NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 17, ISSUE 4: MAY 2016

THROUGH A GLASS DARKLY: FROM PRIVACY NOTICES TO EFFECTIVE TRANSPARENCY[1]

Paula J. Bruening[*]
Mary J. Culnan[**]

Openness is the first fundamental principle of fair information practices with "notice" serving to practically implement openness in most commercial transactions. However, current notices have been widely criticized as being too complex, legalistic, lengthy, and opaque. This Article argues that to achieve the openness required by the first fair information practice principle, data protection and privacy should move from a "notice" model to an environment of "transparency." It asserts that the terms "notice" and "transparency" are not synonymous and that different definitions apply to each.

The Article begins by reviewing the history of notice in the United States and its traditional roles in privacy and data protection. It considers the challenges and limitations of notice, and the attempts to address them and the lessons learned from these efforts. The Article also examines the implications of emerging technologies and data uses such as mobile apps, big data analytics and the Internet of Things for traditional notice. This Article proposes that what is needed is a move from notice to an environment of transparency that includes improved notices, attention to contextual norms, integrating the design of notices into system development as part of privacy-by-design, public education, and new technological solutions. Finally, it presents arguments for business buy-in and regulatory guidance. While the historical

[1] The views expressed in the paper are those of the authors. An earlier version of this paper was presented at the 8th Annual Privacy Law Scholars Conference, Berkeley, California, June 2015. We acknowledge the helpful comments of Lorrie Cranor, Robert Gellman, David Hoffman, Anne Klinefelter, Mary Madden, Dawn Schrader and the PLSC attendees on the earlier version.

[*] Intel Corporation
[**] Bentley University and Future of Privacy Forum

review is limited to the experience in the U.S., the proposals for creating an environment of transparency can apply across jurisdictions. Further, while transparency is necessary but not sufficient for assuring fair data use, a discussion of issues related to the full complement of the fair information principles is beyond the scope of this paper.

I. INTRODUCTION

The first principle of fair information practices states that "[t]here shall be no personal-data record-keeping system whose very existence is secret and there shall be a policy of openness about an organization's personal-data record-keeping policies, practices, and systems."[2] This principle requires that organizations make their information practices visible to the public. Effective implementation of this principle is essential to promoting fairness. A lack of openness potentially enables organizations to collect and use information without protections and outside the scrutiny of regulators, consumers, or privacy advocates.

Since the late 1970s, what has commonly been referred to as "notice" has served to practically establish openness in most commercial transactions.[3] Notice has been relied upon to inform individuals' decisions about the collection, processing, sharing, and reuse of their personal information. In the United States, notice has also served as the basis for regulation by the Federal Trade Commission under Section 5 of the FTC Act,[4] which provides that companies whose practices are at odds with what is stated in their notices may be prosecuted for deception.[5] The European Data Protection Directive specifies the information about data collection, processing, and sharing that must be provided to individuals.[6] The

---

[2] In a 1973 report, a U.S. government advisory committee initially proposed and named Fair Information Practices as a set of principles for protecting the privacy of personal data in record-keeping systems. The Secretary's Advisory Committee on Automated Personal Data Systems issued the report. *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, U.S. DEPARTMENT OF HEALTH EDUCATION AND WELFARE, http://epic.org/privacy/hew1973report/default.html [hereinafter *Records, Computers and the Rights of Citizens*]. See p. 41 for a list of the original Fair Information Practices.

[3] *Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission*, ELECTRONIC PRIVACY INFORMATION CENTER (1977), https://epic.org/privacy/ppsc1977report/.

[4] 15 U.S.C. § 45 (2006).

[5] *Id. See generally* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION: PRIVACY LAW AND POLICY (Cambridge University Press 2016) (discussing privacy policy and the FTC).

[6] Council Directive 95/46, 1995 (EU).

Asia-Pacific Economic Cooperation Framework[7] states that data controllers should provide clear and easily accessible statements that articulate their practices and policies with respect to personal information.[8]

Notice arguably fosters openness by requiring companies to make public the business models, vendor relationships, and data practices that drive the digital economy. However, since the mid-1990s, both online and offline notices have been criticized by regulators, privacy advocates, and businesses as being too complex, legalistic, lengthy, and opaque. Questions about how notices could be improved figure prominently in nearly every discussion about privacy. Businesses complain of the challenge of writing notices that meet regulators' requirements for completeness, while consumer advocates call for clarity and concise, consumer-friendly language. Notices that support individual choice about subsequent use of personal information, often are written in language that allows companies such latitude that consent authorizes nearly any data use. As a result, notices are often perceived as doing little to promote the individual's informed decisions about whether or not to provide his or her data.

Rapid changes in technology further strain the ability of companies to provide useful notice. Ubiquitous deployment of sensors, advances in big data, real-time analytics, and the complex

[7] *APEC: Privacy Framework*, ASIA-PACIFIC ECONOMIC COOPERATION (2005) http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx.

[8] As discussed here, articulations of fair information practices take different forms in different jurisdictions. Issues related to individual awareness and notice can be found within all of them. In this paper, the starting point of the analysis is the fair information practices as the FTC and the White House have articulated them. The FTC's version has been criticized as being too limited and as having excluded several important principles (e.g., purpose specification). The White House adopted a more inclusive version of the Fair Information Practice Principles (FIPPs) in its 2012 Consumer Privacy Bill of Rights. Moreover, in current discussions of privacy governance, some companies have returned to analysis of a more comprehensive articulation of fair information practices as they seek guidance that addresses issues raised by big data analytics, fosters interoperability with non-US privacy laws, and promotes robust global data flows. Achieving the openness described in the first principle challenges organizations regardless of which version of fair information practices they adopted.

vendor relationships and data sharing partnerships that characterize today's data ecosystem challenge organizations' ability to explain their data practices. The need to use data robustly and in innovative ways clashes with requirements that notices specify a particular purpose or use for the data collected. The degree to which data collection is integrated into infrastructures (such as intelligent vehicle highway systems) or environments (such as retail locations or public spaces) can make posting notice difficult, and new technologies such as mobile devices with small screens create new challenges for providing meaningful notice.

Currently, a single privacy notice is expected to support many functions, including regulation, consumer choice, and public education about data practices. This Article argues that the current and emerging data ecosystems call for considering whether the current notice model can continue to serve all of these purposes. Moreover, it raises the question whether notices alone can create the conditions necessary to ensure that there are "no personal data record-keeping systems whose very existence is secret" as stated in the first principle of fair information practices.[9]

This Article argues that to achieve the openness required by the first fair information practice principle, data protection and privacy should move from a "notice" model to one of "transparency." It also asserts that the terms "notice" and "transparency" are not synonymous and that different definitions apply to each. It also defines notice as the posted articulation of a company's privacy practices and policies. In contrast, transparency is a condition of disclosure and openness jointly created by companies and policy makers through the use of a variety of approaches, including notice.

This Article argues that notice is an essential tool for creating transparency, but that establishing transparency requires far more than notice. It requires implementing the measures necessary to create an environment of transparency. Whether transparency is achieved depends not only on the posting of information but also on

[9] *Records, Computers and the Rights of Citizens*, *supra* note 2.

the *perceived quality* of the disclosure.[10] It argues that the Authors' experience with notice over the last twenty years demonstrates that a single notice cannot fully inform consumers, regulators, and the public about data practices. Rather, to achieve the transparency required by the first principle of fair information practices—particularly given the complexity of the emerging data eco-system—organizations must employ a variety of tools that support the various functions notice alone was once intended to serve. Creating a transparent data environment requires an understanding of these functions. It also involves understanding the limitations of traditional notice. Importantly, it requires identifying the various audiences that must be served and the needs of each.

This Article also reviews the history of notice in the United States and its traditional role in privacy and data protection. It considers the challenges and limitations of notice; the attempts of business, government, experts, and technologists to address them; and the lessons learned from these efforts. It also examines the implications of emerging technologies and data uses for notices. Finally, it proposes ways in which effective transparency can be achieved, including the role of notice. It is important to note that this Article is limited to the issues related to notice and to fostering transparency. The authors recognize the importance of the full complement of fair information practice principles and that transparency alone is not sufficient to assure the fair use of data. The authors also recognize the importance of meaningful choice or consent and that notice as it is currently implemented is the mechanism by which individuals now learn about their opportunity to consent or choose if available.[11] However, issues related to the current implementation of the other fair information practices principles are beyond the scope of this Article.

---

[10] *See* A.K. Schnackenberg and E.C. Tomilson, *Organizational Transparency: A New Perspective on Managing Trust in Organization-Stakeholder Relationships*, JOURNAL OF MANAGEMENT 1, 5 (2014).

[11] The history of notice reflected in this paper is admittedly limited to the United States. However, many of the strengths and limitations of notice revealed by this experience are relevant across jurisdictions.

II. BACKGROUND: A HISTORY OF NOTICE

In his seminal work, *Privacy and Freedom*, Alan Westin discussed individuals' awareness about the collection, processing, and storage of data as one means to protect against the unfair treatment that can result when inaccurate information is used or shared to make decisions about them.[12] His work emphasized that when individuals do not know that information systems exist, they cannot challenge either a particular use or disclosure, or the decisions that result.[13]

Notice first emerged as a mechanism to achieve awareness and a basis for promoting legitimate use of personal information when large-scale computerized systems emerged in the 1970s. In the 1990s, the Internet and e-commerce renewed discussion about the need to provide notice to individuals about the collection and use of personal data. This Article briefly reviews the evolution of notice in the United States beginning in the 1970s through the release in 2012 of major privacy reports by both the White House and the Federal Trade Commission.[14] This Article also discusses how 21st century technologies such as mobile applications, big data analytics, and the Internet of Things challenge the utility of traditional notice and the ability to effectively provide it.

A. *The Origins of Notice*

In the early 1970s, then Secretary of Health, Education, and Welfare, Elliot Richardson, established the Secretary's Advisory Committee on Automated Data Systems in response to growing public concerns about the harmful consequences of widespread use

---

[12] ALAN F. WESTIN, PRIVACY AND FREEDOM (New York: Antheneum, 1970). In particular, see Chapter 7, "The Revolution in Information Collection and Processing: Data Surveillance."

[13] *Id.* at 160.

[14] We limit our review to the evolution of notice as an element of fair information principles in the United States. For a comparative analysis of fair information principles outside the U.S., see FRED H. CATE, THE FAILURE OF FAIR INFORMATION PRACTICE PRINCIPLES, IN CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY (Jane K. Winn ed., 2006) ("Failure of Fair Information Practice Principles").

of computer and telecommunications technology. [15] The Committee's report, *Records, Computers, and the Rights of Citizens*, articulated the original Code of Fair Information Practices. The first of these states that, "[t]here must be no personal-data recording keeping systems whose very existence is secret."[16] The report called for any organization maintaining an administrative personal data system to provide public notice once a year and detailed what information the notice should include.[17]

In 1974, Congress passed the Privacy Act,[18] designed to regulate the federal government's collection and protection of information about citizens.[19] The Act's key requirements are based on principles of fair information practices.[20] The Privacy Act also called for the creation of the Privacy Protection Study Commission ("PPSC"), charging it with examining a wide range of record-keeping practices and privacy issues arising in the public sector and in a variety of commercial environments.[21] In its 1977 report, the PPSC articulated objectives for data protection systems [22] and reiterated the

---

[15] *Records, Computers and the Rights of Citizens*, *supra* note 2.

[16] *Id.* For a more complete history of the Code, see Robert Gellman, *Fair Information Practices: A Basic History*, Version 2.12, August 2014, *available at* http://www.bobgellman.com.

[17] *Id.* at 49.

[18] 5 U.S.C. § 552a (2016).

[19] The Privacy Act requires agencies collecting information to, *inter alia*, "inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual— (A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary; (B) the principal purpose or purposes for which the information is intended to be used; (C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and (D) the effects on him, if any, of not providing all or any part of the requested information . . . ." 5 U.S.C. § 522 (e)(3) [hereinafter PRIVACY].

[20] Fair Information Practices (FIPS) refer to a set of principles designed to guide organization in the collection, use and protection of personal data. They serve as a basis for law and self-regulation throughout the world.

[21] *Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission*, *supra* note 3.

[22] Privacy Act of 1974 Pub. L. No. 93-579, 88 Stat. 1896 § 5, as amended by Act of June 1, 1977 Pub. L. No. 95-38, 91 Stat. 179, established the Privacy

importance of openness to fairness. The report included recommendations related to a variety of data uses, among them direct marketing mailing lists.[23] The PPSC was asked to investigate whether a party that engages in interstate commerce and maintains a mailing list should be required to remove an individual's name and address from that list, absent an exception in law.[24] However, the report instead recommended that private sector organizations that share their mailing lists with third parties provide notice of this practice to the individuals on the list and provide an opportunity for individuals to opt out of sharing.[25] The report recommendation effectively articulated what is now referred to as "notice and choice" for the first time.[26]

Protection Study Commission and provided that the Commission study data banks, automated data processing programs and information systems of government, regional and private organizations to determine standards and procedures in force for protection of personal information. It further charged the Commission with reporting to the President and Congress the extent to which requirements and principles of the Privacy Act should be applied to the information practices of those organizations, and that making other legislative recommendations to protect the privacy of individuals while meeting government and society's legitimate need for information. *See* PRIVACY, *supra* note 19.

