2017

Transparency

Leslie P. Francis
S.J. Quinney College of Law, University of Utah, leslie.francis@law.utah.edu

CHAPTER 8: Transparency

By Leslie Francis, PhD, JD

Transparency is one of the key concepts of privacy protection. Transparency means openness about data collection, use, and retention. Individuals need to know what information about them is being collected, how it is being collected, how it is to be used and shared, how it is protected, what has been learned from data use, how what has been learned might benefit them, and how they can seek correction or redress for security breaches or other unjustified uses or disclosures of data. This chapter begins with a highly salient recent example of transparency in action: the principled commitment to transparency in the precision medicine initiative (PMI) and the limited extent to which it has been developed in the initiative to date. The chapter then provides an overview of justifications for transparency and challenges inherent in providing consumers with understanding that is meaningful to them. The chapter then considers methods for achieving transparency through publication or notice and what is known about the success or failure of these methods. For example, privacy notices have grown bloated and legalistic; patients rarely read them and if they do, they do not understand them. The chapter concludes with a discussion of emerging solutions.

The Principle Of Transparency In The Precision Medicine Initiative

The precision medicine initiative is a highly ambitious effort to create a cohort of over a million volunteers who agree to contribute their health data over many years to further investigation of the molecular, environmental, and behavioral aspects of disease. Led by the National Institutes of Health (NIH), it aims to develop an understanding of important variations among patients that will enable targeting therapeutic or other interventions to

maximize success in treatment and prevention of disease. It also aims to create new models for patient engagement not only in care but also in research. And the plan is to try to maximize diversity within the cohort so that individuals of different types are not left behind in the advantages that the PMI may bring. The information collected about cohort participants will be vast and various: blood and possible other tissue samples, information from electronic health records (EHRs), a baseline physical exam, insurance claims, mobile health devices, participant surveys, and other sources. And cohort participants will be expected to agree to be re-contacted over time to participate in a variety of more specific research studies.[1]

As thus envisioned, the PMI presents difficult questions of transparency. Participants in the cohort will vary in location, age, language and culture, race, socioeconomic status, and many other factors. As individuals are enrolled in the cohort, there will be an overall promise of what it may achieve but no precise information about how the data will be used, how frequently individuals will be re-contacted, what studies will be of interest, how long the data will be valuable, whether other data will be needed and combined with the types of data sought initially, and what will ultimately be learned. Any consent at enrollment therefore must perforce be highly general, based on whatever parameters can reasonably be anticipated. But these parameters may change as more is learned. Transparency thus will involve not only information at a single time slice, but information over time as the uses of the cohort change and results emerge.

The initial White House announcement of privacy and trust principles for the PMI included transparency as a guiding principle necessary to building trust among participants in the

[1] Precision Medicine Initiative Working Group. 2015. The Precision Medicine Initiative Cohort Program – Building a Research Foundation for 21st Century Medicine (Sept. 17) https://www.nih.gov/sites/default/files/research-training/initiatives/pmi/pmi-working-group-report-20150917-2.pdf, Executive Summary, pp. 1-5.

program and more generally in society as well. The principle of transparency was fleshed out into five areas, as follows:

Transparency

1. A dynamic information-sharing process should be developed to ensure all PMI participants remain adequately informed through all stages of participation. Communications should be culturally appropriate and use languages reflective of the diversity of the participants.

2. Information should be communicated to participants clearly and conspicuously concerning: how, when, and what information and specimens will be collected and stored; generally how their data will be used, accessed, and shared; types of studies for which the individual's data may be used; the goals, potential benefits, and risks of participation, including risks of inappropriate use or compromise of the information about participants; the privacy and security measures that are in place to protect participant data, including notification plans in the event of a breach; and the participant's ability to withdraw from the cohort at any time, with the understanding that consent for research use of data included in aggregate data sets or used in past studies and studies already begun cannot be withdrawn.

3. Information should be made publicly available concerning PMI data protections and use, and compliance with governance rules.

4. Participants should be notified promptly following discovery of a breach of their personal information. Notification should include, to the extent possible, a description of the types of information involved in the breach; steps individuals should take to protect themselves from potential harm, if any; and steps being taken to investigate the breach, mitigate losses, and protect against

further breaches.

5. All users of PMI data should be expected to publish or publicly post a summary of their research findings, regardless of the outcomes, as a condition of data use. To enrich the public data resource, mechanisms for data users to integrate their research findings back into PMI should be developed.[2]

These are impressive transparency goals. Putting them into practice will not be easy. The NIH working group report on building the PMI cohort, for example, references transparency only three times, and one of these is to mention the White House announcement. The other two references emphasize the return of their own data to participants; what this means is not further explained, but perhaps the goal is to highlight the patient engagement aspects of the PMI. The references do not as yet elaborate other aspects of transparency, such as how to communicate what is being done with information collected for the PMI or what investigators will be expected to do in sharing research results with participants and the public more generally. In the first reference to transparency, in th final sentence of the Executive Summary, the working group states that "Transparency regarding data access and use will be emphasized, with return of information to participants, including aggregate data and return of participant's personal data as desired."[3] And in second reference, in the discussion of data access, use, and analysis, the working group notes, "In the spirit of transparency and collaboration, individuals and organizations that provide data to the PMI cohort should, as a general policy, have unrestricted rights of access to their own submitted data. Individual

[2]White House. 2015. Precision Medicine Initiative: Privacy and Trust Principles (Nov. 9). https://www.whitehouse.gov/sites/default/files/microsites/finalpmiprivacyandtrustprinciples.pdf, pp. 2-3.

[3]Precision Medicine Initiative Working Group. 2015. The Precision Medicine Initiative Cohort Program – Building a Research Foundation for 21st Century Medicine (Sept. 17) https://www.nih.gov/sites/default/files/research-training/initiatives/pmi/pmi-working-group-report-20150917-2.pdf, p. 79.

participants will have varying levels of health and science literacy, and will need assistance with interpretation of their data."[4]

These references are the only elaborations of transparency by the NIH working group. Clearly, much more will need to be said about transparency as the PMI is developed. More needs to be said about transparency for other emerging uses of information as well.

