finally, an individual may not be able to avoid a government operated identification system used universally in a country and still vote, hold a job, or obtain an education. In contrast, a private identification service may not be universal. An individual may be able to exercise choice in using the service or, if possible, using a different service.

Even those who participate fully in other PII-intensive activities may still have concerns about an identification system, especially a system that include surveillance features. Of course, privacy preferences among individuals may vary widely and inconsistently. Also, privacy preferences may change over time, with people demanding either more or less privacy protection. However, the trend in countries with intense use of PII has been to provide more and not less privacy protection as a matter of law and as a matter of practice.

Selected privacy topics and concerns

In countries where the processing of personal data for a large number of purposes by public, private, and non-profit actors is already widespread, struggles over data protection are often more intensive. It seems a reasonable assumption that some of the lessons learned and being learned in these countries may be instructive for countries where processing of personal data has not been as common. This section provides a short overview of existing privacy regulation, trends in data use, and issues that might arise immediately or eventually when adopting biometric identification systems.

Any identification system that involves PII presents privacy issues for analysis. A biometric identification system is an identification system with the addition of one or more biometric identifiers. Yet an analysis of a biometric identification system cannot focus solely on the biometric element. An identification system and the technology it employs are intertwined and must be evaluated for privacy as a whole. It is not practical to seek to separate the elements that are "biometric" from those that pertain only to identification. Personal identification systems and all of their features affect the privacy of personal information.

This section focuses on broader privacy issues that are generally instructive in some way to understanding current privacy issues relevant to biometric identification systems.

1. Models of legal protection for personal data

The European Union offers the leading international model for data protection. The EU Data Protection Directive directs EU Member States to adopt national legislation meeting standards set out in the Directive.[28] The standards implement FIPs. Each EU Member State must have an independent supervisory authority for data protection.[29] With some exceptions, the same standards apply broadly to all data controllers and to all personal data processing in Member States.[30] Many countries around the world have data protection regimes that mirror EU standards.

The United States offers a contrasting model. American privacy laws are sectoral, applying to specific data controllers or to specific classes of personal data. Standards established by statute vary from law to law, often implementing some but not all FIPs standards. Many personal data processing activities remain wholly unregulated for privacy in the US. For example, most merchants and most websites are not subject to any US privacy law. There is no American equivalent to the EU supervisory authority for data protection.[31] Many data controllers in the United States – although not the federal government[32] – could establish biometric identification systems without meeting any legislated data protection requirements.

One reason many other countries follow the EU model is the restriction the Directive places on the export of PII to third countries that do not ensure "an adequate level of protection."[33] Exporting personal data from an EU Member State to a third country can be much more complicated or even impossible if the third country does not meet the EU adequacy standards. Companies and institutions in a country that meets the adequacy standard can readily export data from the EU, a significant advantage for multinational companies and for companies that want to offer information processing services to European companies.[34] For personal data processing activities that occur wholly within a third country, EU export limits may not be a concern except, perhaps, if governments or

---

[28] The EU is considering changing the model to one where an EU regulation would establish a common regulatory framework within the EU. See, e.g., the European Commission's webpage, http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

[29] *EU Data Protection Directive* at Art. 28.

[30] *EU Data Protection Directive* at Art. 3(1).

[31] The US Federal Trade Commission may be the closest equivalent, but the Commission does not have jurisdiction over large parts of the American economy.

[32] The federal government is subject to the Privacy Act of 1974, the first privacy statute that met FIPs standards. 5 U.S.C. § 552a, http://www.law.cornell.edu/uscode/text/5/552a.

[33] *EU Data Protection Directive* at Art. 25(1). The Directive recognizes justifications for data export other than a finding of adequacy. Id. at Art. 26.

[34] So far, the EU recognizes about a dozen countries as having adequate protections under EU standards. See European Comm'n, *Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries*, http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

companies transfer personal data from a third country to Europe for some types of processing.[35] Export rules could also be relevant if one nation allows use of its identification data by external actors or international institutions. This seems a possibility with biometric identification.

2. Mission Creep

One of the core principles in Fair Information Practices is that personal data should only be used or disclosed for purposes specified at the time of collection.[36] Mission creep (or function creep) arises when personal data processing expands beyond the original stated purposes. Once created, a personal information resource often attracts others who want to use that resource in support of an unrelated activity in order to save money, improve efficiency, catch criminals, or accomplish other socially beneficial or commercially attractive goals. The reason it is difficult to resist mission creep is that the additional uses are often advantageous to a worthwhile objective, although that objective may be unrelated to the purpose originally established for the processing. Privacy advocates routinely object to new uses of existing personal data on the grounds of mission creep.

Nevertheless, the broad goal of protecting privacy by applying the purpose standard sometimes gives way to a later idea with political or economic appeal. A recent example from many countries is *finding and preventing terrorism*, a goal that placed pressure on privacy protection established for some databases. In an example from India, a unique identifier program (UID) originally defined as voluntary has been criticized because it is being expanded to be a requirement for receiving government services.[37]

It can be attractive to use an identification system developed for one purpose for other purposes, especially in countries where identification is in short supply. One of the best examples of mission creep for an identification system comes from the United States. In 1935, the US established a program that provided pensions for senior citizens.[38] Individuals participating received a Social Security Number (SSN) and a card. The originally issued card

---

[35] EU data protection rules apply differently and sometimes not at all to those processing personal data on behalf of another. See Art. 29 Working Party, 00264/10/EN, WP 169, Opinion 1/2010 on the Concepts of "Controller" and "Processor" 25 (Feb. 16, 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.

[36] This statement derives from the Purpose Specification Principle and the Use Limitation Principle. Exceptions are allowed with the consent of the individual, when required by law, and for other purposes "not incompatible" with the specified purposes. The US Privacy Act of 1974 includes a similar vague purpose test based on compatibility. 5 U.S.C. § 552a(a)(7) (definition of routine use) & (b)(3) (allowing disclosure for routine uses), http://www.law.cornell.edu/uscode/text/5/552a. The lack of precision of the compatibility standards invites broad interpretation and expanded processing.

[37] See, e.g., Gopal Krishna, Rediff News, *If UID is voluntary, why is it used to deliver services?* (Oct. 19, 2012), http://www.rediff.com/news/column/if-uid-is-voluntary-why-is-it-used-to-deliver-services/20121019.htm.

[38] For a history of the program, see https://www.socialsecurity.gov/history/.

said expressly "For Social Security Purposes • Not For Identification," although that statement was later expanded to say that it was also for tax purposes.

Over the decades that followed, the SSN became a de facto identification number, used for federal income tax purposes, identification of military personnel, passports, federal health insurance, and many other official purposes.[39] Today, most newborns receive a SSN because of the need for a SSN to obtain health care, health insurance, tax deductions, or other benefits or status. The private sector also adopted the number for many purposes as well, a trend spurred by the use of the SSN for tax purposes. For decades, no legislation restricted private use of SSNs.

The decision to expand the use of SSN was often the most expedient alternative. Typically, the choice came without any consideration of the privacy consequences, partly because recognition of information privacy as a public policy concern began slowly in the 1960s and 1970s.[40] A full tally of the costs and benefits of extended SSN usage has not been compiled, but the losses just from identity theft in recent years are measured in the billions of dollars annually.[41] Not all of those costs are attributable to use of the SSN, but the widespread use of the SSN is a major factor. A National Research Council report on identification highlighted one reason for a lack of attention to costs and consequences: "When the parties that issue and rely on an identifier are different, the incentives for risk mitigation are not necessarily aligned."[42]

Starting in the 1970s, Congress began to recognize that the expanded uses of the SSN were affecting individuals in negative and unintended ways. The SSN lacks attributes of a well-designed identifier (e.g., it does not include a check digit[43]), and errors in recording numbers have interfered with the ability of individuals to obtain benefits, employment, insurance, and credit. The SSN also allowed the linking of disparate databases without adequate safeguards.[44] The first legislation seeking to restrict general government use of the SSN came

---

[39] For a history of official actions from 1935 through 2005 affecting use of the SSN, see Social Security Administration, Social Security Number Chronology, http://www.ssa.gov/history/ssn/ssnchron.html.

[40] A presidential Executive Order from 1943 directed agencies to use the SSN rather than create new identification systems. Executive Order 9397, 8 Federal Register 16095 (Nov. 30, 1943). It was not until 2008 that the order was modified slightly. Executive Order 13478, 73 Federal Register 70239 (Nov. 20, 2008), http://www.gpo.gov/fdsys/pkg/FR-2008-11-20/pdf/E8-27771.pdf.

[41] The President's Identity Theft Task Force (US), Combating Identity Theft: A Strategic Plan 11 (2007), http://www.identitytheft.gov/reports/StrategicPlan.pdf.