[23] Privacy Act, *supra* note 22.

[24] Privacy Act of 1974 § 5(c)(2)(B)(i).

[25] PRIVACY, *supra* note 19. *See* Fred H. Cate, *The Failure of Fair Information Practices Principles in* CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY (Jane K. Winn ed., Ashgate Publishing 2006). In 1997, the Direct Marketing Association voted to make compliance with this form of "notice and choice" a requirement for DMA membership beginning in 1999. *See* DIRECT MARKETING ASS'N, PRIVACY PROMISE: MEMBER COMPLIANCE GUIDE (1999).

[26] Notice became an established global principle for privacy in 1980 when the Organization for Economic Co-operation and Development (OECD) issued its *Guidelines Governing the Protection of Privacy and Transborder Data Flow of Personal Data* (c(80)58/FINAL) (Sept. 23, 1980 amended on July 11, 2013), *available at* http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#top. These guidelines have served as the basis for law, regulation, international agreement and industry best practices, most notably the European Union's Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281), http://ec.europa.eu/justice/data-protection; *supra* note 7.

B. *Online Privacy and Notice*

In the 1990s, the promise of a new National Information Infrastructure[27] ("NII") brought with it recognition that new privacy risks threatened the benefits the Internet promised. In 1993, Vice President Gore created the Information Infrastructure Task Force ("IITF"), and he charged it with developing comprehensive policies and programs that would promote the development of the NII.[28] A Privacy Working Group was created within the IITF, and in June 1995 it released *Privacy and the National Information Infrastructure*: *Principles for Providing and Using Personal Information*. [29] Included was a notice principle requiring that individuals be given sufficient information to make an informed decision about his or her privacy. [30] The role of notice was subsequently reinforced in the 1997 White House *Framework for Global Electronic Commerce*,[31] which stated that the IITF privacy principles, built on the 1980 OECD Guidelines, [32] require that "[d]ata-gatherers should inform consumer what information they are collecting and how they intend to use such data[.]"[33]

In the 1990s, the FTC began a separate consumer privacy initiative to examine and understand online privacy issues. In 1996, it reported that participants in a workshop on online privacy generally agreed that notice of information practices is a first principle, essential to advancing privacy online; they disagreed,

---

[27] The term "NII" resulted from the High Performance Computing Act of 1991 (Pub L. No. 102-94,15 U.S.C. §5501). It became a popular buzzword during the Clinton Administration.

[28] *Options for Promoting Privacy on the National Information Infrastructure: Draft for Public Comment*, U.S. DEP'T OF HEALTH & HUM. SERV. (Apr. 1, 1997), https://aspe.hhs.gov/legacy-page/options-promoting-privacy-142716.

[29] *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information, Final Report*, U.S. DEP'T OF HEALTH & HUM. SERV. (June 6, 1995), http://aspe.hhs.gov/datacncl/niiprivp.htm.

[30] *Id.*

[31] President William Clinton, *A Framework for Global Electronic Commerce*, THE WHITE HOUSE (July 1, 1997), http://clinton4.nara.gov/WH/New/Commerce/read.html [hereinafter The White House].

[32] OECD, *supra* note 26.

[33] The White House, *supra* note 31.

however, about the substance of privacy notices.[34] In 1998, the FTC analyzed the content of a sample of commercial websites to determine how many of them posted privacy notices, and among those that did, whether those notices contained the core elements of fair information practices.[35] In its resulting report to Congress, the FTC asserted "the most fundamental principle is notice."[36] Georgetown University and the FTC conducted follow-up sweeps in 1999 and 2000, respectively.[37] While Congress did not enact comprehensive federal online privacy legislation as a result of these findings, online privacy notices nonetheless emerged as a best practice. However, in 2003 California enacted the California Online Privacy Protection Act,[38] which required operators of commercial websites that collected personal information from California residents to post a privacy notice that meets certain requirements.[39] Because online businesses typically serve a national audience

---

[34] *Federal Trade Commission*, *Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure* (Dec. 1996), http://www.ftc.gov/reports/staff-report-public-workshop-consumer-privacy-global-information-infrastructure. The Report also stated that there was general agreement that in addition to notice, organizations should offer choice, provide access, secure and maintain the quality of the personal information in their custody. *Id.*

[35] This research was also described as a "web sweep." Websites included in the sample were first reviewed to see if they collected personal information. If it did, the website was further examined to determine whether it posted a privacy notice, and if so, whether it mentioned how the website used the information, whether it offered choice about how this information was used, and if there were any statements about access or security.

[36] *Privacy Online: Report to Congress*, FED. TRADE COMM'N, 7 (June 1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

[37] "*Self-Regulation and Privacy Online," FTC Report to Congress*, FED. TRADE COMM'N (July 13, 1999), https://www.ftc.gov/news-events/press-releases/1999/07/self-regulation-and-privacy-online-ftc-report-congress; *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress*, FED. TRADE COMM'N, 13 (May 2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf. In the 2000 sweep, the FTC found that only 41% of sites in its random sample and 60% of the "Most Popular Group" met basic standards of notice and choice. *Id.*

[38] *See* CAL. BUS. & PROF. CODE §§ 22575-22579 (West 2003).

[39] *Id.*

independent of where they are based, the California law effectively imposed a requirement for all U.S. online businesses to post a privacy notice.[40]

Both the White House and the FTC revisited notice when they issued major reports on privacy in 2012.[41] The reports discuss notice in the context of *transparency*.[42] In each report, notice remains the fundamental mechanism for providing transparency to consumers.[43] The White House Report extensively references notice in its discussion of transparency, highlighting its role, the challenges faced by organizations providing notice in light of emerging technology, and the significance of the consumer-company relationship in determining how notice is provided.[44] In its report, the FTC emphasized greater transparency as one means to advance its consumer privacy goals.[45] It argued for measures that could make companies' data practices more transparent, including improved privacy notices that promote information practices and enable consumers to compare privacy practices among organizations and choose among them on that basis.[46]

In summary, over more than four decades the privacy discussions in the United States have centered on a common theme: technology holds the potential to provide enormous benefit to the economy, firms and individuals, if the privacy concerns raised by successive generations of technology are addressed. Notice, despite

---

[40] *California Online Privacy Protection Act of 2003*, COOLEY ALERT! (June 2004), https://cooley.com/files/ALERT-Cal_OPPA.pdf.

[41] *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, THE WHITE HOUSE (Feb. 2012), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf [hereinafter Consumer Data Privacy]; *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, FED. TRADE COMM'N (March 1, 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [hereinafter Protecting Consumer Privacy].

[42] *Id.*

[43] *Id.*

[44] *Consumer Data Privacy, supra* note 41.

[45] *Protecting Consumer Privacy, supra* note 41. The report also highlighted simplified consumer choice and privacy-by-design. *Id.*

[46] *Id.*

its limitations, remains the primary method for promoting awareness and addressing these privacy concerns. We now discuss the role of traditional privacy notices, their challenges and limitations.

III. THE ROLES OF TRADITIONAL NOTICE

Since the principles of fair information practices were articulated in the 1970s, traditional notice has evolved to serve many functions for individuals, businesses, regulators, advocates, and the media.

A. *Supporting Consumer Privacy Decisions*

Perhaps the essential role for notice is to inform individuals' decisions about the use of their personal information. In theory, notice supports autonomy by raising awareness and placing decisions in the hands of the individual.[47] As described above, there is widespread agreement that awareness promotes fairness and is the first principle of fair information use. Notice provides the basis for two types of decisions. First, if choice or consent is available, the information in notices about an organization's data practices helps individuals decide whether to engage with the organization or to allow subsequent uses of their personal information. Second, notices enable individuals who value privacy to compare the practices of different organizations and to choose which companies they wish to do business with based on the firm's data practices. Privacy notices then could serve as the basis for a market solution for privacy.

B. *Supporting a Market Solution for Privacy*

In 1997, the Clinton Administration released *A Framework for Global Electronic Commerce,*[48] outlining the Administration's strategy for increasing consumer and business confidence in the use of electronic networks for commerce.[49] After consulting with industry, consumer groups, and the Internet community, the Administration issued five principles to guide government support

---

[47] Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1049 (2012).

[48] *A Framework for Global Electronic Commerce*, *supra* note 31.

[49] *Id.*

for the development of electronic commerce.[50] It made recommendations about three types of issues where international agreements are needed to preserve the Internet as a minimally-regulated medium, one in which competition and consumer choice would shape the marketplace.[51]

In its discussion of privacy, the Framework [52] notes that the privacy principles it articulates build on the OECD Guidelines.[53] The Framework focuses on precepts of awareness and choice and emphasizes that:

> [d]isclosure by data-gatherers is designed to simulate market resolution of privacy concerns by empowering individuals to obtain relevant knowledge about why information is being collected, what the information will be used for, what steps will be taken to protect that information, the consequences of providing or withholding information, and any rights of redress that they may have. Such disclosure will enable consumers to make better judgments about the levels of privacy available and their willingness to participate.[54]

The Framework further noted that in the interest of fostering unimpeded flows of data on the Internet, the U.S. would engage its trading partners in discussions to build support for industry-developed solutions to privacy and for market-driven mechanisms to promote consumer satisfaction about how their data is handled.[55]

---

[50] *See id.* The five principles include: 1) The private sector should leave, 2) Governments should avoid undue restrictions on electronic commerce, 3) Where government involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce, 4) Governments should recognize the unique qualities of the Internet, 5) Electronic Commerce over the Internet should be facilitated on a global basis. *Id.*

[51] *Id.* at 6. The three issue areas are financial issues related to customs, taxation, and electronic payments; legal issues including a UCC for e-commerce, intellectual property, privacy, and security; and market access issues including information technology, content, and technical standards.

[52] *Id.*

[53] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, ORG. FOR ECON. CO-OPERATION AND DEV. (2013), http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[54] *Framework for Global Electronic Commerce, supra* note 31, at 17.

[55] *Id.*; *Privacy and Self Regulation in the Information Age*, U.S. DEPT. OF COM. (1994), http://www.ntia.doc.gov/report/1997/privacy-and-self-regulation-information-age.

To realize this vision of a market solution for privacy, in the mid-1990s, the Department of Commerce engaged in a concerted effort to urge companies to post privacy notices.[56] Based on the privacy practices articulated in notices posted across the commercial sector, individuals could inform themselves, compare notices, and determine whether or not to do business with a particular company, or whether to choose to look elsewhere for a good or service. Privacy could serve as a brand differentiator, arguably attracting individuals who valued companies that collected, shared, and used data responsibly.[57]

The Clinton Administration's Framework also reinforced the role of private sector leadership, and that market forces should guide the development of the Internet. Further, the Internet should not be subject to unnecessary regulation.[58] The Administration emphasized that even in situations where collective action was called for, government should encourage industry self-regulation and private sector leadership wherever possible.[59] It highlighted the need to support the efforts of private sector organizations to develop mechanisms to facilitate the successful operation of the Internet.[60]

The National Telecommunication and Information Administration of the Department of Commerce ("NTIA") highlighted this support for self-regulation as a mechanism to protect privacy and published a compendium of papers authored by experts in law, economics, and business, which examined the strengths and limitations of self-regulation as an approach to

---

[56] *See, e.g*, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information*, US DEPT. OF COM. (October 1995), *available at* https://www.ntia.doc.gov/legacy/ntiahome/privwhitepaper.html.

[57] Eli M. Noam, *Privacy and Self-Regulation: Markets for Electronic Privacy*, COLUM. U., http://www.citi.columbia.edu/elinoam/articles/priv_self.htm (last visited Apr. 28, 2016); *Privacy and Self-Regulation in an Information Age, supra*, note 54; Hal Varian, *Economic Aspects of Personal Privacy*, U. OF CAL. BERKLEY (Dec. 6, 1996), http://people.ischool.berkeley.edu/~hal/Papers/privacy.

[58] *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information, supra* note 56.