Transparency: Its Meaning, Justifications, And Means

Transparency has long been a cornerstone value in the management of information about individuals. What are called Fair Information Practices (FIPs) were first proposed in a 1973 report[5] of the then-Department of Health, Education, and Welfare. The report, *Records, Computers, and the Rights of Citizens*,[6] stipulated that there should be no data collection systems whose existence was secret. Many subsequent formulations of FIPs have fleshed this out to include aspects of data collection: people should be able to know what data about them are being collected, who (or what) is collecting the data, how the data are being collected, and how the data are being stored, disclosed, managed, and used. Understanding what the quite abstract idea of transparency means in different data contexts is challenging, however, and turning briefly to justifications for transparency is useful in this regard.

---

[4] Precision Medicine Initiative Working Group. 2015. The Precision Medicine Initiative Cohort Program – Building a Research Foundation for 21st Century Medicine (Sept. 17) https://www.nih.gov/sites/default/files/research-training/initiatives/pmi/pmi-working-group-report-20150917-2.pdf, p. 20.

[5] For a very useful history of FIPs, see Gellman R. Fair Information Practices: A Basic History, version 2.16; June 17, 2016. Available at: http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

[6] Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers and the Rights of Citizens; July 1973. Available at: http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm.

Justifications for transparency may be rooted in the obligations of the entity collecting the data, the rights of individuals, or contracts between the data collector and the individual. Myriad types of entities today are involved in data collection activities: with respect to health data, these include international organizations, such as the World Health Organization, governments (i.e., public health agencies), healthcare organizations, Internet search providers, newspapers, data brokers, other commercial entities, and most recently in the US the PMI—to name just a few. These data collectors may have very different rights and obligations. Governments—at least, democratic governments—are generally thought to have ethical obligations to their citizens to be open about what they are doing and about what they are learning, unless there are overriding reasons for information protection.[7] These obligations may be especially strong if matters of public interest or public safety are involved, and may be overridden in exceptional cases, such as individual privacy, law enforcement or national security, or commercial secrecy. Freedom of information laws and their exceptions reflect these commitments.[8] Commercial entities that assemble and market databases may assert intellectual property rights through copyright[9] or trade secrets law to these assets, as appears to be happening increasingly in the wake of court decisions limiting patent rights of genetic testing companies.[10] However, these intellectual property rights may

[7] Pozen DE. Deep Secrecy. *Stanford Law Review.* 2010;62:275-339.
[8] The federal Freedom of Information Act is 5 U.S.C. § 552; 2016.
[9] Asserting a copyright requires an element of creativity; mere listings of information such as material gathered from patient records would not be copyrightable, absent more. *Feist Publications, Inc. v. Rural Telephone Services Co.,* 499 U.S. 340; 1991 (telephone white pages listings not copyrightable). There has been considerable controversy regarding when databases are copyrightable, e.g., Bitton M, A New Outlook on the Economic Dimension of the Database Protection Debate. *IDEA.* 2006; 47:93-169.
[10] Trade secrets law requires the entity asserting this intellectual property right to make reasonable efforts to keep the information from being disclosed. Uniform Trade Secrets Act (1985) § 1(4)(ii). This law thus works very differently from patent law, which requires disclosure of the invention as a condition for asserting exclusivity. Companies with large data bases of patient information may claim these as trade secrets to gain competitive advantage—

be limited or overridden by public interests, such as public health or safety.[11]

Although understood in multiple forms, the individual right to privacy has been legally recognized for more than 100 years.[12] This right has been interpreted as rights to control access to the person, as rights to protection against intrusion into secluded space, as rights to control information, and as rights to make decisions about important or intimate matters, among other conceptualizations. The right to privacy also has been distinguished from the right to confidentiality: the right to control access to and disclosure of information about oneself.[13] Data collection, use, or disclosure may implicate both privacy and confidentiality as thus understood.

Many values have been asserted in support of these multiple understandings of privacy and confidentiality rights. These values include autonomy and choice, political liberty, physical security, intimacy, dignity, identity, equality, and justice. Some of these values relate directly to the individual, such as the ability to make choices about one's life. Understanding what information is being collected can help individuals make choices about what information to share, whom to trust with that information, and whether to rely upon their expectations about what will happen to their information. Knowing what information has been collected, who has done the collecting, and whether the information has been disclosed to others can also

---

for example, a genetic testing company may have information about the significance of variants that is not generally available. See e.g. Cook-Deegan R, Conley JM, Evans JP, Vorhaus D. The next controversy in genetic testing: clinical data as trade secrets? *Eur J Hum Genet.* 2013; 21(6):585-8.

[11] Lyndon ML. Secrecy and Access in an Innovation Intensive Economy: Reordering Information Privileges in Environmental, Health, and Safety Law. *University of Colorado Law Review.* 2007; 78:465-531.

[12] Warren S, Brandeis LD. The Right to Privacy. *Harvard Law Review.* 1890; 4(5):193-220; Prosser WL. Privacy. *California Law Review.* 1960; 48(3):383-423.

[13] Francis LP, Privacy and Confidentiality: the Importance of Context. *Monist.* 2008; 91(1):52-67.

help individuals to be aware of, and thus hopefully protect themselves against information disclosures, such as those that might occur through a security breach. Some of these values may also be asserted on the level of a group: information about group members or about the group itself may lead to the group being targeted for attack (even genocide), may alter conceptions of group identity, may stigmatize, or may result in discrimination against members of the group.