[42] National Research Council, Who Goes There?: Authentication Through the Lens of Privacy 138 (2003), http://www.nap.edu/catalog.php?record_id=10656.

[43] A check digit is an alphanumeric code added to a number (or string of letters) that provides a means of verifying the accuracy or validity of the number.

[44] See generally, U.S. Dep't of Health, Educ. & Welfare, Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems (1973), http://epic.org/privacy/hew1973report/default.html. Safeguards might include limits so that information transferred for one purpose is not used for another purpose, adequate security for transferred information, or providing rights of access or correction to data subjects.

in 1974.[45] In the ensuing decades, both federal and state government began to discourage or prohibit use or display of the SSN for some governmental or private sector activities. Many in the private sector also followed the lead of the federal government and voluntarily replaced SSNs with other identifiers. The changes responded to public concerns about privacy and fraud. Eventually, the rise of identity theft exacerbated by the growth of the Internet in the 1990s spurred the ongoing movement to limit use or disclosure of the SSN. However, the number is still in use for many official and unofficial purposes. Secondary uses of SSNs for official, unofficial, or criminal purposes remain as a concern.[46]

For an identification system, a response to concerns about mission creep begins with establishment of a clearly defined statement of uses during planning for the system. However, the more reliable an identification system is, the greater the likely demand for additional uses. A reliable identification system is clearly advantageous, and biometrics can produce a better result than some other identification systems. Conversely, the casual linking of disparate records allowed by a common identification system may lead to unwanted consequences and costs.[47] The conflicts that arise are not easy to resolve, and it can be difficult to resist subsequent requests for use. The marginal effect on privacy of any given use may be small, but the cumulative effects over time may be major. Much depends on the specific details of data collection and operation of the identification system, including how the system might be used to link records and record systems that might otherwise remain separate.

Other responses to mission creep include limiting collection or maintenance of the amount or types of PII (to make the system less attractive for secondary uses), controlling the technology required to access the system (to prevent unauthorized uses), restricting recording information about some uses of identification (to avoid tracking and centralization of activities), public notice and debate over later uses (to allow for informed and responsive decision-making), development of local identification systems for some activities (to avoid reliance on a single system), and effective data subject choice about some uses (to allow consumer resistance).

---

[45] Public Law 93-579, § 7, 5 U.S.C. § 552a note, http://www.law.cornell.edu/uscode/text/5/552a.

[46] University of Miami law professor Michael Froomkin offers an "uneasy" suggestion that the obligation to comply with privacy rules be a requirement for private sector use of a national identity card. His model would impose FIPs on those who seek to benefit from the value created by a national identity card, thus offsetting in part some of the privacy invasive consequences of an identity card by expanding privacy protections as use of the card spreads in the private sector. This idea is "biometric neutral", as it could apply whether or not the identity card uses a biometric. A, Michael Froomkin, *The Uneasy Case for National ID Cards as a Means to Enhance Privacy in Securing Privacy in the Internet Age* in Security Privacy in the Internet Age (A. Chander, L. Gelman, M.J. Radin, eds.) (2008), available at http://law.tm/articles2/Uneasy-Case-for-National-ID-Cards.pdf.

[47] For example, the US Congress enacted legislation in 1988 to control the linking of separate databases, requiring administrative controls and due process for individuals affected by matching. 5 U.S.C. § 552a(o), (p),(q), (u), http://www.law.cornell.edu/uscode/text/5/552a

When designing an identification system, mission creep can be "built in" if the designers intend the system for widespread use or if the design calls for collection of greater amounts of personal data than needed for current activities. Compare an identification system that collects the least amount of personal data (e.g., name, gender, date of birth, and biometric) with a different system that includes place of birth, tribe, religion, address, height and weight, health data, socioeconomic status, next of kin, identification and bank account numbers, etc. An identification system designed from the beginning to serve multiple organizations and multiple purposes may collect many types of PII in order to meet its broadly defined objectives, including some prospective objectives. Regardless, whether multiple uses of an identification system are the result of original design or later decision, the concerns about broad sharing of PII and data linkages remain.

The structure of an identification system can affect the availability of the system for secondary uses and other privacy consequences. A centralized system, with a single issuer of credentials and a central database of transactional information, might be easier to expand to accommodate new uses and new users, but the result may be more accumulation of personal details in a single database. A federated system – and there can be many different designs – can segregate the issuance of credentials and leave authorized users who rely on the credentials to maintain whatever transaction records they require in distinct databases. Wholly separate identification systems for separate functions is another model that may lessen pressures on privacy interests, but possibly at a greater cost or with less capability to control abuses.

3. Identity theft and the advanced persistent threat

Identity theft is the misuse of another individual's personal information to commit fraud.[48] Identity theft (sometimes called *identity fraud*) occurs in many ways, but the basic elements are the same. Criminals gather personal information by stealing mail, workplace records, or other information, or they use high-tech methods such as hacking of websites, fraudulent email (phishing), social media sites, or purchasing information from companies selling background information about individuals. The criminals use the information to open credit accounts, take over existing accounts, obtain government benefits or services, or in other ways. Identity theft has grown in volume and cost in recent years. Losses in the United States are uncertain but total billions of dollars annually.[49]

While the crime of identity theft is not limited to the United States, much of the world's identity theft activity affects Americans. There are many reasons, including the widespread availability of PII about US citizens, the reliance on Social Security Numbers for credit and identification purposes, lack of effective privacy laws, and the wealth of the country. Identity theft is an industry complete with the wholesale buying and selling of personal data by

---

[48] The President's Identity Theft Task Force (US), *Combating Identity Theft: A Strategic Plan* 10 (2007), http://www.identitytheft.gov/reports/StrategicPlan.pdf.

[49] Id. at 11.

criminals. The Internet makes it possible for criminals to engage in identity theft from any place in the world. Today, poorer countries may not be prime targets for identity thieves, especially those operating via the Internet. However, this could change as cell phones, bank accounts, and Internet–based transactions spread. Any personal identification system must consider the possibility that identity thieves will look for ways to capture and exploit identifying information.

The use of biometrics will surely make some forms of identity theft harder. For example, a biometric has the capability of linking an individual to an identifier in a way that other identifiers cannot. It should be more difficult for an individual to impersonate another in situations where physical presence allows for the matching of a biometric to the individual.

However, the use of biometrics does not guarantee protection against identity theft. The Electronic Frontier Foundation (EFF), an international non-profit digital rights group based in the United States, writes about the problems with compromised biometric systems:

> Arguments in support of biometrics rest on the flawed assumption that these ID schemes prevent identity fraud. Yet identity and authentication systems based on biometrics are weak because once these indicators are compromised, they cannot be reissued like signatures or passwords. You cannot change your fingerprints or your irises if an imposter is using this data. Up to five per cent of national ID cards are lost, stolen or damaged each year. Aggregated personal information invites security breaches, and large biometrics databases are a honeypot of sensitive data vulnerable to exploitation. Identity thieves can also exploit other identifying information linked to stolen biometric data. Those at the mercy of these databases are often unable to verify their security or determine who has access to them.[50]

EFF offers three important points. First, a compromised biometric identifier cannot be reissued in the way that a compromised identification number can. Second, a database of biometric identifiers is very attractive to criminals. Third, an identification database with biometrics will also have other identifying data that identity thieves can exploit. Other security vulnerabilities for biometric identifiers exist as well.[51]

The concerns expressed by EFF are not necessarily unique to biometrics. For example, an ID card can be lost whether or not it uses biometrics. However, the problem of reissuing compromised credentials can be more difficult for biometrics than for other identification systems. Any identification system has vulnerabilities and costs, strengths and weaknesses. Any identification database may attract hackers and criminals, regardless of its use of

---

[50] Electronic Frontier Foundation, *Mandatory National IDs and Biometric Databases*, https://www.eff.org/issues/national-ids.

[51] See, e.g., Ann Cavoukian & Alex Stoianov, *A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy* 12-13 (2007), http://privacybydesign.ca/content/uploads/2007/03/bio-encryp.pdf. Ann Cavoukian is the Information and Privacy Commissioner in Ontario, Canada.

biometrics. A privacy and security evaluation must address the advantages and disadvantages of any identification system. The purpose here is to identify issues for that evaluation.

Another factor is the *advanced persistent threat* (APT). APT refers to cyber threats where a particular entity is the target of Internet-enabled espionage by highly-qualified, determined, and well-funded attackers. APT sometimes describes Internet espionage funded by national governments against other governments or private companies with valuable information resources. An assumption of APT is that any information resource, PII or otherwise, maintained in computers connected to the Internet may be the target of attack at any time. Many expect this state of affairs to continue indefinitely.