[59] *Id.*

[60] *Id.*

protecting personal information.[61] In a paper titled "Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information,"[62] Peter Swire describes self-regulation as a governance instrument that encompasses each of the functions of the three branches of government – legislation, enforcement, and adjudication. He discusses the work of industry groups to develop and issue codes for privacy. In some instances, he argues, the guidelines themselves serve no enforcement function, but are made available to industry groups, government, and the public.[63] But in others, the codes incorporate enforcement provisions. He further discusses the role of industry groups in adjudicating complaints and initiating enforcement actions.[64] His paper also lays out the strengths of self-regulation—its ability to benefit from industry expertise, to create flexible guidance that keeps pace with industry developments, and to stave off government regulation that may be too prescriptive and therefore limit innovation.[65]

In these early stages, industry-wide codes of conduct (as opposed to company-specific practices) served as an important tool in FTC enforcement of the terms of notices.[66] Collective self-regulatory groups arguably are positioned to use market dynamics to encourage adherence to industry "best practices" on the theory that no company can afford to be viewed as indifferent to the privacy concerns of the public.[67] Moreover, in contrast to the self-regulatory efforts of individual companies, self-regulatory groups can adopt collective mechanisms to investigate and resolve consumer

---

[61] *Privacy and Self Regulation in the Information Age*, U.S. DEPT. OF COM. (June 12, 1997), *available at* http://www.ntia.doc.gov/report/1997/privacy-and-self-regulation-information-age.

[62] *See* Peter Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information,* U.S. DEPT. OF COM. (June 12, 1997) 3–19, *available at* https://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy.

[63] *Id.*

[64] *Id.*

[65] Swire's analysis also highlights the limitations of the "pro-self-regulation" argument. *See id.*

[66] CHRIS JAY HOOFNAGLE, FED. TRADE COMM'N. PRIVACY LAW AND POLICY 175–81 (2016).

[67] *Id.*

complaints and thus enforce each company's compliance with a given industry's best practices.[68] FTC oversight—in conjunction with that of state and local authorities—complements such self-regulatory enforcement by providing an independent legal incentive for each member company, and the group as a whole, to live up to its promised standard of behavior.

An early example of such a code was developed by the Online Privacy Alliance ("OPA").[69] Formed in 1998 as a cross-industry coalition of more than 80 global companies,[70] the OPA's stated mission was "to lead and support self-regulatory initiatives that create an environment of trust for online privacy."[71] It developed standards of conduct that were tailored to the online environment and which required that all members adopt and post a privacy policy.[72] The organization established guidelines for online privacy notices, a framework for self-regulatory enforcement, and a special policy concerning collection of information from children. It also required that its members adhere to the guidelines and policies, which the organization posted on its website. The OPA's guidance focused on notice to consumers; limitations on purposes and onward transfers; data quality; access to data and correction; security; and collection of data from children.[73] OPA's comments on its notice requirements reflected the role of privacy policies in informed consumer choice and promoting the use of market forces to encourage good privacy practices.[74]

---

[68] *Id.*

[69] *See Privacy Alliance,* ONLINE PRIVACY ALLIANCE, http://www.privacyalliance.org/resources (last visited Apr. 14, 2016). The OPA is no longer active.

[70] *Id.*

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] The data privacy standards announced by the Individual Reference Services Group ("IRSG")—an association of fourteen major companies in the individual reference services industry—are another instance of a cross industry effort to establish standards of conduct as the basis for self-regulation. *Individual Reference Services: A Report to Congress*, FED. TRADE COMM'N (Dec. 1997), https://www.ftc.gov/reports/individual-reference-services-report-congress. The individual reference services industry gathers personal information about

C. *Serving as a Basis for Regulation: The Federal Trade Commission*

In theory, notice is an attractive regulatory vehicle for several reasons. It is based on an assumption that information provides the basis for better individual decisions when individual preferences vary. Notices also allow for flexibility in an environment characterized by a wide variety of business models. A notice regime is also relatively easy to enforce, as regulators only have to verify that the description of the practices is accurate. Notices differ from warnings, as the purpose of warnings is to prevent a high-risk activity related to health or safety, while the goal of a notice is to inform decisions.[75]

---

individuals from a number of sources, both public (e.g., state driving records) and private (e.g., credit information) and provides that information for a fee to privacy parties and the government. *Id.* To protect the often-sensitive personal data with which IRSG members deal on a day-to-day basis, the group has adopted binding standards for the protection of personal information. *Id.* The IRSG developed these rules with the advice and participation of the FTC, and the agency endorsed them as a promising mechanism to "lessen the risk that information made available through [individual reference] services is misused . . . [and] address consumers concerns about the privacy of non-public information in the services databases." *Id.*

[75] *See, e.g.*, Omri Ben-Shahar & Carl Schneider, *The Failure of Mandated Discourse*, 159 U. PA. L. REV. 647 (2011); Ryan Calo, *Against Notice Skepticism in Privacy (And* Elsewhere*),* 87 NOTRE DAME L. REV. 1027 (2012); Archon Fung, Mary Graham & David Weil, *Full Disclosure: The Perils and Promise of Transparency*, CAMBRIDGE UNIVERSITY PRESS, 2007.

Section 5 of the Federal Trade Commission Act[76] empowers the FTC to investigate and halt any "unfair"[77] or "deceptive"[78] conduct in almost all industries affecting interstate commerce.[79] This authority includes the right to investigate a company's compliance with its own asserted data privacy protection policies. Pursuant to

[76] 15 U.S.C § 45 (2012).

[77] The FTC has articulated three elements of deception as: (1) there must be a representation, omission, or practice that is likely to mislead the consumer; (2) the act or practice must be considered from the perspective of the reasonable consumer; and (3) the representation, omission or practice must be material. *See FTC Policy Statement on Deception*, FED. TRADE COMM'N. (Oct. 14, 1983), https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception (last visited Apr. 14, 2016). In *In re Gateway Learning Corp.*, the FTC alleged that Gateway committed unfair and deceptive trade practices by making retroactive changes to its privacy policy without informing customers and by violating its own privacy policy by selling customer information when it had said it would not. *Gateway Learning Corp., In the Matter of,* FED. TRADE COMM'N. (Dec. 28, 2004), https://www.ftc.gov/enforcement/cases-proceedings/042-3047/gateway-learning-corp-matter. Gateway settled the complaint by entering into a consent decree with the FTC that required it to surrender some profits and placed restrictions upon Gateway for the following 20 years. *Id.*

[78] Courts have identified three main factors that must be considered in consumer unfairness cases: (1) whether the practice injures consumers; (2) whether the practice violates established public policy; and (3) whether it is unethical or unscrupulous. FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 244–45 n.5 (1972). The Circuit Courts have concluded that this quotation reflected the Supreme Court's own views. *See* Spiegel, Inc. v. FTC, 540 F.2d 287, n.8 (7th Cir. 1976); *see* Heater v. FTC, 503 F.2d 321, 323 (9th Cir. 1974). Since then the Commission has continued to refine the standard of unfairness in its cases and rules, and it has now reached a more detailed sense of both the definition and the limits of these criteria. *See FTC Policy Statement on Unfairness*, FED. TRADE COMM'N. (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness (last visited Apr. 14, 2016).

[79] In addition to its Section 5 authority, the FTC is delegated broad enforcement power under a variety of statutes designed to promote fair competition and protect the interests of consumers. Certain of these statutes—like the Fair Credit Reporting Act—specifically empower the FTC to investigate and prosecute violations of U.S. law governing the treatment of specific types of information relating to an individual's credit and finances. Others—like the Children's Online Privacy Protection Act of 1998—grant the FTC authority to regulate certain data protection practices and dictate minimum standards for the collection and distribution of discrete types of personal information (e.g., data relating to children).

Section 5, the FTC may issue cease and desist orders and may also order other equitable relief, including redress of damages.[80] The FTC acts under this power to investigate organizations whose practices do not conform to the policy articulated in the privacy notice and to provide oversight and enforcement for the U.S. self-regulatory regime in the absence of an omnibus consumer privacy law.[81]

1. *GeoCities*

The first FTC enforcement action against a website operator, the GeoCities[82] case, demonstrated the FTC's use of Section 5 to require companies to operate in accordance with their posted information protection practices.[83] In *GeoCities*, the FTC challenged the accuracy of the company's posted representations about the use of marketing information collected from individuals registering at the site.[84] The FTC's complaint also alleged that GeoCities implied that it operated a website for children but failed to disclose to the children or their parents that an independent third party operated the site.[85] GeoCities denied the allegations, but established information policies and procedures in accordance with standards proposed by the FTC.[86] GeoCities was required to comply with requirements

---

[80] 15 U.S.C § 45(a)(2) (2006).

[81] For a comprehensive discussion of the FTC's role in oversight and enforcement, see D. Solove and W. Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUMBIA L. REV. 583, (2014) and CHRIS JAY HOOFNAGLE, FED. TRADE COMM'N PRIVACY LAW AND POLICY 2016.

[82] *See* GeoCities, Docket No. C-3850 (F.T.C. August 13, 1998). The full case materials are available at https://www.ftc.gov/enforcement/cases-proceedings/982-3015/geocities.

[83] *Id.*

[84] GeoCities, Docket No. C-3850 (F.T.C. February 5, 1999) (Complaint).

[85] *Id.*

[86] Under the terms of the consent order, GeoCities agreed to provide clear and prominent notice to consumers of its information practices, including what information is collected through its website, the intended uses for that information, any third parties to whom that information would be disclosed, the means by which a consumer might access information collected and the means by which a consumer could have the information removed from the company's databases. GeoCities also agreed that it would not misrepresent the identity of any third party that collected data from a website the company promoted or sponsored. Finally, GeoCities agreed to contact all consumers from whom it had collected

specified in a consent order.[87] In addition, the publicity surrounding the FTC enforcement action concerning a then-prominent website operator motivated other companies to post accurate notices and fulfill the promises made in them.[88]

2. *Toysmart*

In a later case, Toysmart.com agreed to settle charges that the company violated Section 5 of the FTC Act by failing to act in accordance with representations to consumers that it would never share their personal information with third parties.[89] When the company ran into financial problems, it attempted to sell all of its assets, including detailed personal information about visitors to its site—name, address, billing information, shopping preferences, and family profiles, including names and birthdates of children—contrary to the assertions in the company's privacy statement.[90] On July 10, 2000, the FTC filed a lawsuit in the U.S. District Court for the District of Massachusetts against Toysmart to prevent the sale of the customer information.[91] The resulting settlement agreement forbade the sale of this customer information except under very limited circumstances.[92]

---

personal information and afford those individuals an opportunity to have data removed from the data bases both of the company and any third party. *See* GeoCities, Docket No. C-3850 (F.T.C. February 5, 1999) (Consent Order).

[87] *Id.*

[88] *See, e.g.*, CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 2016.

[89] *See* Toysmart.com, LLC, Civil Action No. 00-11341-RGS (F.T.C. July 21, 2000). The full case materials are available at https://www.ftc.gov/enforcement/cases-proceedings/x000075/toysmartcom-llc-toysmartcom-inc.

[90] Toysmart.com, LLC, Civil Action No. 00-11341-RGS (F.T.C. July 21, 2000) (First Amended Complaint).

[91] In re Toysmart.com, LLC, Case No. 00-13995-CJK (Bankr. E.D. Mass. 2000).

[92] Under the settlement agreement, Toysmart was allowed only to sell customer lists as part of a package which included the entire website, and only to an entity that expressly agreed to abide by the terms of the Toysmart privacy statement and to follow certain procedures if it wished to change the policy. *See* Toysmart.com, LLC, Civil Action No. 00-11341-RGS (F.T.C. July 21, 2000) (Stipulated Consent Agreement).

3. *Microsoft*

In the Microsoft[93] case, Microsoft Corporation agreed to settle Federal Trade Commission charges regarding the assertions it made about the privacy and security of personal information collected from consumers through its "Passport" web services.[94] The Commission initiated its investigation of the Passport services in response to a complaint filed by a coalition of consumer groups led by the Electronic Privacy Information Center in July 2001.[95]

The consent order prohibited any misrepresentation of information practices in connection with Passport and other similar services.[96] It also required Microsoft to implement and maintain a comprehensive information security program.[97] In addition, Microsoft was required to have its security program certified as meeting or exceeding the standards in the consent order by an independent professional every two years.[98]

---

[93] *See* Microsoft Corporation, Docket No. C-4069 (F.T.C. December 24, 2002). The full case materials are available at https://www.ftc.gov/enforcement/cases-proceedings/012-3240/microsoft-corporation-matter.

[94] The FTC also addressed issues of false representations about security in Eli Lilly and Company, Docket No. C-4047 (F.T.C. May 10, 2002). The full case materials are available at https://www.ftc.gov/enforcement/cases-proceedings/012-3214/eli-lilly-company-matter.

[95] According to the Commission's complaint, Microsoft made false representations about (1) the measures it deployed to maintain and protect the privacy and confidentiality of consumers' personal information collected through its Passport and Passport Wallet services; (2) the safety and security of the purchases made with Passport Wallet compared to purchases made at the same site without Passport Wallet; (3) the extent to which Passport did or did not collect personally identifiable information; and (4) the extent to which Passport gave parents control over information participating Web sites could collect from their children. *See* Microsoft Corporation, Docket No. C-4069 (F.T.C. December 24, 2002) (Complaint).