Transparency may also be useful for the data collector. People may be more willing to share information—thus contributing to more robust data collection possibilities if they believe they can trust data collectors.[14] Notorious examples highlight how mistrust about data collection and use can harm data collection abilities. In Texas[15] and in Minnesota,[16] failures to inform the public about retention and subsequent uses of blood spots obtained in newborn screening programs resulted in public outcry and the eventual destruction of valuable public health resources and the data they contained. Arizona State University settled with the Havasupai tribe after researchers had used genetic data obtained in a study of diabetes and then de-identified it for research studies of mental illness and migration patterns.[17] Multiple studies sound the theme that consumer concerns about the privacy of their health information may generate reluctance to use patient portals, HIEs, or PHR systems.[18] Although searching

[14] Froomkin AM. A New Legal Paradigm? The Death of Privacy? *Stanford Law Review.* 2000; 52:1461 1543.
[15] Texas Department of State Health Services, Statement: Newborn Screening Settlement; December 22, 2009. Available at: www.dshs.state.tx.us/news/releases/20091222.shtm.
[16] Minnesota Department of Health. Minnesota Department of Health to begin destroying newborn blood spots in order to comply with recent Minnesota Supreme Court ruling; January 31, 2012. Available at: www.health.state.mn.us/news/pressrel/2012/newborn013112.html.
[17] Harmon A. Indian tribe wins fight to limit research of its DNA. *The New York Times.* April 21, 2010. Available at: www.nytimes.com/2010/04/22/us/22dna.html?pagewanted=all.
[18] For example: California HealthCare Foundation. *Achieving the Right Balance: Privacy and Security Policies to Support Electronic Health Information Exchange;* March 2012. Available at: http://www.chcf.org/publications/2012/06/achieving-right-balance.

for health information is a common Internet activity,[19] recent data also indicates that willingness to share information depends on perceived tradeoffs between risks and what is to be gained.[20]

Most generally, transparency refers to openness about what is being done. In contemporary statements of FIPs, this general idea of transparency has taken two importantly different forms: general publication and direct-to-consumer notice. As an example of the former, the U.S. Privacy Act requires that federal agencies publish notice in the *Federal Register* of the existence and character of the systems of records they maintain.[21] Another example of general publication would be the suggestion of the FTC to data brokers—entities that collect and aggregate data for resale—to develop a website register of data collection activities for marketing purposes to allow consumers to understand what they are doing, know their access and choice rights, and opt out of uses of information about them.[22]

A second type of effort to ensure transparency is giving direct notice to the consumer. This has taken many different forms. Early in their development, FIPs were interpreted to require direct notice to individuals about specific disclosures. For example, the U.S. Privacy Act requires that federal agencies make reasonable efforts to provide notice of disclosures made

---

[19] The latest available data from the Pew Internet Project indicates that 87% of US adults used the internet in 2012, and that 72% of these internet users had searched for health information during that year. Pew Research Center. Health Fact Sheet; Dec. 16, 2013. Available at: http://www.pewinternet.org/fact-sheets/health-fact-sheet/.

[20] Rainie L Duggan M. Privacy and Information Sharing; January 14, 2016. Available at: http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/.

[21] 5 U.S.C. § 552a(e)(4);2016.

[22] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers; March 2012; page 69. Available at: www.ftc.gov/os/2012/03/120326privacyreport.pdf. Although this suggestion was made in 2012, it does not appear to have been acted on as of 2016.

under compulsory legal process when the disclosure will become a matter of public record.[23] Notification of security breaches of PHI is required by the HITECH Act amendments[24] to HIPAA for covered entities and their business associates, and for vendors of PHRs.[25] Following California's lead in 2002, most states have also enacted breach notification statutes, although the majority of these do not include health information.[26]

The idea of a notice of privacy practices—either published on a website for readers to use or given in paper form to individuals—is a more recent development. As early as 1995, the European Union's Directive 95/46 on the protection of individuals with regard to the processing of personal data required member states to enact notice standards.[27] Under EU law, directives give member states flexibility in meeting minimum standards while regulations set out requirements for all to meet. In 2016, Directive 95/46 was replaced by the General Data Protection Regulation which incorporates and strengthens the requirements of the Directive.[28] Any collection of personal data requires notice, including the identity and contact details of the data controller and data protection officer, the purposes of the data collection, the legal basis for the collection, the recipients or categories of recipients of the

---

[23] 5 U.S.C. § 552a(e)(8);2016.
[24] HITECH Act §§ 13402, 13407.
[25] HITECH Act § 13407.
[26] Cal. Civ. Code §§ 1798.82, 1798.29(2016); National Conference of State Legislatures, Security Breach Notification Laws; January 24, 2016. http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
[27] Directive 95/46/EC of the European Parliament and of the Council, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Art. 10; *Official Journal of the European Communities.* no.281/31 (23.11.95). Available at: http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.
[28] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); *Official Journal of the European Union* L119/1 (4.5.2016). Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en.

data, and any intent of the data controller to transfer data outside of the EU.[29] Similar information must be provided where personal data have not been obtained from the data subject.[30] All of this information must be provided "in a concise, transparent, intelligible and easily accessible form, using clear and plain language…"[31] Further information "necessary to ensure fair and transparent processing is also required, including the length of data storage, the right to request rectification or erasure of the data, whether the data will be used in profiling and any envisioned consequences of this, and whether the data subject is required to provide the data along with the consequences of refusal."[32]

One major innovation of the Regulation is incorporation of the so-called "right to be forgotten," a right to have data erased under specified circumstances, including that there are no longer overriding legitimate grounds for maintaining the data.[33] A major motivation for the overhaul of EU data protection was the judgment that enforcement of standards for data transfer outside of the EU had become too lenient, especially for transfers to the US. In July, 2016, the EU and the US finalized a Privacy Shield Framework so that data can be transferred back and forth between the two; the framework contains significantly stronger requirements and enforcement guarantees than the prior Safe Harbor arrangement.[34] Among the new requirements for Privacy Shield participants are compliance with EU notice and choice requirements and transparency regarding any enforcement actions against the participant.[35] The Privacy Shield Framework will likely result in increased transparency and

---

[29] Regulation (EU) 2016/679, Art. 13.
[30] Regulation (EU) 2016/679, Art. 14.
[31] Regulation (EU) 2016/679, Art. 12(1).
[32] Regulation (EU) 2016/679, Art. 13(2), Art. 14(2).
[33] Regulation (EU) 2016/679, Art. 17.
[34] U.S. Department of Commerce, EU-U.S. Privacy Shield Program Overview; July 2016. Available at: https://www.privacyshield.gov/Program-Overview .
[35] U.S. Department of Commerce, EU-U.S. Privacy Shield Framework Key New Requirements of Participating Companies. Available at: https://www.privacyshield.gov/Key-

stiffer notice requirements for companies seeking to transfer data from the EU.