A national identification database – with or without biometric identifiers – may become the target of criminals who want to exploit identity information. It could also become the target of other governments looking for dissidents, expatriates, or others. Anyone seeking to destabilize a country's activities that rely on an identification system might target that system. The more any single identification system is used, the greater the vulnerability. APT is something that any identification system must take into account.

Computer security measures as well as other standard physical and process security measures offer protections against misuse of identification information. Biometric identification systems may be subject to the same threats as other identification systems, with the important exception that it may be impossible to reissue an individual's compromised biometric identifier. Unless a system's security is perfect – a seemingly unattainable goal – any identification system must be capable of reissuing an identifier following compromise of the original number or biometric. There are technical solutions to that problem for biometrics.

Biometric encryption is a process that converts a biometric to a cryptographic value, which can be used directly or combined with a PIN to produce another value (or key) so that neither the biometric nor its cryptographic derivation can be retrieved from the stored template. The key is re-created only if the correct live biometric sample is presented on verification. The advantage of biometric encryption is that the key is completely independent of biometrics and can always be changed or updated.[52] The technical challenges of biometric encryption are neither simple nor addressed here.

It is not the purpose of this paper to explore security threats to biometrics in any detail. Security measures and especially encryption are complex technical subjects. The point here is to recognize that there are significant security threats to identification systems and to biometric systems, that biometric systems have some unique vulnerabilities, and that

---

[52] Ann Cavoukian & Alex Stoianov, *A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy* 16 (2007), http://privacybydesign.ca/content/uploads/2007/03/bio-encryp.pdf ("Our central message is that [biometric encryption] technology can help to overcome the prevailing 'zero-sum' mentality, namely that adding privacy to identification and information systems will necessarily weaken security and functionality.") .

measures to protect identification systems exist and are in development. Security is an important element of privacy, and security vulnerabilities must always be considered when evaluating privacy concerns. .

4. Privacy and discrimination

The goals and methods of privacy protection and of preventing discrimination overlap in part, differ in part, and may conflict at times. An awareness of these overlaps, differences, and the potential for conflict is valuable.

As explained earlier, the goals of information privacy protection are not easy to state, but they relate broadly to the fair processing of PII. Discrimination is the prejudicial or distinguishing treatment of an individual based on an actual or perceived characteristic, such as membership in a group, age, ethnicity, gender, sexual preference, national origin, religious preference, skin color, or other characteristic.

Privacy protection does not primarily seek to prevent discrimination. Many personal characteristics are used legitimately to distinguish between individuals. Physicians use age, sex, and racial data to make appropriate choices about treatment of patients. These choices are not necessarily improper. Merchants use information about age and credit of customers for transactions that are lawful and profitable. These activities are not necessarily improper. Government agencies use PII to make decisions about the allocation of benefits to individuals. These decisions are not necessarily improper.

Some forms of discrimination are invidious or illegal. Judgments about what constitutes discrimination vary significantly across the globe, and legal protections differ from country to country. In some cases, a method for preventing discrimination may include limiting the collection of PII. However, when the goal is preventing discrimination based on gender, the gender of an individual may be obvious on sight. Even if information is not recorded, it may not make a difference to achieving an anti-discrimination goal when the information is available otherwise to a decision maker.

Information privacy often seeks to minimize the collection of information as a general principle. In some cases, data not collected may have consequences for discrimination goals. For example, a society might prohibit the collection of handedness information in order to prevent discrimination against left-handed individuals. Yet without the availability of handedness information, it may be impossible to determine after-the-fact if discrimination occurred anyway. Those making discriminatory judgments might rely on unrecorded information or on other information that correlates with handedness in some way. The collection of information to monitor discrimination may be at odds with the privacy goal of minimizing information collection. This is an example where privacy and discrimination goals conflict.

In some instances, individuals will be improperly classified and treated unfairly because the information used for classification is wrong. One privacy standard gives individuals the right

to inspect and seek correction of records. An accurate record may prevent improper discrimination, though this is not always the case. Having correct information furthers both privacy and discrimination objectives.

Data protection standards sometimes seek to prevent or minimize the collection of so-called *sensitive* information. The European Union places additional restrictions on the collection of "special categories of data," including data related to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and health or sex life.[53] The Directive does not make the purpose of the limitations explicitly clear, but limiting collection of data that many people consider more private may further both pro-privacy and anti-discrimination goals. In contrast, the US limits the ability of federal agencies to collect information about an individual's exercise of First Amendment rights (free speech, religion, free press, assembly, and petitioning the government). [54] The goal is probably more to prevent overreaching agency activities than to prevent discrimination against any class of individuals.[55]

Professor Oscar Gandy has written extensively about privacy and discrimination, including the more subtle discriminatory effects that can result from large accumulations of personal data. He supports the argument here that privacy and antidiscrimination goals are not the same.

> [A] privacy or data protection regime will not be adequate to the task of reducing the cumulatively disparate impact of autonomous discriminators. Privacy and data protection regimes focus primarily on the correctness of the "personally-identified information" stored within a database. It simply will not be economically or even technically feasible for data subjects to assess and then challenge the "correctness" or accuracy of the data or analytical models used by sentinels, agents, or environments.[56]

In other words, even when privacy and discrimination goals overlap, remedies will differ. Privacy may assist in meeting some anti-discrimination objectives, but it will not do so completely or consistently.

5. Centralization and Surveillance

In 1988, Australian privacy analyst Roger Clarke introduced the term *dataveillance* to mean the systematic monitoring of people's actions or communications through the application of

---

[53] *EU Data Protection Directive* at Art. 8. Member States can establish other types of sensitive information. Id at Art. 8(6)

[54] US Constitution, amend. 1, http://www.law.cornell.edu/constitution/billofrights#amendmenti.

[55] 5 U.S.C. § 552a(e)(7), http://www.law.cornell.edu/uscode/text/5/552a.

[56] Oscar Gandy, *Engaging Rational Discrimination: Exploring Reasons for Placing Regulatory Constraints on Decision Support Systems*, 15 Ethics and Information Technology 12:29–42, 39 (2010).

information technology.[57] Any identification system raises issues of dataveillance, with biometric systems raising some additional concerns.

The use of an identification system can, but need not, create detailed usage or transaction records. Consider an ID card that a user presents to engage in a transaction or activity that is reported to a central database. The central database may keep a record each time it receives a request for identification. Depending on how those records are maintained, the file for each individual could reveal each time the individual obtained benefits from a government agency, patronized a merchant, used a credit card, received health care, withdrew money from an automated teller machine, borrowed a book from a public library, accessed the Internet, used public transportation, or engaged in any other activity that relied on verification of identity. The record would not only show the activity – possibly include a variety of details about the transaction, such as amount withdrawn from an ATM – but the time and location when the activity occurred. The resulting centralized file would provide a detailed history of each individual's activities, perhaps over an extended period. That type of identification system with its comprehensive activity records would constitute a surveillance system.

For many individuals, a detailed transaction history may be a matter of limited concern most of the time because their activities are routine and mundane. However, political figures, celebrities, journalists, law enforcement agents, military members, judges, dissidents, refugees, and other classes of users may feel differently. For some, a compiled transaction history may become fodder for political campaigns, personal enemies, blackmailers, newspapers, police, government security monitors, and others.

Contrast that example with an ID card that does not rely on a central database. An individual presents an ID card and local equipment verifies the individual's identity from information on the card. Information about the transaction or activity remains local, and no one maintains a central database. This result is much more welcome from a privacy perspective, but it may require tradeoffs in terms of security, reliability, or other features.[58]

The absence of a central database that includes transaction details is a better design for information privacy. The creation of a record of transactions or activities for each identified individual compiles data in a way that does not occur generally today. The centralized records might attract users in government and in the private sector, which might want to exploit the records for marketing and other commercial purposes. Anyone wanting to track the location of an identified individual might seek access (lawful or otherwise) to the central database of transactions.

---

[57] Roger Clarke, Information Technology and Dataveillance, 5 Commun. ACM 498-512 (May 1988), http://www.rogerclarke.com/DV/CACM88.html.

[58] The discussion here addresses two models, one with transaction reporting to a single central database and the other without reporting. Other models are possible including reporting to different databases (rather than a single central database) depending on the type of transaction. The amount transaction information reported can also vary. Different models will have different consequences for privacy.

The point is that the design of any identification system obviously makes a difference to its privacy consequences. Many potential demands for data can be avoided altogether if information is not included in the system. The two alternatives presented here are not the only possible architectures. It may be possible, for example, to maintain information about the entity that sought identity verification rather than information about the transaction undertaken by the data subject.