[96] *See* Microsoft Corporation, Docket No. C-4069 (F.T.C. August 8, 2002) (Agreement Containing Consent Order).

[97] *Id.*

[98] *Id.*

4. *Epic Marketplace*

In a later case, the FTC entered into a settlement with Epic Marketplace,[99] an online advertising company, which accessed users' browser histories to deliver targeted advertising.[100] The FTC found that Epic's failure to disclose this practice in its privacy policies violated Section 5 of the FTC Act.[101] The FTC identified a data activity and a material omission in a privacy policy.[102] It alleged a deceptive practice and entered into an enforcement action.[103] Unlike in previous cases, in which the FTC's enforcement focused on affirmatively inaccurate or false statements as deceptive—for example, in the Upromise case[104]—the Epic case signaled the FTC's inclination to find an organizations' inadequate disclosure about its data practices in itself to be inherently deceptive.[105]

According to the FTC complaint, Epic engaged in online behavioral advertising by tracking consumers' online activities to deliver targeted advertising specific to each user's interests, as identified based on their browsing history.[106] Epic asserted in its posted policy that it was merely tracking user visits to sites on Epic's network.[107] In practice, however, Epic obtained users' browsing histories from their browsers in order to deliver advertisements.[108] Epic observed browsing histories to learn about users' interest in sensitive financial and medical topics such as debt relief, personal

---

[99] *See* Epic Marketplace, Inc., Docket No. C-4389 (F.T.C. March 13, 2013). The full case materials are available at: https://www.ftc.gov/enforcement/cases-proceedings/112-3182/epic-marketplace-inc.

[100] Epic Marketplace, Inc., Docket No. C-4389 (F.T.C. March 13, 2013) (Decision and Order).

[101] Epic Marketplace, Inc., Docket No. C-4389 (F.T.C. March 13, 2013) (Complaint).

[102] *Id.*

[103] *Id.*

[104] The FTC alleged that Upromise's practice of using a web-browser toolbar to collect consumers' personal information without adequately disclosing the extent of the information it is collecting is deceptive. *See* Upromise, Inc., Docket No. C-4351 (F.T.C. March 27, 2012). The full case materials are available at https://www.ftc.gov/enforcement/cases-proceedings/102-3116/upromise-inc.

[105] *See supra* note 99.

[106] *See supra* note 101.

[107] *Id.*

[108] *Id.*

bankruptcy, incontinence, and fertility.[109] Epic's tracking practices involved not only monitoring Epic's network, but also gathering data from other sites as well, despite the claims to the contrary in the company's privacy policy.

D. *Informing the Public Dialogue about Data Use and Protection*

An organization's posted notices make its data and privacy practices public. Notices enable non-governmental organizations, advocates, and the press to monitor an individual company's activity with respect to data. Taken together, the notices posted by companies provide a window into the evolution of data-gathering technology and data practices across industry. In doing so, privacy notices and the information they make available foster a public conversation about data collection and use, and make possible a role for the public in the debate about how data is used and protected. In some instances,[110] privacy watchdogs, advocacy organizations, and interested individuals have discovered discrepancies in privacy notices or have tested a company's practices against the assertions in their notice and then brought their findings to the press and regulators.[111]

The complaint against Facebook brought before the FTC by the Electronic Privacy Information Center ("EPIC") in 2010 provides one example.[112] EPIC alleged business practices it believed to be unfair and deceptive under Section 5 of the FTC Act, including Facebook's disclosure of users' personal information to its partners without first obtaining users' consent, its disclosure of personal information to which users previously restricted access, and its disclosure of the information to the public when users elected to make that information available to friends only.[113] Central to EPIC's complaint was a detailed review of the representations in

---

[109] *Id.*
[110] *Id.*
[111] *Id.*
[112] In re Facebook, Inc., No. C-4365, (F.T.C. 2012), *available at* https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc. (The web site includes all the materials for the case).
[113] Epic Complaint to F.T.C. (Dec. 17, 2009), *available at* https://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.

Facebook's posted privacy policy and a comparison of those assertions against what EPIC asserted were actual information practices.[114] This complaint led the FTC to issue a consent decree with Facebook that bars Facebook from making deceptive privacy claims, requires that the company obtain consumers' approval before it changes the way it shares their data, and requires that its privacy practices undergo periodic assessment by independent, third-party auditors for the ensuing 20 years.[115]

E. *Providing an Opportunity for Internal Review of Data Practices*

The development and articulation of an accurate, current privacy notice requires considerable effort on the part of companies. To write a clear, comprehensive notice requires an understanding of the types of data the organization collects; the points and methods of collection; how data is used and with whom it is shared; where and how it is stored and how long it is kept; and how it is secured and protected from loss, wrongful access, or inappropriate use. It also requires that companies understand the data protection and privacy rules and laws that apply.

In conducting the inventory necessary to understand the company's data practices, organizations are given the opportunity to ask questions and make decisions about data. What do I collect? Do I need to collect it to carry out a particular function? With whom do I share data? Do I trust that third party to use data responsibly? How is the data secured? Have the circumstances of storage and the

---

[114] For example, Facebook has represented, expressly or by implication that, through their Profile Privacy Settings, users can restrict access to their profile information to specific groups, such as "Only Friends" or "Friends of Friends." In truth and in fact, in many instances, users could not restrict access to their profile information to specific groups, such as "Only Friends" or "Friends of Friends" through their Profile Privacy Settings. Instead, such information could be accessed by Platform Applications that their Friends used. *See* In re Facebook, Inc., No. C-4365, (F.T.C. 2012) (Complaint), *available at* https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc.

[115] In re Facebook, Inc., File No. 092 3184, (F.T.C. 2011) (Agreement Containing Consent Order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf.

threats of data intrusion changed since these security practices were last reviewed?

While not originally envisioned to function in this way, the drafting of a privacy notice provides a company with an opportunity to inventory and assess internal practices, making sure they are up to date, necessary, and appropriate. It can also serve as a platform for decision-making about whether to continue with a data practice or deployment of technology in light of considerations related to brand, and developments in law, policy, or market practices.

However, it provides the added benefit of helping companies keep abreast of data collection and use across the organization, stay aware of the privacy impact and potential risk of data use, and make reasoned decisions about appropriate data use and protection.[116]

IV. CHALLENGES AND LIMITATIONS OF CURRENT NOTICES

Critics of notice often argue that notices are of limited utility.[117] They assert notices are not useful because they are not drafted in a way that makes them useful to individuals; they also argue that because meaningful choice is rarely available to individuals, notice is no longer needed to inform individual choice. This Section addresses these arguments.

A. *Notices are often found to be complex, unclear, and too lengthy to be useful to consumers or to support meaningful choice.*

In the United States no omnibus federal law requires organizations to post notices. As a result, companies post notices to comply with state laws such as the California Online Privacy Protection Act of 2003[118] or they post notices voluntarily. The FTC generally has not articulated requirements about format, length,

---

[116] *See* Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1060 (2012).

[117] FRED H. CATE, CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY 360–63 (Jane K. Winn, 2006).

[118] The Online Privacy Protection Act of 2003, CAL BUS. & PROF. CODE §§ 22575-22579 (2004), *available at* http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=BPC&division=8.&title=&part=&chapter=22.&article=.

readability, or content of a given privacy notice.[119] As discussed above, the FTC brings actions based on unfair or deceptive practices to hold companies to whatever assertions they make in their posted policy.[120] Thus, even if law does not require a company to post a notice, once a company does post a notice, it is subject to enforcement of its terms. Because a company potentially incurs liability by posting a notice, corporate counsel offices are understandably motivated to limit legal exposure and draft notices that are lengthy and legalistic.[121] As a result, notices lack the attributes needed to provide consumers with what they need to know about an organization's data and privacy practices. Moreover, notices were originally intended to facilitate a one-on-one relationship between individuals and websites. Today, the complex technologies, business models and data practices, and networks of vendor relationships that support digital services (e.g., Internet of Things, cloud computing, big data, behavioral advertising) are difficult to explain and challenge attempts to draft simple, readable notices. It has been suggested that even if at a given moment a notice could reasonably describe an organization's information flows and data protection measures, the rapid change in technology, analytics, and business relationships can quickly render it inaccurate.[122]

To make traditional privacy notices useful to individuals, drafters face the challenge of communicating large amounts of complex, often technical information in a succinct, reader-friendly way. The notices that result often are hard to read (and even more difficult to understand), read infrequently, and do not support

---

[119] One exception is the GLB model form that specified content and format for GLB privacy notices. *See infra* Part V.C.1.

[120] *See supra* Part III.C.

[121] For example, one longitudinal study hypothesized that concerns about FTC enforcement actions resulted in a decrease in readability of privacy notices from 2001 to 2003. *See* George R. Milne, Mary J. Culnan and Henry Greene, *A Longitudinal Assessment of Online Privacy Notice Readability*, 26 J. OF PUB. POL'Y AND MKTG., 238, 249 (2006).

[122] Helen Nissenbaum, *A Contextual Approach to Privacy Online*, DAEDALUS, 32, 36 (2011).

rational decision making about privacy.[123] Because individuals have limited ability to process information, traditional notices often result in information overload and do not promote informed decisions.[124] Researchers estimate that the time alone invested in reading the privacy notices for the websites an individual visits on average in a given year is approximately 201 hours per year per person, representing a total national opportunity cost of $781 billion.[125] Further, privacy notices are only one type of disclosure that individuals encounter in a typical day, resulting in what Ben-Shahar and Schneider describe as the "accumulation problem" where people encounter too many disclosures overall to digest the majority of them.[126]

Whether a notice is clear or not depends upon whether the target audience reasonably can be expected to be able to read and comprehend it. Research has revealed significant readability issues with current privacy notices.[127] For example, Jensen and Potts measured readability for online privacy notices for 47 high-traffic Web sites and found that on average, these notices had a grade-level readability score of 14.2—two years past high school.[128] Milne and his colleagues conducted a longitudinal assessment of the readability of privacy notices of 321 top Web sites based on unduplicated visitors.[129] The initial grade-level readability score was

---

[123] *See, e.g.*, George R. Milne & Mary J. Culnan, *Strategies of Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices*, 18 J. OF INTERACTIVE MKTG., 15, 29 (2004).

[124] *See* Calo, *supra* note 116.

[125] Alecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, I/S, A J. OF L. AND POL'Y FOR THE INFO. SOC'Y, (2008), *available at* http://www.is-journal.org.

[126] Omar Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosures*, 159 U. PA. L. REV. 647, 705–08 (2011) (providing an interesting illustration of the accumulation problem).

[127] Carlin Jensen & Colin Potts, *Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices*, 6 CHI LETTERS 471, 478, (2004).

[128] Jensen and Potts reviewed 64 privacy policies, analyzing among other things their accessibility. They attributed ease of use to how easily it is for consumers to locate the policy, a function of where the link is placed and how visible it is to users. *Id.*

[129] Milne et al., *supra* note 121.

11.2—equivalent to some high school.[130] Two years later, the grade level increased to 12.3 and 58 percent of the notices had increased in length.[131] Both studies criticized existing notices for being written at an educational level exceeding that of a large proportion of the population. In a survey of 119 participants, Acquisiti and Grossklags found that 41 percent read privacy policies only rarely, even after expressing a high degree of concern about privacy.[132] Further, recent studies also found that a majority of the public incorrectly assumes that the existence of a privacy policy necessarily means that the firm will protect the confidentiality of all their personal information. [133]

A notice's usefulness also depends in part on whether or not an individual can easily locate it. When privacy notices are difficult to access – obscured by their location or posted in lettering that blends with other text – they provide little help to individuals attempting to understand data practices or choose whether or not to engage with a company or use a device or service.

The FTC addressed this issue in 2009, when it entered into a consent decree with Sears Holding Management Corporation.[134] The FTC enforcement action began after Sears disseminated a "research" software application for consumers to download and install on their home computers in connection with the "My SHC Community" program.[135] According to the FTC, Sears represented to consumers that this software application, if downloaded and

---

[130] *Id.*

[131] *Id.*

[132] Alessandor Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, JAN./FEB. IEEE SECURITY & PRIVACY 24, 30, (2005).

[133] *See* Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, FACT TANK, PEW RESEARCH CENTER, (Dec. 4, 2014), http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/; Joseph Turow, Michael Hennessy & Nora Draper, *The Tradeoff Fallacy*, ANNENBERG SCH. FOR COMMC'N., UNIV. OF PENN, (June 2015), https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.

[134] *In the Matter of Sears Holdings Management*, Docket No. C-4264 (2009), https://www.ftc.gov/enforcement/cases-proceedings/082-3099/sears-holdings-management-corporation-corporation-matter.