Other federal and state laws also require privacy notices. Federally, the Financial Services Modernization Act of 1999 (otherwise known as Gramm-Leach-Bliley) requires financial institutions and insurance companies to send their customers conspicuous yearly notices explaining their policies with respect to information protection and disclosure.[36] Without the notice and information about how to opt out, these institutions may not disclose identifiable personal information to unrelated entities.[37] California state law requires a privacy notice to be included in a conspicuous manner on any commercial website collecting personally identifiable information about consumers.[38]

With respect to health information specifically, the HIPAA Privacy Rule requires covered entities to provide patients with an NPP. The HIPAA NPP must include prescribed language, in all capital letters, calling the reader's attention to what the notice concerns. Prescribed information includes a description of the types of uses and disclosures that are permitted without individual authorization, a statement that other uses and disclosures may occur with authorization, and separate statements about certain uses and disclosures, such as for fundraising. The NPP must also tell the individual about their rights of access to health information, rights to an accounting of uses and disclosures, and rights to request amendments.[39] The notice also requires contact information and information about how to file complaints. It is fair to say that the HIPAA regulation is prescriptive and complex, and

---

New-Requirements .
[36] 15 U.S.C. § 6803; 2016.
[37] 15 U.S.C. § 6802; 2016.
[38] Cal. Bus. & Prof. Code §22577; 2016.
[39] 45 CFR §164.520; 2016.

encourages lengthy and formalistic notices.

Over the past decade or more, privacy notices and statements of privacy policies have become a standard practice across the Internet. Many of these notices also feature a notice/choice format in which consumers are invited to make particular choices. Consumers may be asked to click "I agree," thus potentially becoming contractually bound to the contents of the notice. Or, they might be told that their data will be used in specified ways unless they opt out, and are offered a method for exercising this choice. For particularly controversial types of data use, such as marketing, consumers may be told that they must opt in to have their data used in this way and offered a "yes" button or some other mechanism of acceptance.

Understanding what these privacy notices should be like, what they should say, and what they can be expected to achieve has evolved as well. This chapter returns to these developments after reviewing widely understood challenges to successful transparency.

Transparency: Barriers To Achieving Successful Communication

Understood passively, transparency is not difficult to attain. Information about data collection activities can be published and individuals can be handed or mailed notices about these practices. If transparency is understood in terms of its justifications however, passive publication is not enough. Openness on the part of government requires more than lists buried in the *Federal Register* or some other publicly-accessible document; it requires education of and interaction with the public so that at least a reasonable proportion has sufficient understanding to exercise any rights they might have and to participate in the political process

with respect to information-gathering by their governments. A notice/choice model with respect to information uses and disclosures does not succeed in respecting individual autonomy unless individuals have sufficient understanding and opportunities to make meaningful choices. Thus understood, transparency requires at least some success in communicating. It is an ongoing process and its achievement is a matter of degree. But there are significant barriers to achieving transparency in this sense. The issues themselves are complex and answers are not easy.

First, individuals are not ideal recipients of communication, to say the least. In the background are variations in literacy, access to media, Internet familiarity, time and energy, cognitive biases, and cultural practices and attitudes. Commentators lament a "digital divide"[40] between those who have ready and skilled access to the Internet and those who do not, largely the poor, racial minorities, and rural populations, especially in the Southeast.[41] The advent of widespread smartphone use may be mitigating this divide, but in a manner that brings additional challenges associated with smartphone privacy, such as lack of password protection, lack of data encryption, or ease of loss. Demographically, at least in general, the elderly may have less familiarity with and understanding of technology and the Internet. Many internet users are now very concerned about privacy but do not know a great deal about mechanisms they might use to protect it.[42] Also according to this study, people who are new to the internet are more likely to need help to figure out how to use features of websites that

[40] Council of Economic Advisers Issue Brief. *Mapping the Digital Divide*; July 2015. Available at: https://www.whitehouse.gov/sites/default/files/wh_digital_divide_issue_brief.pdf.
[41] Lee Rainie. *Digital Divide 2016*; July 14, 2016, slide 30. Available at: http://www.pewinternet.org/2016/07/14/digital-divides-2016/.
[42] Lee Rainie. *Digital Divides 2016*; July 14, 2016, slide 41. Available at: http://www.pewinternet.org/2016/07/14/digital-divides-2016/.

enable them to protect information.[43]

With respect to privacy, social scientists have identified a so-called "privacy paradox."[44] Although individuals say that they value privacy, they do not act as though they do. Failure to search or to read privacy notices may exemplify this paradox.[45] Some economists and social commentators draw the conclusion that actions speak more loudly than words, and individuals' failures to protect their privacy may simply reveal that they do not value it very much and that privacy protection is therefore inefficient.[46] In a much-quoted remark, Scott McNealy, then-CEO of Sun Microsystems, opined: "You have zero privacy anyway. Get over it!"[47] On the other hand, there may be significant variations in the extent to which people value privacy, to some extent correlated with age cohort. People also may value privacy less if they believe that they will get important benefits from sharing their information—through social networking sites, such as Facebook, or through network sites that share information about health conditions, such as PatientsLikeMe. Additionally, individuals may lack understanding of what privacy policies and law actually provide to them. One study suggests that misconceptions are widespread, especially in younger age cohorts; many people believe that having a privacy policy is the same as protecting privacy (it is not; a policy must simply state what protections exist, if any) and that they have rights to sue for damages if their privacy is violated (in general, they do not).[48] This confidence, based