There may be other factors to the design choice. Choices about allocating liability may be important. If a central registrar bears liability for improper identifications, then more extensive central record keeping may be needed than if each user of an identification system bears the risk. The reliability and cost of telecommunications may matter. The ability to provide security in central or remote locations may matter. Strict rules limiting data retention may allay some but not all privacy concerns.

One aspect of an identification system where certain types of biometrics add a significant additional risk to privacy results from the possibility of a different type of surveillance. The simplest example comes from facial recognition, although other types of biometrics may create the same opportunity. If a biometric identifier allows the identification of an individual without the individual's knowledge and consent, then the possibility exists that everyone identified in the system could be tracked when walking down the street or in other public or private locations. With enough cameras connected to a central database of facial photographs, it would be possible to trace every movement of every individual with a biometric identifier. With enough computing power, real-time tracking of individuals could result. Ubiquitous surveillance of individuals in public has obvious unwelcome privacy consequences.

6. What types of PII can biometrics reveal and how may it be collected?

Depending on the technology used, biometrics may reveal some information about health characteristics or other personal information. For example, a facial recognition system may capture information on scars, tattoos, deformities, or specific health conditions. A fingerprint identifier is less revealing. Much will depend on how an identification system stores information. A facial recognition system that stores a photograph may have the potential to reveal more health information than a system that reduces a facial image to a code. The same is true for some other forms of biometrics, especially if an identification system stores samples (e.g., DNA samples) rather than data or coded data.

For some forms of biometrics, some individuals lack the required physical attribute or cannot perform the behavioral activity needed. Some people do not have fingerprints or hands. Some people may not be able to talk, write, type, or walk. If the identification system captures these incapacities and provides an alternative form of identifier, the system will necessarily include physical or information about some individuals. That information is PII and may be health information.

Perhaps the ultimate biometric is DNA. If an information system uses some or all information derived from DNA, the data used constitutes PII that might include personal information about the health of the data subject and even about the health of the data subject's relatives. Even the limited amount of DNA used today for identification may eventually reveal personal characteristics.[59]

Any privacy analysis must take into consideration the possibility that some health information may be part of a biometric identification system. Whether any particular data element would be objectionable would depend on many factors, including local sensibilities. The EU Directive categorizes all health data as sensitive,[60] but the Directive allows non-consensual processing under some circumstances.[61] In the US, federal law regulates the processing of health data by health care providers and health insurers, but the health data regulations do not cover banks, marketers, gyms, and others who may process the same health data.[62] In any country, there may be specific rules or general concerns that may or may not extend to the processing of any health data captured and used by a biometric identification system. These rules and concerns would be part of a privacy analysis. Many issues respecting the definition of health data remain unexplored here, except for the observation that it is not always clear how to distinguish between health and non-health data.

The possibility that health data may be part of a biometric identification system is not fatal to the adoption of a system. A privacy evaluation should consider any PII that becomes part of a biometric identification system, the rules applicable to that class of PII, the concerns that would arise within the affected jurisdiction, and any concerns and traditions of the population affected by the system.

The same need for consideration of local sensitivities is true for the process used to collect biometric identifiers. Different cultures may be more or less accepting of an identification system's need to take facial photographs. In many countries, few would object. In some regions, local religious or fashion practices could present barriers. Perhaps in all countries, a biometric that required individuals to disrobe would not be acceptable. In the United States, the association of fingerprinting with criminal law enforcement limited popular acceptance

---

[59] DNA once considered "junk DNA" with no significance has been found to have important uses. See, e.g., *'Junk' DNA Has Important Role, Researchers Find*, Science News (May 21, 2009), http://www.sciencedaily.com/releases/2009/05/090520140408.htm. This development suggests the need for caution when making choices based on current knowledge of DNA attributes. The use of DNA, whether in the form of information or samples, has the potential to arouse greater concern about privacy and especially about secondary uses. A DNA database would be likely to attract great demands for health research, law enforcement, and national security uses, some of which might be politically difficult to resist at times, and regardless of the conditions under which the DNA was collected.

[60] *EU Data Protection Directive* at Art. 8(1).

[61] *EU Data Protection Directive* at Art. 8(2)-(5).

[62] Health Insurance Portability and Accountability Act, 45 C.F.R. Parts 160, 162 & 164. http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=dedf774127f09bc1a708447c5828fe80&rgn=div5&view=text&node=45:1.0.1.3.76&idno=45.

for a time, but objections diminished as the technology became more familiar and more widespread.

Applying privacy policy and processes to biometric identification systems

This section of the report seeks to move a step closer to applying privacy standard and practices to the development and implementation of biometric identification systems. The goal here is to show at a high level of generality how FIPS, Privacy by Design (PbD), and Privacy Impact Assessments (PIAs) might be useful in addressing privacy concerns. FIPs offer the substantive content for a privacy policy. PbD offers a pro-active approach to the protection of privacy that relies on advance planning rather responding to problems after they arise. PIAs offer a formal way to consider and assess the privacy consequences of technology or other choices, including consideration of alternatives early in the planning stages. These three methodologies are not mutually exclusive and can be combined to achieve a better result.

Using FIPs to develop laws, policies, and best practices

The elements of Fair Information Practices provide general standards for designing, operating, and evaluating the information privacy features of any information system. A review of FIPs with suggestions how they might shape a biometric identification system follows. As previously stated, FIPs can be implemented in many different ways so the ideas presented here include only some of the available options. The FIPs principles can and should always be adapted to the technologies involved, applicable laws, and local institutions and needs.

Collection Limitation Principle

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.

Limiting the collection of personal data is important because the collection and maintenance of personal data elements may be unnecessary, may increase costs, may affect the rights and interests of data subjects in known and unforseen ways, and is likely to result in greater pressure to use the data for secondary purposes. Data not collected does not become part of a central file on individuals, need not be protected against misuse, will not become a target for criminals seeking to engage in identity theft, and will not attract secondary users.

Collecting the minimal amount of data does the most to protect privacy. A biometric identification system might be able to function with only a name and one or more biometrics. Gender and data of birth might be important depending on the intended uses for

the identifier. Each data element collected should be evaluated and debated. The casual inclusion of information that "might be useful someday" should be resisted.

If a country intends to use biometric identification for a variety of purposes, then there may well be justification for additional data elements. The principle of collection limitation does not mandate any specific set of data elements. Rather, it asks that there be a good reason for each element collected.

The collection of information by fair and lawful means may not be difficult to meet in most circumstances. An example of an unfair data collection would be telling data subjects that the system collects facial photographs but not informing them that the system secretly collects iris scans as well.

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.

The relevance standard of the data quality principle is consistent with the collection limitation principle. Data that is neither necessary for nor relevant to the purpose of a biometric identification system should not be collected or maintained. When data is not collected, no costs are incurred for keeping the data accurate, maintaining security, or granting individuals rights of access and correction.

It is important to recognize that the accuracy, completeness, and currency standard of the data quality principle is qualified by the phrase *to the extent necessary*. The principle does not mandate the expenditure of resources to change records regularly unless the purpose of the systems requires that the records be accurate, complete, or up-to-date. A record necessarily kept for an archival purpose would not require updating if the old record would not affect a current or future right, benefits, or privilege of the data subject. For a biometric identification system, the principle would not require, for example, that a photograph taken ten years earlier be replaced by a more current photograph as long as the original photograph remains adequate for identification.

A data privacy element implied by the data quality principle is that a record containing PII should not be maintained at all if no longer needed. Alternatively, the record should not be kept in identifiable form longer than necessary. For a biometric identification system, the basic function may legitimately require that core records remain identifiable permanently. Consider, however, if the identification system also collects transaction information each time someone verifies an individual's identity. The transaction information may be needed for determining liability or for another defined purpose. When the purpose has been fully satisfied (e.g., the statute of limitations for assessing liability expires), the need for

identifiable transaction records may no longer exist. The records might be discarded entirely at that time or adequately de-identified if the records have research value. The EU Directive, for example, directs Member States to establish appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.[63]

Purpose Specification Principle

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 [the Purpose Specification Principle] except: a) with the consent of the data subject; or b) by the authority of law.

The purpose specification principle works together with the use limitation principle, and both are considered together here. The specification of the purposes for any personal data processing implements the general policy that data collected for one purpose should not be used for another purpose. Failure to follow this principle is what allows mission creep to occur. It may be unfair to ask an individual to provide personal information for any given activity and then to use that information for another purpose without either notice to the individual or consent. For example, it would be inappropiate to ask citizens to cooperate with a national census for the stated purpose of collecting statistical information for use on a non-identifiable basis and then to allow the police to use individual responses to consider criminal charges against the citizens.