[135] *Id.*

installed, would track consumers' "online browsing" activities.[136] The FTC alleged that Sears failed to disclose to consumers that the application would (i) track nearly all of the consumers' online behavior (including information provided in secure sessions with third-party websites, shopping carts and online accounts), (ii) track certain offline activity on the computer, and (iii) transmit most of the tracked information to Sears' remote computer servers.[137] In its complaint, the FTC argued that these facts would be material to consumers when deciding whether to install the software, and Sears' failure to disclose the information constituted a deception in violation of Section 5 of the FTC Act.[138] The FTC acknowledged the application "functioned and transmitted information substantially as described in the [Privacy Statement and User License Agreement]," but noted that this disclosure was available only in the lengthy agreement provided near the end of the multi-step registration process.[139]

B. *Choice is increasingly less meaningful, appropriate and/or available to the consumer, raising the question of why notice is relevant or necessary at all.*

In the fair information practices principles, choice was articulated to allow individuals to limit secondary use when personal information was collected for one purpose and used for other purposes.[140] In practice, choice is offered for a limited set of practices: individuals can opt-out of unwanted marketing email or targeted advertising based on their online browsing behavior, but not the receipt of online advertising in general.[141]

---

[136] *Id.*
[137] *Id.*
[138] *Id.*
[139] *Id.*
[140] The principle of use limitation is found in the principles of fair information practices as articulated by the Organization for Economic Cooperation and Development. *See Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, ORG. FOR ECON. CO-OPERATION AND DEV. (2013), http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.
[141] CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 178 (Cambridge University Press, 2016).

Further, as data sharing and processing drives more and more of society's most essential functions, individual choice about the collection, processing, and secondary uses of data has become more circumscribed. Use of data for socially valuable purposes, e.g., law enforcement, locating lost children, tracking deadbeat parents, medical research, fraud detection, and network security argue against restricting collection and use of certain kinds of data on the basis of choice.

In the emerging data eco-system, characterized by sensor-rich environments, complex vendor relationships and analytic processing of big data, the ability of individuals to consent to any particular instance of data collection or use may be vastly more limited than it was in the era when data was collected almost exclusively through websites, and where the individual interacted with a single entity, typically the web publisher. Given this diminished role of consent, some commenters question whether notice remains relevant at all.[142]

V. ADDRESSING THE CHALLENGES OF NOTICE

Attempts to address the challenges of informing the individual and the limitations of traditional privacy notices have taken two forms: (1) efforts to improve written privacy notices - both offline notices distributed on paper and online privacy notices and (2) efforts to create alternatives to written notices.

---

[142] Cate, *supra* note 117. Cate argues that a system of data protection based on consumer choice no longer works and that notices provide individuals only with an "illusion of enhanced privacy." He describes the proliferation of notices that are rarely read and little understood by individuals and asserts that they serve as a formality rather than a mechanism that promotes transparency or informs individual choice. He highlights in particular that in many cases, services cannot be offered subject to individual choice because to make choice available would run contrary to other societal interests. Cate proposes an approach that would require notice only where collection of data is not reasonably obvious to the individual. In contrast to Cate's view, we believe that even when not used or acted upon by consumers, traditional notices remain essential to transparency, serving the functions we describe elsewhere in this paper – the basis for enforcement, the support for public awareness and action through the activity of the press and advocacy community, and the opportunity for internal review of data collection, processing and protection practices.

A. *Efforts to Improve Written Privacy Notices*

In 2001, the FTC and the Centre for Information Policy Leadership ("CIPL") undertook projects to develop a standard format for short or layered notices.[143] In 2014, NTIA moderated a multi-stakeholder process to develop transparency guidelines for mobile apps. Both are reviewed below.[144]

Early attempts to design short or layered notices were a response to the provisions of the Gramm-Leach-Bliley Act of 1999[145] ("GLBA"). GLBA requires that financial institutions issue privacy notices to their customers,[146] and specifies the content - but not the format - of the notice. In December 2001, the eight GLB agencies convened a joint public workshop titled "Get Noticed" to examine the challenges of providing effective notice and to identify strategies for improving the readability of notices required by GLBA.[147] Subsequently, the Regulatory Relief Act of 2006[148] directed the GLB agencies jointly to develop a model form that companies could use to issue their GLBA privacy notices. The agencies released a model form in March 2007.[149] The final rule, issued in the Federal

---

[143] *See Centre for Information Policy Leadership*, HUNTON & WILLIAMS LLP, https://www.informationpolicycentre.com/projects_archives/ (last visited Apr. 26, 2016).

[144] *See* Privacy Multistakeholder Process: Mobile Application Transparency, NAT'L. TELECOMM. & INFO. ADMIN. (Nov. 12, 2013), https://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency.

[145] Pub L. 106-102, 113 Stat. 1338, enacted November 12, 1999.

[146] Because of the broad scope of GLBA, eight federal agencies were responsible for developing compliance standards and subsequently enforcing GLBA. They are: Board of Governors of the Federal Reserve, Commodity Futures Trading Commission, Office of the Controller of the Currency, Office of Thrift Supervision, the FDIC, the SEC, and National Credit Union Administration and the FTC.

[147] *See Get Noticed: Effective Financial Privacy Notices*, FED. TRADE COMM'N. (Dec. 4, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/interagency-public-workshop-get-noticed-effective-financial-privacy-notices/glbtranscripts.pdf.

[148] Pub. L. 109-351, October 13, 2006.

[149] *See* Final Model Privacy Form Under the Gramm-Leach-Bliley Act - 16 CFR Part 313, FED. TRADE COMM'N. (Dec. 1, 2009), https://www.ftc.gov/policy/ federal-register-notices/final-model-privacy-form-under-gramm-leach-bliley-act-16-cfr-part.

Register on December 1, 2009,[150] specified the content and format for institutions choosing to adopt the standardized GLBA notice.[151]

Also in 2001, the Centre for Information Policy Leadership at the law firm of Hunton and Williams LLP undertook a project to develop a multi-layered online privacy notice that would complement an organization's existing "long" privacy notice.[152] The goal of the project was to provide a standard, simplified format that would promote better consumer decisions about whether or not to share personal information with a particular organization.[153] The simplified format was expected to communicate effectively with individuals about how an organization collects, uses, shares, and protects personal information; individuals wishing more detail about the organization's practices could also consult the long notice.[154] In November 2004, the EU Article 29 Working Party[155] endorsed the

[150] For a copy of the final rule, *see* FEDERAL REGISTER, FINAL MODEL PRIVACY FORM UNDER THE GRAMM-LEACH-BLILEY ACT; FINAL RULE (2001), https://www.ftc.gov/sites/default/files/documents/federal_register_notices/final-model-privacy-form-under-gramm-leach-bliley-act-16-cfr-part-313/091201gramm-leach.pdf (last visited Mar. 14, 2015).

[151] *See* FED. TRADE COMM'N., PRIVACY MODEL FORM, https://www.ftc.gov/system/files/documents/rules/privacy-consumer-financial-information-financial-privacy-rule/privacymodelform_optout.pdf (last visited April 18, 2016). The model form consists of two pages and is formatted as a table with sections for information collection and use, information sharing, how to opt out of information sharing (if relevant), definitions of affiliates and joint of marketing, and other information the institution wishes to provide.

[152] *Ten Steps to Develop a Multilayered Privacy Notice*, CENTRE FOR INFORMATION POLICY LEADERSHIP (Feb. 2006), *available at* https://www.huntonprivacyblog.com/wp-content/files/2012/07/Centre-10-Steps-to-Multilayered-Privacy-Notice.pdf.

[153] *Id.*

[154] *Id.*

[155] EUROPEAN COMMISSION, ARTICLE 29 WORKING PARTY, http://ec.europa.eu/justice/data-protection/article-29/index_en.htm (last visited Apr. 26, 2016).

concept of a multi-layered notice.[156] At least two organizations currently use the layered notice.[157]

A third effort to improve written notices began in summer 2012 when the NTIA launched a multi-stakeholder process to address how to provide notices for mobile apps.[158] The White House Consumer Privacy Bill of Rights called for the use of a multi-stakeholder process to develop voluntary, enforceable codes of conduct to address privacy questions raised by new technologies and specific data practices; this was the first such process.[159] The multi-stakeholder group agreed to limit the scope of its work to developing a code of conduct for a short form notice for mobile devices.[160] On

---

[156] The EU recommendation called for two layers in addition to the long notice. Layer 1 of the short notice was to include the identity and contact details for the data controller, and the purpose for processing. Layer 1 was to be used when space was very limited. Layer 2 of the condensed notice was to provide six items in less than a page with subheadings: scope, personal information collected, uses and sharing, choices (including any access options), important information, and contact information. The content of the "important information" section, as well as the wording and format of the condensed notice, was left to the organization. *See Opinion 10/2004 on More Harmonised Information Provisions*, ARTICLE 29 DATA PROTECTION WORKING PARTY (Nov. 25, 2004), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_en.pdf.

[157] *See, e.g.*, *Privacy Policy Highlights*, U.S. POSTAL SERVICE (2016), http://about.usps.com/who-we-are/privacy-policy/privacy-policy-highlights.htm; *P&G Privacy Notice*, PROCTER & GAMBLE (2016), http://www.pg.com/privacy/english/privacy_notice.shtml.

[158] *See First Privacy Multistakeholder Meeting*, U.S. DEPT. OF COMMERCE: NAT'L TELECOMM. & INFO. ADMINISTRATION (July 12, 2012), https://www.ntia.doc.gov/other-publication/2012/first-privacy-multistakeholder-meeting-july-12-2012.

[159] *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, THE WHITE HOUSE (Feb. 23, 2012), *available at* https://www.whitehouse.gov/sites/default/files/privacy-final.pdf. For more information about the multi-stakeholder process itself, see *Privacy Multistakeholder Process: Mobile Application Transparency*, U.S. DEPT. OF COMMERCE: NAT'L TELECOMM. & INFO. ADMINISTRATION (Nov. 12, 2013), http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency.

[160] *See Privacy Multistakeholder Meeting: Mobile Application Transparency*, U.S. DEPT. OF COMMERCE: NAT'L TELECOMM. & INFO. ADMINISTRATION (Oct. 16, 2012), https://www.ntia.doc.gov/files/ntia/publications/10162012_agenda_revised.pdf.

July 25, 2013, the Department of Commerce released a draft of the code, which specified the data categories to be included in the notice.[161] It also required adopters to describe the types of data collected, how user-specific data is shared, where an individual can access a long form privacy notice if one exists, and the identity of the entity providing the app. The draft code includes design guidelines for the notice.[162] The multi-stakeholder group has not been active since the draft code was issued in 2013.[163]

The GLB model form was subjected to quantitative consumer testing, which assessed the performance of the final notice.[164] While focus groups were used in the design of the CIPL layered notice, neither the CIPL notice nor the NTIA notice for mobile applications were subject to quantitative performance testing.[165]

Carnegie Mellon researchers tested the mobile applications notice generated by the NTIA process. They found that many users

---

[161] *See Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices*, U.S. DEPT. OF COMMERCE: NAT'L TELECOMM. & INFO. ADMINISTRATION (July 25, 2013), https://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf.

[162] *Id.*

[163] *Privacy Multistakeholder Meeting*, *supra* note 160.

[164] *See* Alan Levy & Manoj Hastak, *Consumer Comprehension of Financial Privacy Notices* (Dec. 15, 2008), *available at* http://www.ftc.gov/privacy/privacyinitiatives/Levy-Hastak-Report.pdf (describing how the GLB model form was tested for consumer comprehension).

[165] Typically, two types of research inform the design of new disclosures. Qualitative research (e.g. focus groups) is used to design initial prototypes. Quantitative research is used to test prototypes to see which performs best in meeting the objectives of the new disclosure. Quantitative testing is important because ad hoc theories about what works best are not always reliable and must be validated against objective criteria. For example, the FTC conducted both qualitative and quantitative research to design the GLB model form. In the quantitative research, the researchers engaged by the FTC tested three alternative notices using a sample of 1032 individuals from five different geographical areas. The testing assessed the alternatives on their ability to help consumers (a) compare across banks based on the banks' information practices, (b) evaluate available "opt-out" choices, and (c) make informed choices across banks. *See id.*; *see also* Alan S. Levy, Sara B. Fein & Raymond E. Schucker, *Performance Characteristics of Seven Nutrition Label Formats*, 15 J. PUB. POL'Y & MARKETING 1, 1–15 (1996).

had limited understanding of the terms used in the NITA notice.[166] In another study, Carnegie Mellon researchers tested traditional privacy notices and layered notices.[167] They found that consumers processed information articulated in layered notices faster than that found in long notices, but that readers of the layered notices came away with a less accurate sense of an organization's data and privacy practices.[168] They also found that people did not choose to continue to read the long notice when they did not find the information they sought in the short notice.[169] This suggests that testing should be an integral part of the design of alternative notices if the alternatives are to be useful.

B. *Alternatives to Traditional Notice*

This section describes three efforts to develop alternatives to traditional privacy notices. The Platform for Privacy Preferences ("P3P") represents the most ambitious attempt to date to use technology to improve online disclosures. The AdChoices "icon" provides a way to provide better visibility for online behavioral advertising. Finally, some organizations have independently begun to develop tools to help inform their users.