---

[43] Lee Rainie. *Digital Divides 2016*; July 14, 2016, slide 40. Available at: http://www.pewinternet.org/2016/07/14/digital-divides-2016/.
[44] Nordberg PA, Horne DR, Horne DA. The privacy paradox: personal information disclosure intentions vs. behaviors. *Journal of Consumer Affairs.* 2007; 41(1):100-126.
[45] Groom V, Calo MR. Reversing the Privacy Paradox: An Experimental Study. Available at: http://ssrn.com/abstract=1993125.
[46] Posner RA. The Right of Privacy. *Georgia Law Review.* 1978; 12(3):393-422.
[47] Sprenger P. Sun on Privacy: 'Get Over it! *Wired.* January 26, 1999. Available at: www.wired.com/politics/law/news/1999/01/17538.
[48] Hoofnagle C, King J, Li S, Turow J. How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes & Policies; April 14, 2010. Available at:

in misunderstanding, may explain why many people fail to read privacy notices. Other explanations include the length and difficulty of many privacy notices—as well as the fact that they may appear legalistic and boring.

Several studies have discerned cognitive biases as playing a major role in apparently paradoxical behavior about privacy, arguing that these biases can help explain what seems paradoxical. For example, increasing perceived control over publication of private information may increase willingness to disclose, even when the increase in perceived control is coupled with reduced protection of the information from access by others . This is a paradox of perceived control and risky behavior: the greater the perceived control, the greater the likelihood of risk-taking, with the perverse result of worse outcomes.[49] A further complexity is that differences in perceived relative risk—how much greater the risk of one alternative is in comparison to another—may be more influential on individual behavior in actual circumstances than differences in absolute risk.[50] (Adjerid, Peer and Acquisti 2016). Thus a change in a privacy notice about a decreased level of protection may be more impactful on individual privacy behavior than lack of notice in the first place. Another illustration of this irrationality is the status quo bias and default settings: consumers are much less likely to change default privacy settings, even when they do not reflect their actual preferences. Policy makers are beginning to consider how to take these factors into account in designs of websites and their privacy policies, as a conference series at the US Federal Trade Commission called PrivacyCon illustrates.[51]

---

http://ssrn.com/abstract=1589864.

[49] Brandimarte L, Acquisti A, Loewenstein G. Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological & Personality Science* 4(3); 2013: 340-347.

[50] Adjerid I, Peer E, Acquisti A. Beyond the Privacy Paradox: Objective versus Relative Risk in Privacy Decision Making; 2016. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2765097.

[51] Federal Trade Commission. PrivacyCon. Available at: https://www.ftc.gov/news-

Second, data collectors—whether public or private—may have legitimate reasons for caution about transparency requirements. Data collectors may be concerned that if they reveal the information that they have or what they are doing with it, they may be less able to protect it. They may find themselves overwhelmed with requests for the data—or worse, subject to criminally-motivated attacks now that they have been identified as a likely target. They may be concerned that knowledge of their activities will lead to public objections or protest, or may generate litigation. Revealing the kinds of information they possess to competitors may diminish competitive advantages resulting from careful (and expensive) investments in data. Finally, transparency—at least of the sort designed to generate real understanding—takes time and may be expensive. For example, healthcare providers who work under significant time pressures may believe that the time they might spend on explaining a privacy notice could be far better spent on explaining patients' conditions or treatment alternatives.

On the other hand, both individuals and data collectors may act in ways that cannot be justified with respect to transparency. Individuals may be careless, lazy, or inattentive; they may not behave as responsible, rational consumers. Data collectors, too, may have problematic reasons for transparency reluctance. They may believe that consumers will be unwilling to share data if they become better informed about what will happen to it. They may wish to use data in ways that many people find objectionable—for example, for marketing. They may wish to use data in ways that violate individuals' moral—or even legal—rights (for example, to dismiss an employee in violation of anti-discrimination laws).

Efforts to achieve transparency must contend with both legitimate barriers and unjustifiable

reasons for failure. The next section considers notice and choice as an instructive model for efforts to achieve transparency.

Notice As A Method For Achieving Transparency

As explained above, the idea of a privacy notice came into being relatively recently as a means for informing consumers about data collection activities. Privacy statements have become standard fare in the bottom margins of websites, waiting to be clicked on by interested consumers. These notices are frequently long, written in language that may appear reassuring, but actually convey little information to the average consumer, and designed to protect companies from liability.

The notice/choice model is rooted in a specific vision of autonomy. The idea is that if individuals are told what will happen to the data (given notice), they will then be able to make choices about what data they are willing to share, with whom, and for what purposes. In its most passive form, notice/choice simply tells a consumer that particular activities—use of a website, for example—constitutes consent to the privacy practices. If people do not read notices, however, it is questionable whether their activities constitute genuine consent. Somewhat more active notice/choice models require individuals to signify agreement (an "I agree" or "I accept" hot button), possibly after actually opening a privacy notice. Although these models leave evidence of a statement of agreement and have been used in court to limit companies' contractual obligations to customers,[52] they do little to ensure that individuals actually read the notices or are informed about the content to which they are agreeing. Even so, they do remain available for consumers to examine at a later time. These notices also

[52] *Hill v. Gateway 2000*, 105 F.3d 1147 (7th Cir. 1997), cert den. 118 S.Ct. 47; 1997.

provide a statement of privacy practices that put a data collector on record about policies and establish rules for their employees.[53] Failure to adhere to a stated privacy policy is an unfair trade practice in that it may mislead the consumer and may subject the entity to an enforcement action by the FTC. Additional defenses of these limited notice/choice models could contend that individuals' failure to read notices signifies that privacy is not very salient to them or that individuals are responsible for what they allow to happen with information about them.