Implementing the purpose limitation and use limitation principles consistently and fairly can be challenging. A biometric identification system can, consistently with the data quality principle, be used for a wide variety of *identification* activities. However, using an identification system to also determine program eligibility, to look for research subjects, or for other unrelated purposes would likely violate the purpose and use principles if those other purposes were not defined in advance. Another example of a broader and questionable activity is the use of an identification system as a general purpose surveillance system. If

[63] *EU Directive*, Art. (6)(1)(e).

allowed, any identification system that maintains location or transactions may allow police or other government agencies to track individuals, particularly if done without any lawful process such as a search warrant or other measures (e.g., high-level supervisory approval and/or for specific and limited purposes of compelling importance). Any identification system runs the risk of becoming a general purpose surveillance system in the absence of clearly defined limits.

The purpose and use principles recognize a number of important exceptions. First and most important is the specification of purpose at the time of collection. Nothing in the principle expressly prevents a broad statement of purpose. Thus, an identification system that stated as its purpose determining both identification and program eligibility would not violate the principle by making eligibility determinations. Indeed, it would be possible in theory to define *any lawful activity* as a purpose. However, an overly broad or vague purpose statement would mock rather than implement the principle. The EU Directive attempts to address this concern by stating in a recital that purposes *must be explicit and legitimate*.[64]

Second, the principles recognize that it may not be possible or practical to specify in detail and in advance each purpose for which personal data is intended to be used. For example, any collection of personal data for identification may be subject to quality review by auditors or criminal review by police investigating misuse of the system by those in charge of system operations. These activities might not always be identified expressly in advance.[65]

The principle recognizes the problem by allowing use for other purposes that are *not incompatible* with the stated purposes. For example, the EU Directive expressly states that secondary activities for historical, statistical, or scientific purposes are not considered as incompatible with the purpose of any system.[66]

The incompatibility standard is a difficult one, and, frankly, its vagueness allows for mischief.[67] The EU exception for historical, scientific, or scientific purposes illustrates the breadth of activity that arguably qualifies as *not incompatible*. That particular judgment may be reasonable, but it can be difficult to control abuse of the standard.

---

[64] *EU Directive*, recital 28.

[65] An example of an activity for some data systems rarely considered in advance is locating individuals following natural disasters. A recent report highlights some of the privacy problems raised by this type of humanitarian activity. See Joel R. Reidenberg et al, Privacy and Missing Persons After Natural Disasters (2013), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2229610.

[66] *EU Directive*, at Art. 6(1)(b).

[67] A US privacy law – the Privacy Act of 1974 applicable to federal government agencies – has a similar standard for allowable disclosure for specific collections of personal data. The Act allows each agency to define allowable disclosures ("routine uses") that are "compatible with the purpose" for which a record was collected. 5 U.S.C. § 552a(a)(7) (definition of routine use) & (b)(3) (authorizing agencies to define routine uses), http://www.law.cornell.edu/uscode/text/5/552a. The Act has been criticized from the beginning because it allows agencies to interpret the compatibility standard too loosely. See, e.g., Privacy Protection Study Commission, Personal Privacy in an Information Society 517 (1977), http://aspe.hhs.gov/datacncl/1977privacy/toc.htm.

There are ways to impose controls on abuse of the incompatibility standards. Procedural controls may help, such as requiring appropriate supervisory approval, preventing individual staff members from making ad hoc determinations, notifying individuals of specific uses, or even requiring advance publication of any new *not incompatible* purposes. Advance legislative notice is also an option. Another is public notice and comment on any determination regarding purposes determined to be not incompatible. Review or approval by a Chief Privacy Officer or other data protection supervisory official may also provide some discipline.

Third, the principle allows uses with the consent of the data subject. For many activities involving personal data and large numbers of data subjects, however, it will be impractical to rely on consent. The administrative costs of managing consents can be high. It may nevertheless be appropriate to use consent for some activities. An example is a research project looking at the uses of a biometric identification system in health activities. A research project of that type may also be appropriate for review by a human subjects protection process, which may or may not include waivers of the need to obtain individual consent. Much would depend on national standards and existing policies for controlling research.

Fourth, the principles allow use by authority of law. A later statute can expand the purpose for an identification system and allow use of a biometric identification system for a new purpose not originally provided for by the statement of purpose. Later statutes can also be the cause of mission creep by expanding purposes far beyond the original plan.

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.

The security safeguards principle is a high level statement that personal data should be protected by reasonable security safeguards. The principle specifies the need for protections against loss, unauthorized access, destruction, use, modification, or disclosure. Concerns about identity theft suggest that record keepers bear a significant burden of protecting their data subjects from being the subject of criminal activity. Because security requirements vary over time and technology, the principle goes no further than generalities.

The security threat to a biometric identification system is significant. The use of encryption and specifically biometric encrytion may be appropriate or necessary given the value of an identification database and the threats posed by hackers, criminals, and other governments. As a country places greater reliance on biometrics to identify individuals for financial and other basic activities, the risk of a breach of an identity database may also increase. Details about security are beyond the scope of this paper, except for the observation that it has

become a common practice to conduct a *risk analysis* (or *risk assessment*) of the appropriate security requirements for any complex information system.[68]

One security-related issue that grew in prominence after the promulgation of FIPs is breach notification. Following the lead of the US State of California in 2002, many provincial and national legislatures around the world enacted legislation mandating notice to data subjects about the loss or unauthorized acquisition of an information resource containing PII. The scope and standards of these these laws vary, and the details are not important here. However, many organizations that suffered a breach learned that the cost of providing notice to data subjects can be large, and other consequences are also potentially disruptive and significant.[69] Some laws limit breach notificaition obligations when the underlying data is adequately encrypted.

For a biometric identification database, providing a breach notice to the presumably large numbers of individuals in the database could be an enormous undertaking.[70] If a breach made an identification system unusable or unreliable, repair or replacement could be costly and broadly disruptive, especially if a country relies on single identification system for multiple purposes.

Whether a breach notification law applies in any given situation would depend on any legislation establishing the biometric database or other legislation generally applicable in the jurisdiction. Even if there were no applicable legal requirement, any identification system might adopt breach notification as a matter of policy. Regardless, today any database with PII should have a policy and procedure addressing breach notification as well as plans for responding to an actual data breach.

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 and usual residence of the data controller.

[68] See, e.g., International Organization for Standardization, ISO/IEC 27002 (a standard establishing guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization), http://www.27000.org/iso-27002.htm. Laws in various jurisdictions sometimes mandate risk assessments for governmental or private databases containing personal information.

[69] The Ponemon Institute has conducted several studies of the cost of data breaches. See generally http://www.ponemon.org/library.

[70] When the number of affected individuals is large, some breach laws allow notice through newspapers or other mass media in place of individual notice.

The openeness principle requires that any data subject be able to learn of the existence of a processing operation, who is the data controller for that processing, and what personal data is being processed. Clearly explaining data policies and the limits of those policies should contribute to consumer acceptance of an identification system and diminish fears. For a biometric identification system that requires the cooperation of each data subject, meeting the openness principle should not be difficult. Full particulars of the system should be available by means appropriate to the nation where the system operates. This may mean paper notices that each individual registering in the system can keep, along with Internet notices. Notices should include information that allows each data subject to exercise his or her rights to individual participation.

Individual Participation Principle

An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) 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; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

This principle cover access and correction rights. Each individual should have a right to know whether a data controller has data pertaining to the individual; a right to see and/or copy that data; a right to be given a reason if a request for access is denied and to challenge the denial; and a method to challenge data that is not accurate or complete.

For a biometric identification system, these rights are particularly important. First, if a biometric identifier is necessary to exercise basic human rights, the right to review and seek correction of the records becomes the equivalent of a human right as well. An individual without a working identifier may not be able to function in society. This is of the highest importance, for example, if a biometric identifier is needed to vote to to exercise other political rights. It may be just as important if the identifier is necessary to engage in economic transactions. In his classic novel 1984, George Orwell coined the word *unperson* to mean an individual who usually for political or ideological reasons is removed completely from recognition or consideration. In a society where a biometric identifier is necessary to function, an individual without a working identifier may be an political or economic unperson.

Second, if a biometric identifier is not adequately reliable and secure, one individual may be able to exercise the rights of another. Identity theft, which is the misuse of another individual's personal information to commit fraud, may be the result. An individual who is the victim of identity theft tied to a biometric identifier needs a fast and effective remedy. The epidemic of identity theft in the United States illustrates that it can be difficult for a victim to convince data controllers that a crime occurred, that records need to be corrected, that the errors not be reintroduced repeatedly, and that new identity credentials are needed.[71] A biometric identification system must be prepared to address the problem of a compromised identifier.