1. *The Platform for Privacy Preferences*

P3P is a standard developed by the World Wide Web Consortium ("W3C") through a multi-year process that began in 1997.[170] A final Last Call specification was issued in September

---

[166] *See* Rebecca Balebako, Richard Shay & Lorrie Faith Cranor, *Is Your Inseam a Biometric? A Case Study on the Role of Usability Studies in Developing Public Policy*, (Feb. 2014), *available at* http://lorrie.cranor.org/pubs/usec14-inseam.pdf.

[167] *See generally* Alecia M. McDonald et. al., *A Comparative Study of Online Privacy Policies and Formats*, *in* PRIVACY ENHANCING TECHNOLOGIES: 9TH INTERNATIONAL SYMPOSIUM, PETS 2009, SEATTLE, WA, USA, AUGUST 5–7, 2009. PROCEEDINGS 37–55 (Ian Goldberg & Mikhail J. Atallah eds., 2009).

[168] *See id.*

[169] *See id.*

[170] LORRIE FAITH CRANOR, WEB PRIVACY WITH P3P 46 (O'Reilly & Associates, eds., 2002) (Chapter 4 describes the history of P3P).

2001.[171] Adoption of P3P was voluntary.[172] P3P provides a syntax with which websites can code the privacy practices described in their traditional privacy notice.[173] Using a standard XML format, the notice can be retrieved automatically and interpreted easily by user agents such as browsers or other applications.[174] These user agents allow online users to learn about the information practices of the sites they visit without needing to read the written privacy notice.[175]

Many perceived P3P as too difficult and complicated to use, and it never was widely implemented.[176] Microsoft was the only major browser to support P3P; Internet Explorer 6 ("IE6") used P3P to implement cookie filtering.[177] Using a slider, individuals set their privacy preferences in IE6 along a spectrum ranging from high to low. If IE6 found a P3P policy, it evaluated the website's privacy practices as described in its P3P policy and decided, based on the set preference, which cookies were acceptable. IE6 could, for example, accept a cookie, accept a cookie but downgrade it to a session cookie, or suppress or reject a cookie entirely.

---

[171] *See generally id.* For a copy of the most recent P3P specification and other documents related to the development of P3P, see Lorie Cranor & Rigo Wenning, *Platform for Privacy Preferences (P3P) Project: Enabling smarter Privacy Tools for the Web*, W3: PLATFORM FOR PRIVACY PREFERENCES INITIATIVE, *available at* http://www.w3.org/P3P/ (last updated Nov. 20, 2007).

[172] *See* Cranor, *supra* note 170, at 55.

[173] *See* Cranor & Wenning, *supra* note 171.

[174] *Id.*

[175] *Id.*

[176] An internal Citibank white paper argued that implementing P3P could also limit a company in terms of the commerce, cross-selling, and marketing information collected online. The authors state that the paper it is simply a statement of the opinion of two Citibank employees and does not represent the official position of Citibank. *See generally* Kenneth Lee and Gabriel Speyer, *White paper: Platform for Privacy Preferences (P3P) & Citibank*, CITIBANK ADVANCED DEV. GRP. (Oct. 22, 1998), *available at* http://www.w3.org/P3P/Lee_Speyer.html.

[177] *Platform for Privacy Preferences (P3P) (Windows CE 5.0)* contains a description of Microsoft's implementation of P3P for cookie filtering. *Platform for Privacy Preferences (P3P) (Windows CE 5.0)*, MICROSOFT https://msdn.microsoft.com/en-us/library/ms905230.aspx (last visited Apr. 14, 2016).

Two standalone applications also implemented P3P: Privacy Bird and Privacy Finder.[178] Privacy Bird automatically searches for P3P privacy policies at every website a user visits.[179] The Privacy Bird software asks the user to describe their privacy concerns; it then communicates to the user whether a visited site's policies match their stated privacy preferences.[180] The software displays a green bird icon at websites that match, and a red bird icon at sites that do not.[181] If the software cannot find or fetch a P3P policy from the visited website, the Privacy Bird displays a yellow icon.[182]

Privacy Finder is a privacy-enhanced search engine that delivers search results based on websites' computer-readable privacy policies.[183] A privacy meter with green boxes indicates how closely the website's privacy policy matches a list of preset privacy preferences. If no privacy meter is displayed, it means that a valid P3P policy could not be located for a given website.[184]

2. *AdChoices Icon*

The research projects described above were early attempts to better inform the individual in an environment where website content was provided by a single source, typically the site owner. Today, a web page is likely to be supported by many vendors and comprise content from many different sources, each of which may follow different information practices. In February 2009, the FTC issued a staff report articulating self-regulatory principles that applied to online advertising where ads were targeted based on

---

[178] PRIVACY BIRD, http://www.privacybird.org/ (last visited Apr. 14, 2016); PRIVACY FINDER, http://www.privacyfinder.org/ (last visited Apr. 14, 2016).

[179] Lorrie Faith Cranor, Praveen Guduru & Manjula Arjula, *User Interfaces for Privacy Agents*, 13 ACM TRANSACTIONS ON COMPUTER-HUMAN INTERACTION 135, 135–78 (2006).

[180] *Id*. at 136–39.

[181] *Id.* at 148, 155.

[182] *Id.* at 155.

[183] PRIVACY FINDER, *supra* note 178.

[184] Privacy Bird was originally developed by AT&T Corp. *See* PRIVACY BIRD, http://www.privacybird.org/ (last visited Apr. 20, 2016). Both applications are currently maintained by the CyLab Usable Privacy and Security Lab at Carnegie Mellon University. *See* CYLAB, http://cups.cs.cmu.edu (last visited Apr. 14, 2016).

tracking individuals over time. [185] The principles excluded contextual advertising where an ad was based on a single visit to a web page or a single search request and "first party" advertising where data was not shared with third parties.

In response to the FTC report, the online advertising industry formed the Digital Advertising Alliance ("DAA") – an alliance to promote implementation of the FTC principles and to create a clickable icon, which would appear on online ads.[186] The AdChoices Icon represents an attempt to provide greater awareness in an environment where networks of online advertisers track browsing behavior across websites.[187]

Stakeholders hoped that over time, the icon would become as recognizable to consumers as the recycling symbol.[188] Currently, the program applies to online behavioral advertising for both the desktop and mobile environments and includes a webpage that individuals can visit to opt out of receiving advertising that has been targeted based on their browsing behavior.[189]

---

[185] FEDERAL TRADE COMMISSION, *Self-Regulatory Principles For Online Behavioral Advertising* (2009), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf.

[186] DIGITAL ADVERTISING ALLIANCE (DAA) SELF-REGULATORY PROGRAM, http://www.aboutads.info/ (last visited April 14, 2016). Preliminary research on the feasibility of developing an icon for online behavioral advertising was conducted by the Future of Privacy Forum. *See, e.g., Online Behavioral Advertising "Icon" Study,* FUTURE OF PRIVACY FORUM, http://www.futureofprivacy.org/2010/02/15/online-behavioral-advertising-icon-study/ (last visited Apr. 14, 2016).

[187] The desktop version was launched in 2011 and the mobile version was launched in 2015. For an example of the icon, visit http://www.yahoo.com. When a user clicks on the icon, a notice "Why this Ad?" is displayed. *Why this Ad*?, YAHOO, https://info.yahoo.com/privacy/us/yahoo/relevantads.html (last visited Apr. 14, 2016).

[188] Stephanie Clifford, *A Little 'I' to Teach about Online Privacy*, N.Y. TIMES (Jan. 26, 2010) http://www.nytimes.com/2010/01/27/business/media/27adco.html?&_r=0.

[189] The AboutAds consumer choice page is available online. DIGITAL ADVERTISING ALLIANCE CONSUMER CHOICE PAGE, http://www.aboutads.info/choices/ (last visited April 14, 2016).

The DAA program appears to have been widely adopted; however researchers found instances of non-compliance.[190] Further, the effectiveness of the program has not been extensively assessed, and there is no indication that usability testing was conducted as part of the AdChoices design process.[191] Researchers at Carnegie Mellon University independently assessed Internet users' perceptions of disclosures about online behavioral advertising.[192] Drawing on prior research, they tested icons, taglines, and landing pages and found that all fell short in terms of notifying study participants about online behavioral advertising and clearly informing them about their choices.[193]

3. *Company-generated Tools*

Organizations have taken independent steps to create tools by which consumers can view and control their personal information. For example, the Google privacy policy includes a section on "Transparency and Choice," which describes tools generated by Google that allow users to access their account history, view and edit their preferences about the Google ads they receive, and control who people share their information with through their Google Account.[194] Acxiom, a large data broker, offers "About the Data," a tool to help consumers learn about the data Acxiom has collected about them.[195]

---

[190] Saranga Komanduri et. al., *AdChoices? Compliance with Online Behavioral Advertising Notice and Choice Requirements,* CARNEGIE MELLON CYLAB, (2011), https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11005.pdf.

[191] Kate Kaye, *Study: Consumers Don't Know What AdChoices Privacy Icon Is*, ADVERTISING AGE (Jan. 29, 2014) http://adage.com/article/privacy-and-regulation/study-consumers-adchoices-privacy-icon/291374/.

[192] *See* Pedro Giovanni Leon et al., *What Do Online Behavioral Advertising Disclosure Communicate to Users?,* CARNEGIE MELLON CYLAB, (2012), https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12008.pdf.

[193] *Id.* Specific findings included 1) notices are not noticed, 2) "AdChoices" is not an effective tagline, 3) users are afraid to click, 4) users are confused about the meaning of opt out, and 5) user education is needed.

[194] *Welcome to Google Privacy Policy*, GOOGLE PRIVACY AND TERMS, https://www.google.com/intl/en/policies/privacy/?fg=1 (last visited April 14, 2016).

[195] ABOUTTHEDATA.COM, https://www.aboutthedata.com/ (last visited April 14, 2016).

C. *Lessons Learned and Unresolved Challenges*

While it is widely acknowledged that most traditional privacy notices are too long, lack uniformity, and are difficult to comprehend, notice is still viewed as the primary means whereby organizations make the public aware of their data practices.[196] The efforts to improve notices described above yielded mixed results. For example, only two of these efforts, the AdChoices icon and the GLB model form, were widely adopted.[197] Nonetheless, these efforts, particularly the GLB model form, provide useful insights about what enhances or inhibits the ability to provide more effective notices.

1. *Lessons of the GLB Model Form*

Legislation and implementing rules offer organizations incentives to adopt the GLB model form. GLBA requires that covered organizations disseminate privacy notices that meet criteria established in the law's disclosure requirements and the privacy rule implementing the law.[198] While the use of the model privacy form is voluntary, organizations that do so benefit from certainty that they satisfy these criteria. Moreover, the standardized format and content of the model form creates efficiencies for consumers by better

---

[196] *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS, FTC Report (Mar. 2012) https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers; THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY, (Feb. 2012) https://www.whitehouse.gov/sites/default/files/privacy-final.pdf; THE WHITE HOUSE, ADMINISTRATION DISCUSSION DRAFT: CONSUMER PRIVACY BILL OF RIGHTS ACT (Feb. 27, 2015) https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

[197] *See, e.g*, Lorrie Faith Cranor et al., *Are They Actually Any Different? Comparing Thousands of Financial Institutions' Privacy Policies*, WEIS, (2013) http://weis2013.econinfosec.org/papers/CranorWEIS2013.pdf; *Digital Advertising Alliance (DAA) Announces "Your AdChoices" Consumer Education Campaign*, 4A's (Jan. 20, 2012) http://www.aaaa.org/news/press/Pages/012012_daa_adchoices.aspx.

[198] *See* Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106–102, 113 Stat. 1338 (1999).

enabling choice about information use (to the extent available under the law) and allowing consumers to compare choices across financial institutions. Finally, the notice as articulated in the model form continues to provide a basis for FTC regulation.

Moreover, because the GLBA implementing rule does not provide the assurances of a safe harbor,[199] some companies perceive that posting a notice in a way other than that prescribed by the model form increases their risk of exposure to an FTC enforcement action. The model's clear rules for content and format arguably lessen that exposure. Finally, rigorous consumer testing increased the probability that the form would be effective.

In 2013, researchers at Carnegie Mellon University assessed over 3,000 GLBA policies based on data collected using an automated web crawler.[200] The study highlighted the challenges that organizations using the form face when disclosing what types of information they collect.[201] Restrictions on what language may be used to describe how information is collected also posed problems.[202] While standardized language facilitated transparency and comparisons across institutions, the researchers found some of the terms used were redundant or ambiguous.[203] However, when researchers compared privacy practices across similar institutions, they found differences in their privacy practices, suggesting that making a company's data practices more conspicuous could empower consumers' decision-making.[204] The standardized table format used in the GLB model form thus appears to hold promise for a better way to deliver necessary information about data and privacy practices to individuals.