More granular notice/choice models permit or require individuals to agree to particular data practices. A privacy notice might offer individuals a menu of data uses, inviting them to opt out if they so wish. Such opt-out approaches leave data use or disclosure as the default, and there is evidence that many individuals leave default settings in place even if they do not reflect their preferences in fine-grained fashion.[54] Some notice/choice models, especially for sensitive data or controversial uses, require specific opt-in. Here, the default setting is that information will not be used or disclosed, and evidence suggests that some individuals do not opt in even when they would prefer the data practice in question. In the attempt to avoid such problems with default settings, another notice/choice model asks "yes/no" questions for particular types of uses or disclosures. These structures are more cumbersome, but it is arguable that they provide a better reflection of actual consumer preferences.

---

[53] Statement of Robert Gellman, HIT Policy Committee, September 18, 2009. Available at: http://bobgellman.com/rg-docs/rg-HITPolicy-9-18-09.pdf.

[54] Madden M, Lenhart A, Cortesi S, Gasser U, Duggan M, Smith A, Beaton M. *Teens, Social Media, and Privacy Part 2: Information Sharing, Friending, and Privacy Settings on Social Media*; May 21, 2013. Available at: http://www.pewinternet.org/2013/05/21/part-2-information-sharing-friending-and-privacy-settings-on-social-media/. *See also* Thaler RH, Sunstein CR. *Nudge: Improving Decisions About Health, Wealth, and Happiness*. New Haven: Yale University Press, 2008; Trout JD. Paternalism and Cognitive Bias. *Law and Philosophy*. 2005; 24:393-434.

Designing notices to reflect actual choice raises a number of issues in addition to granularity. Explaining complex matters at a reading level most people can understand is one challenge. Another question is whether there should be a standardized format used by all notices to facilitate consumer comparison. Another is timing: whether the consumer should be presented actively with the notice at the particular point at which data are being used or disclosed, or whether it is sufficient to provide consumers with a notice only at the time of original collection.

Recognizing difficulties with respect to communicating through notices, the FTC has proposed "flexible" notice requirements.[55] In general, the FTC urges, privacy notices should be shorter, more clearly written, and more standardized to facilitate consumer understanding. Any notice and choice requirements should be tailored to the purpose and sensitivity of the transaction at hand. For some activities—for example, ordering commonly-used consumer products over the Internet—notice may be very simple. If practices are consistent with the context of the transaction or the relationship between the company and the consumer, or if data collection is required by law, the FTC's judgment is that this simple notice and no further consumer choice is all that is required. For other transactions—for example, entering health information into a website designed for individuals with serious medical conditions—direct notice and choice at the time of entry are required. The FTC Report opts for an objective "context of the interaction" standard for consumer choice, in contrast to either a subjective standard of consumer expectations or a list of "commonly accepted" practices not requiring choice, in order to allow for innovation and the development of new business models. "First-party marketing"—such as follow-up service notifications from a dealership

[55] FTC. Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers; March, 2012. Available at: www.ftc.gov/os/2012/03/120326privacyreport.pdf.

from which the customer has purchased an automobile—would not require consumer choice but tracking across other websites would do so. "Data enhancement" activities—adding third-party data to data collected from the consumer—would also not require choice.

In reaching these conclusions about flexible notice requirements, the FTC assumes a background of what it calls "privacy by design." This means that appropriate levels of privacy protection are built into all data collection activities. For example, third parties that are the sources of data sets used for enrichment are assumed to have built appropriate privacy practices into their collection as well, so that all the data used for enrichment has been subject to whatever notice and consent is appropriate for that data and use. To the end of achieving privacy by design, the White House discussion draft of a consumer privacy bill of rights included industry-specific codes. Compliance with these codes, the discussion draft suggested, could serve as a safe harbor from FTC enforcement actions.[56] Whether such self-regulatory efforts are likely to achieve progress in transparency remains to be seen.[57]

Case Study: Onc's Model PHR Privacy Notice And Beyond

Personal health records (PHRs), in many ways eclipsed today, are one vehicle for data collection in which the use of privacy notices has been explored extensively. PHRs allow individuals to create, develop, and control information about their health. At one point, they were thought to be an excellent way to involve consumers in their health care, although they appear to have been largely supplanted by other methods such as internet apps or wearable

[56] White House. Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015 Title III. Available at: https://www.insideprivacy.com/wp-content/uploads/sites/6/2015/02/cpbr-act-of-2015-discussion-draft.pdf.
[57] Bracy J. Will Industry Self-Regulation Be Privacy's Way Forward? *The Privacy Advisor* [online]; June 24, 2014. Available at: https://iapp.org/news/a/will-industry-self-regulation-be-privacys-way-forward/.

devices. Evaluations suggested that PHRs were simply too complex for many intended users.[58] Many of the PHRs remaining in use are linked to EHRs maintained by healthcare providers; these PHRs are typically structured so that the information in them is protected by HIPAA and subject to HIPAA notice requirements. Some PHRs, however, are freestanding and may contain health information that has been uploaded by the patient or downloaded from HIPAA-protected entities, but the information in them is not subject to HIPAA because these freestanding PHRs are not HIPAA-covered entities. The vast explosion of internet apps and wearable devices for collecting health information also has taken place largely outside of the realm of HIPAA protection, except for those devices that are directly linked to patients' medical records. The development of PHRs and later methods of health data collection thus provide an instructive case study for analyzing issues raised by reliance on notices as a method for achieving transparency.

In 2008, ONC began a process of developing a model PHR notice for PHR vendors to use, a process culminating in September 2011 with release of a voluntary model notice. The project's goals were to increase consumer awareness and provide consumers with an easy method for comparing the practices of different PHR vendors.[59] ONC's background statement judged that the model notice should help vendors be transparent about their privacy and security policies, generate trust in PHRs, and compete on the extent to which their policies protect consumers.[60] ONC's model notice was not designed to tell vendors what

---

[58] NORC. Evaluation of the Personal Health Record Pilot for Medicare Fee-For Service Enrollees from South Carolina. Available at: https://aspe.hhs.gov/sites/default/files/pdf/75991/report.pdf.