Third, a feature of biometrics already discussed briefly above is that it may not be possible to reissue a compromised biometric. An individual can receive a new identification number or card following a compromise of the old one. An individual cannot receive a new fingerprint if a thief manages to copy that fingerprint (or the digital code for that fingerprint) and impersonate the individual. Some forms of biometric encryption may offer a remedy for this problem, and there may be other methods including the use of more than one biometric identifier. However, regardless of the technology employed, an individual should be able to obtain an adequate substitute for a compromised biometric identifier. A method for addressing the problem of compromised identifiers is implied by the right of individual participation.

The right to see and seek correction of records may be important in other, less dramatic circumstances. Some records may simply be wrong for a variety of mundane reasons. For example, an individual whose identifier wrongly represents his gender or her date of birth must be able to ask for and receive a correction promptly and preferably at no cost. Maintaining accurate and current records in any identification system benefits users and data subjects alike.

Accountability Principle

A data controller should be accountable for complying with measures, which give effect to the principles stated above.

There are many ways to provide accountability measures for FIPs. For example, the accountability principle for compliance with FIPs can be met with civil or criminal penalties, civil lawsuits, administrative enforcement, arbitration, internal or external audits, complaint processing, staff training, a privacy office or officer, and more. As an information system grows in importance, more measures may be appropriate. Some accountability measures focus on providing individuals with their rights under law. Some measures focus on

[71] See generally The President's Identity Theft Task Force (US), *Combating Identity Theft: A Strategic Plan* 45 (victim recovery) (2007), http://www.identitytheft.gov/reports/StrategicPlan.pdf

institutional accountability. Obviously, accountability measures in any jurisdiction must reflect the legal, administrative, and culture norms of that jurisdiction.

A chief privacy officer (CPO) requires more discussion. A CPO is an official in a government agency, business, or organization who typically is responsible for managing the institution's privacy policy and its response to privacy laws. CPOs are relatively new institutions, arising in the last fifteen years.[72] The 1990 German Federal Data Protection Law was the first to require an in-house data protection official for many non-governmental companies and organizations.[73] CPOs are not the same as privacy supervisory authorities established under the EU Directive in Member States at the national level and found in other countries as well.[74] Some countries also have provincial supervisory authorities.

A CPO functions at the organization level or, sometimes, at the program level. EU privacy supervisory authorities must operate with "complete independence."[75] In Germany, in-house data protection officials by law have a degree of independence from corporate management.[76] Given the potential importance and scope of a national biometric identification program, it may be suitable for the program to have its own dedicated and, perhaps, independent CPO. Full independence for a CPO may not be possible, but the authority to report directly to the head of the agency operating the program, to the legislature, and to the public may be worthy of consideration. A CPO with sufficient authority can be especially valuable in representing the interests of data subjects, identifying and limiting mission creep, reviewing security measures, and addressing data breaches.

Privacy by design

Privacy by Design (PbD) is a more recent concept that emphasizes the idea of adopting a proactive rather than a reactive compliance approach to the protection of privacy. PbD originated with work done in the 1990s by Ann Cavoukian, Information and Privacy Commissioner, Ontario, Canada.[77] Dr. Cavoukian has been a principal advocate for PbD.

---

[72] See generally Kenneth A. Bamberger & Deirdre K. Mulligan, New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry (2011), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1701087.

[73] See generally Douwe Korff, New Challenges to Data Protection Study - Country Report: Germany 48 (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1638959.

[74] EU Data Protection Directive at Art. 28. The EU ministry responsible for data protection maintains a list of national supervisory authorities. http://ec.europa.eu/justice/data-protection/bodies/index_en.htm.

[75] EU Data Protection Directive at Art. 28(1).

[76] Douwe Korff, New Challenges to Data Protection Study - Country Report: Germany 49 (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1638959.

[77] See Ann Cavoukian, Privacy by Design: The 7 Foundational Principles (2011), available at http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf. A 2012 European Union Article 29 Working Party opinion supported PbD for biometric identification systems. See Opinion 3/2012 on developments in biometric technologies (2012) (WP193), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf,

The idea of PbD is useful, especially when creating an information system or other activity that makes intensive use of PII. The seven foundational principles of PbD as described in a recent paper coauthored by Ann Cavoukian are:

1. ***Proactive*** not Reactive; ***Preventative*** not Remedial

The *Privacy by Design* approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events. It does not wait for risks to materialize, nor does it offer remedies for resolving infractions once they have occurred – it aims to prevent them from occurring. In short, *PbD* comes before the fact, not after.

2. Privacy as the ***Default Setting***

We can all be certain of one thing – the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, his or her privacy remains intact. No action is required on the part of the individual to protect his or her privacy – it is built into the system, by default.

3. Privacy ***Embedded*** into Design

Privacy is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. Full Functionality – ***Positive-Sum***, not Zero-Sum

PbD seeks to accommodate all legitimate interests and objectives in a positive-sum, or doubly enabling "win-win" manner, not through the dated, zero-sum approach, where unnecessary trade-offs are needlessly made. It avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible, and far more desirable, to have both.

5. End-to-End Security – ***Full Lifecycle Protection***

Privacy, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, and in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, lifecycle management of information, end-to-end.

6. ***Visibility*** and ***Transparency*** – Keep it ***Open***

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations must remain visible and transparent, to users and providers alike. Remember, trust but verify!

7. ***Respect*** for User Privacy – Keep it ***User-Centric***

Above all, *PbD* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric – focused on the individual.

Respect for user privacy (like the other *PbD* principles) is not a stand-alone principle. It is intertwined with the remaining principles, enabling users to become empowered to play an active role in the management of their personal data. This in turn creates an effective check against abuses and misuses, and ensures higher levels of data quality and accuracy.[78]

In some ways, PbD is a successor to the earlier notion of Privacy Enhancing Technologies (PETs), which are information and communications technology measures to protect privacy by eliminating or minimizing PII. An example of a PET is an anonymizer that hides the online identity of a user. Although PETs attracted attention for a time, the idea did not have widespread influence. While PbD has attracted some broader interest at present, both it and PETs appear to be good basic ideas that lack enough specificity to offer detailed guidance or benchmarks to address the design of a biometric identification system. Nevertheless, the principles of PbD listed above offer some useful ideas and are compatible with FIPs. The PbD principles are also compatible with privacy impact assessments, offering both a foundation and justification for them.

Privacy impact assessments

Privacy impact assessments (PIAs) emerged in recent years as a useful tool for evaluating the effects of any activity on privacy. In Europe, they are often called *data protection impact assessments*. David Wright and Paul De Hert, editors of a recent book on PIAs, offer this definition:

> A *privacy impact assessment* is a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative

[78] Ann Cavoukian & Marc Chanliau, *Privacy and Security by Design: A Convergence of Paradigms* 11-12 (2013), http://privacybydesign.ca/content/uploads/2013/01/pbd-convergence-of-paradigms-oracle-web.jpg. See generally http://privacybydesign.ca.

> which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts.[79]

The book collects a variety of other definitions used in different countries, most with a significant degree of similarity. Core ideas are identifying and evaluating risks to privacy, considering compliance with privacy legislation, and addressing ways to mitigate or avoid the risks. Wright and De Hert emphasize that a PIA is a *process* that should begin at the earliest possible stages when there are still opportunities to influence the outcome of a project and that a PIA can continue to play a role even after a project has begun.[80] The idea behind a PIA *process* is a counterweight to the concern that a PIA will be a report prepared only to meet a legal requirement and that a PIA will have no meaningful influence on the development or implementation of a PII intensive activity.

PIAs appear to have originated in the United States in 1996 with the privacy advocate at the Internal Revenue Service.[81] The idea spread to other countries, including Canada, Hong Kong, New Zealand, Australia, and elsewhere. In many places, data protection supervisory authorities support and encourage government and private entities to conduct PIAs, and some provide guidance.[82] In some countries, PIAs are sometimes required by law. In the United States, for example, federal agencies must conduct PIAs when developing information technology systems that collect, maintain, or disseminate identifiable information about members of the public.[83]

The basic idea and value of a PIA has achieved a significant degree of consensus in countries that have paid the most attention to privacy policy matters. While a PIA is not expressly dependent on either PbD or FIPs, a PIA can be viewed as a marriage of the *plan ahead* notion of PbD with the standards established by FIPs (or other statement of privacy principles, if available). The result is an advanced evaluation of the privacy consequences and privacy risks of any personal information system or activity at a time when information system designers can provide the most practicable and achievable result for the protection of privacy consistent with other goals and objectives. At its core, this is the same notion behind environment impact statements and regulatory impact assessments.