---

[199] The implementing rule originally provided safe harbor protection for organizations using the model form. The final rule eliminated the safe harbor.

[200] Lorrie Faith Cranor et. al., *Are They Actually Any Different? Comparing Thousands of Financial Institutions' Privacy Policies*, WEIS (2013) http://weis2013.econinfosec.org/papers/CranorWEIS2013.pdf.

[201] *Id.*

[202] *Id.*

[203] *Id.*

[204] *Id.*

2. *Promise and Challenges of a "Nutrition Label" Format for Privacy Notices*

The CyLab Usable Privacy and Security Lab ("CUPS Lab")[205] at Carnegie Mellon University researches, develops, and tests alternatives to traditional privacy notices.[206] In a recent study, researchers tested four alternative forms of privacy notices, comparing them to natural language, full-text policies.[207] They found that of the five options, the standardized table yielded the best results.[208] They concluded that the success of this approach resulted from both the table format and the standardized language.[209] Both the format and the language improved accuracy, the ability to locate information, the speed with which an individual could locate information, and the individual's experience in reading notices.[210] These findings argued for developing a format for short privacy notices similar to nutritional labels.[211]

Despite their promise, developing a privacy notice modeled after food nutrition labels poses significant challenges. The nutrition content of food can be analyzed and quantified, and the numerical values posted on the labels can be objectively tested and verified by a third party. The result is a set of reliable numbers the consumer can compare easily. A consumer interested in purchasing, for example, a loaf of bread can quickly compare several brands based

---

[205] *CyLab Usable Privacy and Security Laboratory*, CARNEGIE MELLON CYLAB., http://cups.cs.cmu.edu/.

[206] *See id.*

[207] Patrick Gage Kelley et al., *Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach*, CARNEGIE MELLON CYLAB. (Jan. 12, 2010), https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab09014.pdf. For further CUPS research on this topic, see *Privacy Nutrition Labels*, CARNEGIE MELLON CYLAB, http://cups.cs.cmu.edu/privacyLabel/.

[208] Kelley et al., *supra* note 207. The four alternatives evaluated in addition to a natural language notice include: (1) the standardized table, a variant of the nutrition label; (2) the standardized short table (an abbreviated version of the standardized table, minus categories of data the organization does not collect); (3) the standardized short text, which translates the standardized short form table into English statements; and (4) the layered text, an approach adapted from the CIPL layered notice described above. *Id.*

[209] *Id.*

[210] *Id.*

[211] *Id.*

on calories per serving and cholesterol, vitamin, fat, and fiber content. In the United States, they can also use the label to compare products against numerically expressed government nutrition recommendations. These values are unlikely to change quickly, and if they do, their accuracy can be readily tested in a lab. Creating an accurate nutritional label involves simply filling in the boxes on the form. As a result, the nutrition label has been at least moderately effective at promoting consumer choice, creating a basis for regulation, and providing a source of information for consumer advocates and the media.[212]

While the effectiveness of both nutrition labels and privacy notices depends on consumers' ability to understand the information disclosed in the notice, privacy notices pose challenges not faced by entities adopting the nutrition label format. First, data practices and protections do not lend themselves to quantified expression. For example, while nutrition labels are based on "percent of Recommended Daily Allowance," there is no comparable standard for information practices given the variety of business models and industries. Moreover, for food, the product is fixed at purchase and the individual controls its use after purchase. For information, the individual currently has little comparable control as the company controls future uses of the data. All future uses are unlikely to be known at the time of disclosure and may be subject to change. This, and the fact that personal information touches many entities within an organization, challenges attempts to accurately describe the organization's data practices.

C. *Looking Ahead*

In its 2012 report, FTC proposed that to promote better comprehension and comparison of privacy practices, notices should be "clearer, shorter, and more standardized."[213] It recognized that a rigid format for use across all sectors is not appropriate, and that it would be necessary to accommodate differences in business models

---

[212] *See* ARCHON FUNG, MARY GRAHAM & DAVID WEIL, FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY (2007) at 84–85. *See also* SUSAN G. HADDEN, READ THE LABEL (1986) at 145-151.

[213] *Protecting Consumer Privacy in an Era of Rapid Change*, *supra* note 41, at 61.

across industry sectors.[214] It stated that to allow individuals to compare privacy practices across companies and encourage companies to compete on privacy, privacy notices should contain some standardized elements such as terminology and format.[215] How this would work in practice remains an open question. Further, the time required by efforts aimed at improving notices described previously suggest that creating new forms of effective notice is a long-term project and that these efforts are unlikely to be successful unless consumer testing is part of the design process. New technologies such as mobile applications and the "Internet of Things" pose further challenges to notice.

VI. EMERGING TECHNOLOGICAL CHALLENGES

The prior sections focused primarily on issues related to providing notice in traditional computing on desktops and laptops. This Section reviews the challenges raised by new technologies and data ecosystems, which may provide little opportunity to interface with the consumer. This limited opportunity for interaction with the consumer makes providing notice difficult and sometimes impossible.

The broad implementation of notices starting in the 1990's began in a data environment that centered primarily on the collection of data via websites.[216] Privacy protections were based on a theory of control – individuals who were made aware of data practices and protection measures and provided the opportunity to choose based on assertions in a posted privacy policy could make decisions about the collection and use and sharing of data pertaining to them.[217]

Increasingly, individuals will navigate spaces throughout which data is collected, shared, and processed silently and ubiquitously—and for a wide variety of purposes. Sensors will be embedded in rooms and across spaces to facilitate such functions as climate control, physical security, employee and equipment tracking, and

[214] *Id.* at 62.
[215] *Id.* at 62.
[216] *See* Hoofnagle, *supra* note 5, at 147.
[217] *Id.* at 148.

energy distribution.[218] Sensors will also be deployed across geographically distributed systems to manage, for example, resource delivery, supply chain management, and traffic control.[219] It is not clear how individuals could be provided real time notice in such environments, whether and to what extent individuals should be provided with an opportunity to consent, and if so, how it could be granted or withheld.

The advent of big data and new technologies such as mobile applications the Internet of Things, and sensor-rich environments pose new privacy concerns and new challenges for addressing these concerns. Privacy concerns arise when information practices conflict with an individual's reasonable expectations about how their information should be used.[220] The physical characteristics of these new technologies may make it difficult to make these new uses visible to the individual, and these issues are exacerbated in a global environment with varying literacy issues.

A. *Big Data Analytics*

Using analytics to process what is commonly referred to as "big data"—very large data sets, rapidly gathered and compiled from diverse sources—raises its own challenges. Analytics are often applied to data originally collected for another purpose and combined with data from other sources.[221] The individual may be aware of the initial collection and uses of data, but not of the

---

[218] *See generally* Michael Chui, Markus Löffler, & Roger Roberts, *The Internet of Things*, MCKINSEY QUARTERLY (Mar. 2010), http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things.

[219] *Id.*

[220] For example, in its 2012 Privacy Report, the FTC identified data practices that are consistent with the context of a particular transaction or with the organization's relationship with a consumer as being generally consistent with consumers' reasonable expectations. FED. TRADE COMM'N, *Protecting Consumer Privacy.*

[221] Brian Hengesbaugh & Amy de La Lama, *When the Big Data Surge Crashes Against the Big Privacy Rocks: The Conflict Between the Commercial Value of Information and Increasing Privacy Regulation*, THE PRIVACY ADVISOR (Oct. 21 2013), https://iapp.org/news/a/when-the-big-data-surge-crashes-against-the-big-privacy-rocks-the-conflict.

subsequent analytic processing.[222] Further, the information may also be shared with and used by third parties of whom the individual is not aware.[223] There are also calls for increased transparency around algorithms when these are applied using analytics to make automated decisions.[224]

Perhaps the aspect of big data analytics that poses the greatest challenge is the nature of the processing itself. Researchers do not approach large data sets in search of the answer to a question; rather, they explore the data for what it may reveal.[225] What results is the use of data in ways that could not have been anticipated and therefore, would not have been included in a privacy notice.[226]

Providing effective notice later, when these new uses actually occur, is not practical—data may have been collected long before its use and amassed from many different sources, and it may no longer be possible to locate and contact what could be thousands of individuals whose data was used. Further, when big data analytics are used to create personal information from non-personal information after collection, this poses additional challenges.[227] Absent new restrictions on data collection and use, proposals for addressing some of the privacy and other fairness challenges of secondary use of big data include companies' implementation of privacy impact assessments, privacy-by-design processes,

---

[222] *Id.*

[223] *Id.*

[224] *See* Danielle Keats Citron & Frank A. Pasquale, *The Scored Society: Due Process for Automated Protections*, 89 WASH. L. REV. 1, 5 (2014).

[225] Fred Cate and Victor Mayer-Schoenberger, *Notice and Consent in a World of Big Data*, MICROSOFT, at 3 (Nov. 2012), *available at* https://www.microsoft.com/en-us/download/details.aspx?id=35596.

[226] *Id.*

[227] *See* Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 96 (2014), http://bclawreview.org/files/2014/01/03_crawford_schultz.pdf. Crawford and Schultz cite the familiar Target example where analytics were used to infer a customer was pregnant from her purchases, thereby creating new personal information. *Id.* at 94–95.

accountability programs, and ethical reviews to avoid undertaking legal but questionable data uses.[228]

B. *Mobile Application*

Mobile applications also pose challenges to transparency that do not exist with applications that run on a traditional PC. First, the small screens on mobile devices provide limited space to display a traditional privacy notice. The NTIA multi-stakeholder process described previously [229] attempted to address this challenge by proposing a short form notice that only addressed privacy issues related to information considered sensitive.[230] Second, applications can access information on the user's phone such as contacts, photos, or actual location, even when that information is not necessary for the application to function or may be generated by another function on the device, such as the use of an individual's location by a flashlight application.[231] Users may be unaware of these information practices if they are not disclosed to the user or potential user of the application. [232] Without awareness, it may be impossible for individuals to make informed choices about using a particular application. [233] Finally, the constraints of the application environment raise questions about how and when notice should be

---

[228] *See* Ryan Calo, *Consumer Subject Review Boards: A Thought Experiment* (Sep. 2013), *in* BIG DATA & PRIVACY: MAKING ENDS MEET DIGEST, http://www.futureofprivacy.org/big-data-privacy-workshop-paper-collection. The White House Discussion Draft: Consumer Privacy Bill of Rights of February 27, 2015 also calls for privacy review boards. Some have suggested that companies could provide transparency if they made the results of their internal privacy reviews public. However, making such reviews public could result in sanitized reports that don't serve their intended purpose.

[229] *Privacy Multistakeholder Meeting*, *supra* note 160.

[230] *Id.*

[231] *See, e.g.*, *Android Flashlight App Developer Settles FTC Charges It Deceived Consumers*, FED. TRADE COMM'N (Dec. 5, 2013), https://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived.

[232] *Id.*

[233] *See, e.g.*, Rebecca Balebako et. al., *"Little Brothers Watching You:" Raising Awareness of Data Leaks on Smartphones*, SYMPOSIUM ON USABLE PRIVACY AND SECURITY (SOUPS) (July 2013) https://cups.cs.cmu.edu/soups/2013/proceedings/a12_Balebako.pdf.

provided, where the notice should be stored, and when it should be displayed.

C. *Internet of Things and Sensors*

The Internet of Things (IoT) refers to the ability of everyday objects to connect to the Internet and to send and receive data.[234] This can include automobiles, home appliances, or wearable fitness devices among other "smart devices."[235] Mobile devices with WI-FI or Bluetooth turned on enable sensors in physical places to receive signals from nearby devices. For example, sensors in retail stores can use a unique identifier broadcast by the mobile device to track how customers move through the store; often a third-party analytics firm may do this tracking without the customer's knowledge.[236] As is the case with mobile applications, individuals are unlikely to be aware of the information capabilities of these devices or the fact their device is being tracked, highlighting the need for awareness at the time the individual makes a purchase decision about a device or chooses to enable a particular feature. Further, because many of these devices may not contain a screen, let alone a small screen, they pose even greater transparency challenges than mobile applications and big data analytics. As a result, new and creative approaches to disclosure are needed including decoupling the notice from the actual device.[237] For example, in its 2015 Staff Report on the Internet of Things, the FTC suggested some alternatives to traditional web privacy notices for the IoT such as QR codes, choices at the point of sale, or choices during setup of the device.[238]

---

[234] Crawford & Schultz, *supra* note 227, at 5.

[235] *Id.* at 7–9.

[236] *See* Ashkan Soltani, *Privacy Trade-offs in Retail Tracking,* FEDERAL TRADE COMM'N (Apr. 30, 2015), https://www.ftc.gov/news-events/blogs/techftc/2015/04/privacy-trade-offs-retail-tracking.