[59] ONC. Personal Health Record (PHR) Model Privacy Notice. Available at: http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov_draft_phr_model_notice/1176.

[60] ONC. About the PHR Model Privacy Notice: Background, Development Process, Key Points; September 2011. Available at: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_4108_1176_15440_43/http%3

choices they should offer consumers or whether to provide additional information to meet legal requirements applicable in their jurisdictions. Instead, with transparency as the goal, the model notice was developed based on consumer testing and research involving cognitive usability and provided a standard template for insertion of "yes/no" answers into pre-set fields.

The template was titled "What are [company name] PHR data practices?"[61] It covered two topics: data release and security. "Release" questions asked whether data would be released for marketing and advertising, medical and pharmaceutical research, reporting about the company and customer activity, insurers and employers, and developing software applications—in each case as either personally identifiable or statistical forms. For "security," the questions were whether data are stored in the United States only and whether activity logs are kept for customer review. The template also encouraged vendors to add a "hot button" at the end for individuals to click on to access the vendor's complete privacy and security policies.

An earlier edition of this chapter reported significant problems with PHR privacy notices ten months after ONC published its voluntary model privacy notice.[62] Notices were long and had an average reading level of 14.54, with a low of 12.44 and a high of 18.02, making it quite unlikely that the notices would be accessible by the many Americans without college degrees. By contrast, the National Cancer Institute recommends a eighth grade reading level for

---

B/wci-pubcontent/publish/onc/public_communities/p_t/privacy_and_security/model_phr_privacy_notice_home_portlet/files/phr_model_privacy_notice_backgrounder___final.pdf.

[61] http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_4108_1176_15440_43/http%3B/wcipubcontent/publish/onc/public_communities/p_t/privacy_and_security/model_phr_privacy_notice_home_portlet/files/phr_model_privacy_notice_final_2011.pdf.

[62] Cite to 1st edition.

informed consent forms used for patients in research studies.[63] Several notices included explicit statements that the policy limited their liability to the consumer; these policies could be characterized as company-protective rather than consumer-informative. Many policies indicated that they would disclose information in response to requests by law enforcement or government agencies such as Homeland Security and only one indicated that the site would attempt to notify the consumer before disclosing the information. Because these disclosures might adversely affect consumers' legal rights, privacy advocates have been especially concerned that PHR vendors should at least inform consumers in order to give them an opportunity to object.[64] Many notices reserved the right to change privacy policies, in some cases without directly informing the consumer. A few indicated that consumers could delete information or terminate accounts, but others were silent about consumers' rights in this regard.

PHRs have been largely supplanted in the market by internet apps for tracking various health measures such as diet or weight, and by wearable technologies such as fitness trackers. Because these mechanisms are outside of HIPAA protections, concerns about privacy protection have been significant. In 2016, ONC embarked on an update of its model privacy notice aimed at these mechanisms.[65] It solicited comments and received thirteen comments representing broad coalitions of stakeholders. A search of these comments revealed frequent

---

[63] National Cancer Institute. Simplification of Informed Consent Documents. Available at: www.cancer.gov/clinicaltrials/patientsafety/simplification-of-informed-consent-docs/page2.
[64] Center for Democracy and Technology. Building a Strong Privacy and Security Policy Framework for Personal Health Records; July 21, 2010. Available at: www.cdt.org/files/pdfs/Building_Strong_Privacy_Security_Policy_Framework_PHRs.pdf; The World Privacy Forum. Personal Health Records: Why Many PRHs Threaten Privacy; February 20, 2008. Available at: www.worldprivacyforum.org/pdf/WPF_PHR_02_20_2008fs.pdf.
[65] ONC. Personal Health Record (PHR) Model Privacy Notice Project Updates. Available at: https://www.healthit.gov/policy-researchers-implementers/personal-health-record-phr-model-privacy-notice#comments.

statements about the importance of transparency and a few suggestions of how that might be achieved. The following table summarizes these results:

[Table 4.1 goes here]

These results indicate a commitment to transparency but less discussion of what transparency actually means or how it can be achieved. Perhaps the explanation is that the comments were submitted in response to ONC's request to answer other specific questions regarding updating model privacy notices for PHRs. Nonetheless, only two—CDT and patientprivacyrights—refer to difficulties in achieving communication of data uses in real time to consumers. Many do indicate the importance of sharing types of uses with consumers, including the company's own planned uses and uses of de-identified information. All approve of ONC's plan to extend the voluntary model privacy notice to entities beyond PHR vendors; the AMA is perhaps the most forceful in stating that these entities should be moved towards the standards applicable to physicians because of the sensitivity of the health information they possess. Other commentators such as the Consumer Technology Association would give app developers a great deal of flexibility in how they communicate with consumers about what will be done with information. Achieving transparency for consumers over the life cycle of information use remains a challenge; this is a challenge that will surely need to be addressed as the PMI and other novel uses of large data sets evolve.

BEYOND POSTED NOTICES: PRESCRIBED PRODUCT LABELS AND OTHER TECHNIQUES FOR INFORMING CONSUMERS

This section considers several additional methods for attempting to achieve transparency. Product labels have become a common method of conveying information to consumers. They have the advantage of appearing every time the consumer purchases a product and, if they are

noticeably affixed to the product, every time it is used. Nutritional labeling is one example. Statutory authority regarding nutrition labels is drawn from the Nutrition Labeling and Education Act of 1990,[78] thus enabling the FDA to prescribe their form and content by regulation. Current labels list information about calories, fat content, vitamins, and minerals as a percentage of daily requirements. The amounts are listed per serving, with an indication of how many servings are in a package; consumers reading only the amounts may fail to recognize that a package contains several servings. The UK by contrast uses a "traffic light" system that indicates by red, yellow, or green whether a food is "high," "medium," or "low" in comparison to recommended daily allowances. The Patient Protection and Affordable Care Act (ACA) requires restaurants with more than 20 locations nationally to provide calorie labels for standard menu items.[79] Another familiar product label required by statute is the gasoline miles per gallon (mpg) disclosure for automobiles.[80] Further illustrations can be found in the many disclosure requirements that apply to lending, securities transactions, insurance, and other financial transactions. This use of disclosure as a substitute for regulation gained traction in the Reagan administration and has been a standard proposal of critics of government regulation ever since.[8155]