---

[79] David Wright & Paul De Hert, *Introduction to Privacy Impact Assessment* at 5 in Privacy Impact Assessment (David Wright & Paul De Hert, editors, 2012) (hereinafter cited as *Wright & De Hert*).

[80] Id.

[81] Id. at 9.

[82] See, e.g., Privacy Commissioner (New Zealand), *Privacy Impact Assessment Handbook*, http://privacy.org.nz/privacy-impact-assessment-handbook.

[83] E-Government Act of 2002, Public Law 107-347, § 208, 44 U.S.C. § 3501 note, http://www.law.cornell.edu/uscode/text/44/3501. See Office of Management and Budget, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (2003) (M-03-22), http://www.whitehouse.gov/omb/memoranda_m03-22.

The PIA process may be especially well-suited for use with biometrics. A biometric identification system relies heavily on technology. A system may affect many disparate institutions both in and out of government, include most or all residents of a national or region, affect the rights, privileges, and opportunities of individuals, require high-levels of physical, administrative, and technical security measures, and present significant privacy risks to individuals. PIAs would be just as valuable for any identification system, but use of biometrics presents a range of additional technical choices that need a detailed study of the options and consultation with users and individuals affected by the system.

Scholars and practitioners from different countries who have written about PIAs have been critical of many actual PIA implementations.[84] Problems commonly identified are a lack of openness, inconsistency, political barriers, conflicts of interest, insufficient resources, absence of accountability, and badly timed reviews. For all of the criticism, however, the same writers also find some successes and enough promise in the PIA process for all of them to believe that PIAs can be a useful tool despite the shortcomings.

Examples of PIAs

It is difficult to offer short descriptions of PIAs because of the need for background knowledge of law, administrative practice, politics, and history, among other things to achieve a full understanding. Nevertheless, a few examples are offered here based on Wright & De Hert's Privacy Impact Assessment and other sources.

• Hong Kong.[85] Multiple PIAs were commissioned for the Hong Kong Smart ID card which contains a microchip and biometric information. The recommendations of the first, in 2000, were not well received, and the full PIA was not made public for over a year. Three more PIAs were conducted, and not all of them became public. The later PIAs focused on detailed system designs and procedural safeguards rather than the broader justifications for privacy intrusion, alternatives, and function creep that were raised at earlier stages. The study concludes that all parties need to have a more sophisticated understanding of the practical and political realities when commissioning, reading and using PIAs.

• New Zealand.[86] In 2003 a New Zealand agency was considering options for online authentication for e-government services. A PIA was commissioned early in the process and was conducted by a project team committed to addressing

[84] See *Wright & De Hert*.

[85] Nigel Waters, *Privacy Impact Assessment in Hong Kong from an International Perspective* (2010), available at http://www.cyberlawcentre.org/2010/Waters_PIA_Dec_2010_v2.pdf.

[86] Nigel Waters, *Privacy Impact Assessment – Great Potential Not Often Realised in Wright & De Hert* at Chapter 6.

privacy issues. The warnings in the PIA about privacy risks inherent in the more ambitious options appear to have resulted in more focused and less intrusive choices. A key recommendation adopted was the concept of federated identity and managing multiple identities.

• United Kingdom.[87] The UK Office for National Statistics (ONS) conducted a PIA for the 2011 census. Finding expertise was difficult. The PIA needed to be conducted internally and came late in the review process. Partly because of its timing and rigorous preparatory work by ONS, it found nothing unexpected. It was nevertheless helpful in pulling together different parts of ONS' work and also provided further evidence that the agency took privacy seriously. With hindsight, ONS stated that earlier consultation with privacy regulators and stakeholders would have been better.

• United States.[88] The U.S. Department of Homeland Security (DHS) planned US-VISIT as an immigration and border management system. The system collects biometric data (digital fingerprints and photos)) and checks the data against a database to track non-US citizen visitors to the US with the goal of identifying individuals deemed to be terrorists, criminals, and illegal immigrants. DHS conducted meetings with privacy and immigration organizations, published two separate PIAs, collected comments on the PIAs, and reflected those comments in the ultimate design of the project. A leading privacy advocacy group found the process to be a good model, although not entirely without flaws.

While there is much consensus about PIAs at the highest level of abstraction, there is considerable divergence of opinion about how to conduct a PIA. Efforts at standardization are underway. The European Union's Privacy Impact Assessment Framework for data protection and privacy rights (PIAF) seeks to encourage the EU and its Member States to adopt a PIA policy to address privacy. The project reviewed PIA policies in several jurisdictions, researched the factors that affect adoption of a PIA policy, and offered two sets of recommendations. The first set – for policy makers intending to develop a PIA policy in their jurisdictions or improving existing ones – considers the rationale and methods of introduction of a PIA policy, identifies and describes the elements of a PIA, and discusses

---

[87] Adam Warren & Andrew Charlesworth, *Privacy Impact Assessment in the UK* in *Wright & De Hert* at Chapter 9

[88] Kenneth A. Bamberger & Deirdre K. Mulligan, PIA Requirements and Privacy Decision-Making in US Government Agencies in Wright & De Hert at Chapter 10.

the role of data protection authorities. The second set – addressed to the assessors actually carrying out PIAs – offers guidance on best practice.[89]

There is no single way or "right" way to conduct a PIA. Nor is there a guarantee that a PIA will have an influence or make a difference. A poorly conducted PIA can be useless or worse by giving the appearance that privacy was assessed even though the assessment was not even-handed, thorough, timely, or given attention. Program managers can ignore even a well-done PIA if they choose to assume that the preparation of a PIA meets their obligation and that implementation of the recommendations of the PIA is unnecessary.

Another factor affecting a PIA is cost. A full PIA on a complex undertaking such as a biometric identification system can be expensive on its own terms. In addition, if properly utilized, the time needed to conduct the PIA (perhaps in multiple stages) and recommendations for change may affect implementation of the system, possible increasing costs in other ways. Better planning, of course, may result in a better and lower cost system. In any event, resource limits may determine the terms of a PIA.

As with many other human activities, a PIA will succeed more often when prepared by a dedicated individual or group and when received and acted upon in good faith by program managers. In the United States, the Department of Homeland Security took an indifferently written statutory PIA requirement and turned it into a meaningful and effective tool that on some occasions influenced departmental operations on behalf of privacy. Other comparable government departments applying the same statute produced thin reports that no one reviewed and that had no effect.

The discussion that follows of the principal questions surrounding PIAs sets out the issues. The questions presented are not wholly independent of each other. Thus, choices made about who will conduct a PIA may influence the timing of the PIA.

Whether

Does every project involving PII require a PIA? While there is much to debate on this question, the answer is simple in the context of this report. It would be appropriate that any biometric identification system involving a significant number of individuals should include a PIA. A national or regional identification system is a major undertaking, collecting and using PII on many individuals with obvious privacy consequences. The consequences should be evaluated in advance.

Who

Should the manager of an information project conduct the PIA? This is not an easy question to answer. No matter who conducts the PIA, the possibility exists that there will be some

---

[89] Privacy Impact Assessment Framework, Recommendations for a privacy impact assessment framework for the European Union (Nov. 2012), http://www.piafproject.eu/ref/PIAF_D3_final.pdf . See generally http://www.piafproject.eu/Index.html.

type of conflict of interest resulting from the selection and payment of the assessor by the program manager. It may be hard to avoid this type of conflict entirely.

If conducted inside a project by the program manager and the manager's team, the PIA assessor will know more about the goals, plans, and design for the system, and that can be a distinct advantage. However, the team may not have sufficient understanding of privacy or other needed skills to do a complete job. A privacy assessment may require a high degree of computer security expertise, legal skills to evaluate privacy and other legal constraints, knowledge of encryption, and other knowledge as well. The biometric elements may require additional levels of technical expertise.

Other considerations may be important. If a government or a minister in that government publicly committed to a biometric identification system or to some elements of the system, it may be politically or bureaucratically difficult for an internal report critical of the system to succeed in moving through an agency, reach the highest level within the agency, or inform political or public debate on the project. Similarly, if the contractor designing or building a biometric identification system also conducts the PIA, the same political or bureaucratic barriers may arise. The contractor may be unwilling to criticize elements of its proposal that won the contract in the first place.

Further, a biometric identification can be structured in varying ways, including various combinations of centralized and decentralized elements. The basic idea of a single manager of the system may not be reflective of all the alternatives, suggesting the need to consider multiple perspectives when selecting who conducts the PIA.