Some research has addressed the efficacy of nutrition labels and attempted to apply the model to privacy policies. A group at Carnegie Mellon found that although consumers would like more information in the labels, they might actually be confused by it.[82] The Carnegie Mellon

---

[78] 21 U.S.C. § 343(q); 2016.
[79] Patient Protection and Affordable Care Act § 4205(b).
[80] 16 CFR § 259.2; 2016.
[81] Dalley PJ. The Use and Misuse of Disclosure as a Regulatory System. *Florida State University Law Review.* 2007; 34:1089-1131.
[82] Kelley PG, Bresee J, Cranor LF, Reeder RW. A 'Nutrition Label' for Privacy. Symposium On Usable Privacy and Security (SOUPS), July 15-17, 2009; Mountain View, CA; Kelley PG, Cesca L, Bresee J, Cranor LF. Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach. CMUCy-Lab-09-014; January 12, 2010.

group's research also indicated that nutrition labels do have a small effect on consumer behavior, especially for consumers who are already interested in the information because they are trying to control their weight.

Other research has explored methods for conveying the information in notices. A group at the Stanford Center for Internet and Society has explored presentation techniques for encouraging consumers to read notices and to make notices more vivid for them.[83] An experimental study on notice in the context of privacy by these researchers attempted to understand whether different formats achieved greater success in influencing people's actual privacy behavior. The researchers hypothesized that "visceral" notice strategies—notice strategies with apparent non-cognitive appeal—would achieve superior success in influencing how much information people revealed deliberately or inadvertently.[84] The researchers constructed a website for a supposed new search engine and manipulated several different aspects of the website design: the formality of the website; whether the website revealed prior search history; whether the website featured interaction with a humanlike representation (such as an interface that includes an image of a human face); and whether the website revealed information about the user's current Internet location. The dependent variable of interest in this study was the extent to which participants revealed information about themselves when selecting questions for Internet searches. One conclusion was that informal website design increased the frequency of both direct and unwitting disclosure, probably because informality signaled to participants low levels of data collection by the website. Another conclusion was that participants were more likely to make unwitting disclosures under the notice conditions that prevail on websites today—a privacy policy containing

[83] Groom V, Calo MR. Reversing the Privacy Paradox: An Experimental Study.
[84] Groom V, Calo MR. Reversing the Privacy Paradox: An Experimental Study.

standard notice conditions available for clicking at the bottom of the site. The presence on the website of a humanlike representation reduced the likelihood of disclosures. The research also concluded that there was no difference between traditional notices and simplified versions of these notices in the rates at which participants followed links to privacy policies on the website; users simply did not click on the link to the policy at all.

More research on the efficacy of forms of notice and their presentation is clearly needed, however, as is research on other forms of disclosure.[85] As a former administrator of the Office of Information and Regulatory Affairs at the Office of Management and Budget, Cass Sunstein called for further empirical research to assess the efficacy of different kinds of disclosure requirements.[86] As an example, Sunstein cites the mpg regulation. As originally structured, the notice told consumers only the estimated mpg of the vehicle under different driving conditions. This structure encouraged consumers to believe that the relationship between mpg and gasoline savings is linear, when it is not. Thus consumers erroneously assumed that moving from a car burning 10 mpg to a car burning 15 mpg and moving from a car burning 25 mpg to a car burning 30 mpg produced equivalent savings. New labels now require additional information about gallons/100 miles driven and annual fuel costs that are intended to counter this consumer error, but Sunstein does not cite empirical evidence concerning the change.

An additional challenge is that these required statutory disclosures have major advantages over current model privacy notices. Their statutory foundation allows agencies to issue non-voluntary regulations, specifying what is to be said and how it is to be presented. They are

[85] Szanyi JM. Brain Food: Bringing Psychological Insights to Bear on Modern Nutrition Labeling Efforts. *Food and Drug Law Journal.* 2010; 65:159-184.
[86] Cass Sunstein, "Empirically Informed Regulation," *University of Chicago Law Review* 78: 1349-1429 (2011).

ubiquitous; consumers see them on the packages of any food, car, or menu and so become familiar with them over time. By comparison, use of PHRs never took widespread hold among consumers and there is no standardization and often little use of privacy notices among newer vehicles collecting health information. Consumers also see nutrition labels, menu labels, or mpg disclosures at times when they might be expected to be alert, non-threatened, and interested in reading them: comparing the prices of food on grocery store shelves, shopping for cars, or sitting in a restaurant waiting for a server to take their order. And they view readily understandable information about familiar products.

These familiar notices also have advantages over HIPAA privacy notices. Although consumers do see HIPAA privacy notices more frequently and so may be more familiar with them, to date HHS has not used its regulatory authority to prescribe a common notice form like the nutrition label. In addition, consumers are given privacy notices when they access healthcare. Unlike shopping or eating in a restaurant, accessing healthcare may be a time of stress for patients and their attention is likely to be elsewhere than the privacy notice. Moreover, information from these devices and many other sources may be used in a wide variety of ways, including the PMI.

Conclusion

As described in this chapter, transparency is a goal for collectors and users of data to achieve. Transparency as openness about practices cannot be equated with notice and choice models for concluding that consumers have consented to data collection or use. Instead, transparency must be understood as a process of education, information-communication, and, in appropriate circumstances, well informed consumer choice. This process must continue over

time and cannot simply be a one-off in a privacy notice that consumers may or may not pay attention to when they originally agree for their information to be collected. Transparency must also be set within a commitment to FIPs more generally. Ongoing study of consumer attitudes, communication barriers, and methods for effective information delivery remain imperative if individual choice is to be respected.

References