An independent assessment offers the promise of impartiality, which may be especially valuable if skeptical funders, agencies, or members of the public need reassurance that privacy concerns were adequately considered and that the project design offers a reasonable balancing of the interests involved. However, it may be harder for outsiders to develop a full understanding of the goals and methods of the project, and an independent contractor may be more expensive than and internal assessor. It may also be more difficult to make use of the results of the PIA in planning the system, especially if the timing of the PIA does not coincide with the milestones for the project. Further, if the same external consultant undertakes PIAs for different agencies within the same government, the consultant may be concerned that a report unwelcomed by one agency will make it more difficult to obtain a new PIA contract from another agency.

A PIA need not be wholly internal or wholly external, of course. Blended approaches may work, perhaps with external or independent oversight of an assessment largely conducted by the project's staff, perhaps supplemented with other expertise. External review of a draft PIA by a privacy supervisory authority, by external stakeholders, or by the public may help to prevent a poor or one-sided PIA. Some form of peer review may also be useful. Unfortunately, there are no widely accepted industry standards for measuring the adequacy of PIAs. This may change over time.

When and What

The timing for preparing a PIA is another complex issue, and it is closely intertwined with a determination of what should be evaluated. It may be most appropriate for considerations of privacy to precede the design of the system or to otherwise begin at the earliest possible time. Any biometric identification system can have a wide range of designs, users, and purposes. The earlier that basic options can be evaluated, the better the chance that the result will meet overlapping objectives. However, an early review may not always be possible or practical. Some systems may be in late stages of planning or even in implementation before recognizing the value of a PIA. Evaluation of a new identification activity may have to build on existing activities that did not benefit from a privacy review and that may not be subject to change. Further, until a system design is determined – and especially if many designs are in competition – it may be difficult or too expensive to do a full evaluation of all alternatives. However, if the PIA only evaluates the final design of the project, then options that might have produced better outcomes for privacy may never have been considered.

One way to address the uncertainty of the timing is to conduct a PIA in stages, with a preliminary review at the earliest possible stage. A PIA can be an evolving activity, with a revised assessment as choices are narrowed and implementation decisions are made. However, an assessor too entangled with the decisions and decision-making may lose necessary independence and objectivity. Nevertheless, even a preliminary assessment of privacy may uncover options or pitfalls not previously considered.

The PIA process need not end when a project finishes planning or even when the project begins operation. Any major personal information project will seek to become more efficient, need to incorporate new technology, react to public and marketplace demands, and find new or additional ways to accomplish its mission. A PIA process could evolve into a continuous monitoring of a biometric identification system for fairness, compliance with established privacy standards, and consistency in operation. A chief privacy officer created to carry out continuing oversight for the system might carry out these activities. If a higher level national, regional, or departmental privacy supervisory authority exists, some of the continuing functions might be carried out, reviewed, or subject to approval by that authority.

How

How should a PIA be conducted? There may be many answers to this question. A first step is likely to be setting the terms of reference for the assessment. The terms of reference should describe the project so that the scope of the effort is clear. The description should include all planned processing of PII and cover the complete life cycle from information collection to information destruction. The terms should establish deadlines for the privacy report so that the assessment matches with project milestones. Terms may also describe resources available to the assessor, processes for review and comment, and publication expectations. If general privacy policies already established apply to the planned system, then the terms should reference those policies. If there is no established privacy policy, someone must provide the assessor with guidance on privacy standards or allow the assessor to develop and describe appropriate privacy measures.

Another preliminary step is selecting a suitable person to conduct the assessment. The qualifications of the assessor depend on the type of activity or project under review. A biometric identification system that may have broad use within a governmental context requires considerable knowledge of government policies and practices as well as familiarity with the government departments that will use the system. If the private sector will use the system, the assessor needs some familiarity with the institutions that will use it and the technologies they employ.

The assessor should provide a privacy risk assessment that enables identification of major areas of concern. Identification of and consultation with all relevant stakeholders is an essential part of the assessment. Obtaining the necessary biometric expertise is another basic requirement. Another task is reviewing or proposing suitable security measures, privacy-enhancing technologies, and other technological or managerial approaches that can improve privacy. Part of this effort requires identifying tradeoffs between privacy goals and other system goals. A closely related activity is a review of the adequacy of compliance mechanisms planned for the system.

Ideally, an assessor has a free hand in making recommendations to anyone involved in the planning, designing, building, or implementation of the project. The terms of reference should describe who the assessor reports to and who is responsible for responding to the assessor's preliminary or final report.

Publish

Should a PIA be published and when? The practice around the world varies considerably. PIAs are published in whole, in summary, or not at all. There may be security issues, proprietary information, or other concerns that militate against publication of parts of an assessment. It may be tempting to recommend full publication of all PIAs, but that policy may be impractical.

Nevertheless, publication brings many benefits, including making the PIA process more rigorous because of the knowledge that it will be made public. Publication provides an opportunity for public and other input that may help to find and correct deficiencies. Other benefits include greater public knowledge of and confidence in the project and in the agency sponsoring the project, and faster public acceptance of the new technology. Ideally, a PIA should be published at several different stages up to and including the final report.

Use

How will a PIA be used in practice? A requirement that an agency conduct a PIA may accomplish little unless policy makers and system managers are obliged to read, consider, and react to the assessment. Unless a PIA actually has a reasonable chance to influence policy, design, or implementation, the PIA become a report that sits on a shelf without much purpose. In a recent book on privacy impact assessment, multiple authors expressed concern that PIA requirements might produce a "box-ticking" mentality on the part of bureaucrats seeking to meet a legal requirement and without any interest in fulfilling the PIA's

fundamental objective of truly informing decision makers.[90] Ways to make PIAs relevant to real world decisions include making as much of the process as public as possible, requiring formal responses by system planners to PIAs, maintaining some degree of external oversight of those responses, and establishing an ongoing mechanism, such as a chief privacy officer, to oversee privacy matters.

Conclusion

The challenge of addressing privacy in biometric identification systems is not simple or static. Yet the challenge is not impossible, nor is it appreciably harder than or different from other identification systems or other PII-intensive activities.

The paper offered definitional approaches to privacy, discussed selected privacy topics and concerns, and broadly considered the principles of fair information practices, privacy by design, and privacy impact assessments to illustrate how familiar approaches to privacy might be relevant to biometric identification systems.

Among most countries, there is a rough consensus about the value of information privacy and about the need for processes for evaluating the adequacy of information privacy standards and policies in most contexts. While privacy or even information privacy does not have a clear, fixed, or universal definition, much of the world has established meaningful information privacy standards and policies, albeit with significant variations and important ongoing debates about many aspects of privacy and privacy regulation. Addressing privacy in biometric identification systems means starting from existing standards and familiar processes. Policy makers can draw on those standards and processes to weigh and balance privacy against competing goals. This is not intended to suggest that solutions suitable to countries with robust forms of identification will necessarily work in countries that lack an identification infrastructure.[91] The terms of debate (but not necessarily the best outcomes) are broadly known

For biometric identification systems in countries that do not have well-established privacy traditions, laws, or institutions, the challenges are greater. It can be difficult to develop a process that factors in privacy concerns at the appropriate time in the political, policy, and implementation processes for a complex biometric identification system that calls for government agencies and many others to adopt advanced technology. The demands on the

---

[90] See, e.g., David Parker, (Regulatory) Impact Assessment and Better Regulation at 96 in Wright & De Hert.

[91] For example, a 2003 study on personal identification and authentication for the United States by the National Research Council of the National Academies found great value in systems that facilitate the maintenance and assertion of separate identifies in separate contexts. That conclusion was based on the existing robust and multiple identification systems already in use in the United States. In another jurisdiction where identification methods are scarce or non-existent, the same conclusion may not have any applicability. National Research Council, Who Goes There?: Authentication Through the Lens of Privacy 78 (2003) (recommendation 3.1), http://www.nap.edu/catalog.php?record_id=10656.

public, who will be the data subjects of the system, will also be new. However, a robust and timely privacy impact assessment for a biometric identification system can evaluate the issues, suggest alternatives, and present choices for decision makers who will be better informed of the consequences of those choices.

This paper offers a high-level perspective of information privacy as it has developed over the last fifty years or so when privacy has become a widely recognized concern. One of the good things about the vagueness and uncertainties of the privacy standards and processes used today is that they allow for considerable variability in application. FIPs can apply in many ways to any given information system. A PIA can be done in various ways, at various times, and by various players. PbD is adaptable to any PII-intensive activity.

The variability allows much room for others to borrow from work already done and to adapt policies and processes to their own governmental and political traditions, to their own administrative structures, and to their own ways of finding consensus when policy conflicts arise, as they do routinely in many types of endeavor. This paper set out some of the lessons to be learned from privacy debates with the hope that those lessons will help countries, as well as donors who may be assisting them, make choices about how to address information privacy concerns in biometric identification systems.