[237] *See, e.g.*, Florian Schaub et. al., *A Design Space for Effective Privacy Notices*, *Usable Privacy and Security (SOUPS 2015)*, Carnegie Mellon University (2015), *available at* http://ra.adm.cs.cmu.edu/anon/isr2015/CMU-ISR-15-105.pdf.

[238] *See Internet of Things: Privacy & Security in a Connected World*, FEDERAL TRADE COMM'N (January 2015) https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (last visited March 21, 2015).

VIII. RECOMMENDATIONS

Until recently, the term "organizational transparency" primarily was used as a rhetorical device or as an *ad hoc* construct, the meaning of which varied by field of study.[239] For example, the meaning of transparency differed depending upon whether one referred to, for example, financial markets, organizational governance or trust in online commerce.[240] In their recent review of the literature on transparency, Schnackenberg and Tomlinson define transparency as a *perception of the quality of information received from a sender w*hich includes three dimensions of information quality: the *degree* of information disclosure (including the perception that relevant information is received in a timely fashion), the *clarity* of the disclosure, and the *accuracy* of the disclosure.[241]

Schnackenberg and Tomlinson further argue that transparency is a mechanism to increase trust in organizations, because information quality can enhance perceptions that an organization is trustworthy.[242] Other research has shown that consumers are generally willing to disclose their personal information if the benefits of disclosure exceed the perceived risks.[243] Trust affects consumers' willingness to assume the risks of disclosing personal information; it is important over the life of a customer relationship where consumers must rely on "strangers" to protect their interests due to information asymmetries.[244] Organizations can help create

---

[239] A.K. Schnackenberg & E.C. Tomlinson, *Organizational Transparency: A New Perspective on Managing Trust in Organization-Stakeholder Relationships*, J. OF MGMT. (2014).

[240] *Id.* While the authors did not specifically address privacy notices, the conclusions appear to be relevant to privacy.

[241] *Id.* Given this definition, the research on traditional privacy notices and alternative notices, most notably, that done at Carnegie Mellon University, provide support for our assertion a notice model does not support transparency.

[242] *Id.*; *see* Kirsten Martin, *Privacy Notices as Tabula Rasa: An Empirical Investigation into how Complying with a Privacy Notice is Related to Meeting Privacy Expectations Online*, J. OF PUB. POL'Y AND MKTG. (2015).

[243] *See* M. Culnan and P. Armstrong, *Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation*, 10 ORG. SCI. 104, 104–15 (1999).

[244] *Id.*

trust if they provide assurances that they will not behave opportunistically. Therefore, good quality disclosures can signal to individuals that a company can be trusted with their personal information, providing the company abides by the practices disclosed in the notice.[245]

By understanding the dimensions of transparency, organizations can better improve the quality of their disclosures to stakeholders, meet regulatory and self-regulatory requirements, and contribute to fair data use. This work informs this Article's recommendations for moving beyond the current reliance on notices to a more robust approach to transparency.[246]

Notice as a general concept will continue to be the starting point for transparency. However, given the growing complexity of the emerging data eco-system, the ubiquity of data collection, and the incidence of real-time processing, a single notice can no longer reasonably be expected to serve the many purposes of supporting individual choice, regulation, and public awareness and education. This Article proposes instead that to achieve an environment of transparency, organizations should deploy, and policy makers should support a variety of methods for reaching all stakeholders.[247] In particular, the perceived quality of consumer disclosures should be improved along the three dimensions of transparency: degree of disclosure, clarity, and accuracy. We now turn to our specific

---

[245] *See* M. Culnan & R. Bies, *Consumer Privacy: Balancing Economic and Justice Considerations*, 59 J. OF SOC. ISSUES 323, 323–42 (2003).

[246] *See Privacy Online: A Report to Congress*, FEDERAL TRADE COMMISSION (1998); *see, e.g.*, Fred H. Cate, *The Failure of Fair Information Practice Principles* in CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY, (Jane K. Winn ed., 2006). Cate argues that while transparency (or openness) is explicit in the original HEW Fair Information Principles, the OECD Guidelines and the EU Directive, it is not mentioned in the FTC's 1998 articulation of the FIPS where the broader goal of transparency was reduced to a set of procedural rules against which compliance could be measured and where notice serves as "the most fundamental principle." *Id.*

[247] *See* Michael S. Wogalter et al., WARNINGS AND RISK COMMUNICATION, (Taylor and Francis eds., 1999). Research on risk communication argues for a system of warnings consisting of multiple disclosures designed for multiple audiences. Further, the design of warnings should be viewed as an integral part of the overall system design process.

recommendations for improving transparency including the need for business buy-in and regulatory guidance.

A. *Organizations should continue to provide comprehensive, technical notices to facilitate the roles of regulators and advocates.*

Long notices often read like legal documents and include comprehensive technical descriptions of data collection and use, technologies, and complex networks of business partners and vendors. Such notices often are of little use to individuals, who are unwilling and uninterested in investing the time to read them, and are often ill equipped to understand them. In spite of these familiar shortcomings, these notices are still important and necessary to transparency, as they provide a basis for oversight by regulators who can use them to compare assertions about data protection against actual practices. Comprehensive privacy notices also provide knowledgeable experts and privacy advocates with the information necessary to raise important societal questions about surveillance, appropriate and inappropriate uses of data and the evolution of technology. These notices ensure that the advances in technology and data processing benefit from the oversight that can support consumer protection and keep organizations accountable. However, these notices lack the clarity and accuracy needed by individuals and therefore, fail to provide transparency to an important group of stakeholders.[248]

[248] *Id.* Research has shown notice to play a role in building consumer trust and promoting disclosure. For example, comprehension of online notices was found to be positively related to both reading notices and trusting the notice. Conversely, notices perceived by consumers to be obfuscated or excessively legalistic contribute to skepticism. Trust in online notices has also been positively related to lower levels of privacy concern.; *see also Results of Consumer Data Privacy Survey Reveal Critical Need for All Digital Citizens to Participate in Data Privacy Day*, PR NEWSWIRE (Jan. 28, 2015) http://www.prnewswire.com/news-releases/results-of-consumer-data-privacy-survey-reveal-critical-need-for-all-digital-citizens-to-participate-in-data-privacy-day-300026888.html. A 2014 survey by the National Cyber Security Alliance found that 83% of respondents cited using only trusted websites and companies as a strategy to protect their privacy; this was the second most used strategy after having a strong password.

B. *Organizations should also develop alternative forms of disclosure for individuals, providing them with relevant information in clear, understandable language, in a format that promotes comprehension and that is delivered at the appropriate time.*

Comprehensive notices do not support transparency for individuals because they are perceived as being unclear, and they may not be available at the appropriate time. Further, they may be too general to provide an accurate picture of the organization's information practices.[249] In a recent study, Martin argues that the "designed obscurity" of privacy notices achieved through the use of ambiguous language sends a false signal to individuals and may undercut the ability of notices to support market decisions based on differences in information practices. [250] Therefore, alternative disclosures are needed that are brief, succinct, and accurate yet include the relevant information that promotes individual understanding about data collection and use. In some environments, these disclosures will simply communicate pertinent information. In others, the disclosure should be designed and delivered at a time to facilitate rational choice when choice is available, such as whether or not to allow a mobile application to make use of the individual's exact location.

To create these disclosures, organizations will need to need understand how to communicate effectively with their target audiences. Consumer disclosures should include only the information that is most relevant and meaningful to a specific audience at a particular time. They should also disclose appropriate information about how data is used at a particular point in time. In

---

[249] *See* Joel R. Reidenberg et al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, (TPRC, 42nd Research Conference on Communication, Information, and Internet Policy 2014). For example, Reidenberg and his colleagues argue that broad or vague statements about collection practices are the functional equivalent of an absence of notice. Incomplete notice results when information collection occurs outside the scope of the firm's notice.

[250] *See* Kirsten Martin, *Privacy Notices as Tabula Rasa: An Empirical Investigation into how Complying with a Privacy Notice is Related to Meeting Privacy Expectations Online*, 34 J. OF PUB. POL. AND MKTG. 210, 210 (2015).

some cases, they should alert the individual about the specific data practice, particularly if the practice is unexpected as is the case with newer technologies described previously.[251] Firms will need to understand what information individuals need and develop methods for communicating this information quickly and clearly. In particular, it is necessary to understand how to effectively communicate information in specific situations, and how people process this information.[252] Solutions can include layered text notices and alternatives to text. One such example are "visceral notices," which include auditory or visual prompts embedded in a particular technology and activated at the appropriate moment while the individual is using the product to alert the individual that the product is collecting personal information.[253] Existing research on labels and warnings may also prove instructive here.[254]

It will also be important to develop ways to make the notice clearly available and easily located at the time of decision-making or "just-in-time." This is particularly true for new technologies with small screens or no screens at all, or for situations where multiple parties are involved in collecting or delivering information. For example, many mobile applications now offer notice the first time the application attempts to collect sensitive information, or to use information in a way that is unexpected. For some technologies, an "it takes a village" approach may be appropriate where responsibility for delivering notice is shared among business partners. For example, for mobile applications, initial notice may be provided by an application store so the user can review an application's information practice before they decide to download

---

[251] Florian Schaub et. al., *A Design Space for Effective Privacy Notices*, Symposium, *Usable Privacy and Security (SOUPS 2015)*, Carnegie Mellon University (2015) http://ra.adm.cs.cmu.edu/anon/isr2015/CMU-ISR-15-105.pdf.

[252] *See, e.g.*, Michael S. Wogalter et al., *supra* note 247.

[253] *See generally* Ryan Calo, *Against Notice Skepticism in Privacy (And Elsewhere)*, 87 NOTRE DAME L. REV. 1027 (2012).

[254] For more information on label and warning research, *see generally* George R. Milne & Mary J. Culnan, *Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices*, 18 JOURNAL OF INTERACTIVE MARKETING 2, 15–29 (2004). *See also Privacy Nutrition Labels,* CYLAB USABLE PRIVACY AND SECURITY LABORATORY (last visited Apr. 5, 2016) https://cups.cs.cmu.edu/privacyLabel/.

it. This approach may also be appropriate for behavioral advertising, data brokers, and the collection of information from sensors operated by third parties where the individual is unaware of the firm collecting their information and does not have a relationship with it.[255] The Internet of Things, in particular, will require creative approaches to notice, particularly where devices may not have a screen and where collection of information is unexpected or not obvious or visible.[256]

C. *Notices should be developed as part of privacy-by-design*

Because privacy notices have served an integral role in regulation (see Section II above), legal counsel has usually been tasked with drafting notices independent of the development of the applications described in the notice. Based on an inventory of the kind and method of data collection, the nature of the data use, and the security measures implemented, lawyers have written notices that are comprehensive and designed to avoid liability. Importantly, because notices are often viewed as a vehicle for compliance, they largely have been drafted at the end of the system development process, after decisions about data practices have been implemented. The drafting and posting of the notice has often been one of the final steps an organization takes before rolling out a technology or data driven service. In some cases, organizations have side-stepped the review of their data practices as part of their drafting process and have looked instead to boiler-plate notice language as their starting point.[257] Given this disconnect, the rapid development cycles in

[255] An example is where retail or other locations contract with an analytics firm, who use sensors to perform mobile tracking for the retailer. A retailer who has contracted with the analytics firm and who has direct contact with the consumer bears major responsibility for notifying their customers about the tracking.

[256] The FTC called for innovation in notices in its 2014 report on the Internet of Things.

[257] When privacy notices are viewed as a compliance responsibility, overseen by the legal department, the rapid pace of system development makes it difficult to coordinate the privacy notice with new features of the application. Representatives of tech companies made this point during the discussion of this Article at the 2015 Privacy Law Scholars Conference (PLSC). PLSC operates under Chatham House Rules so comments cannot be attributed to a specific individual.

many firms increases the likelihood that their privacy notice will not reflect the details of current data practices.

Over the past several years, some companies have adopted an approach to privacy governance that involves looking at and implementing privacy considerations throughout the entire design and development process.[258] Developers, legal staff, and compliance officers at various points in the development cycle question the collection, use, sharing, and protection for data, asking question like: What data are we collecting? Is all of this data necessary? What measures are we employing to secure the data? With whom do we plan to share it, and why? Can we offer the individual the opportunity to consent or exercise choice about the use of his or her data? If so, how can we build that into the user experience?

While privacy-by-design increasingly is considered fundamental to responsible governance within organizations, it has focused almost exclusively on data practices, often as they are implemented in technology. Yet privacy-by-design also offers an opportunity to build and improve transparency. It allows organizations the chance to create notices that are suited to the particular service or device. Rather than add them on at the end, privacy notices can be integrated into the design of the system. Doing so could result in notices that are more relevant, communicate better to individual users, and become part of the user's interaction with the device or system. Designers, supported by compliance, legal, and appropriate personnel, can take advantage of these support opportunities and overcome the constraints of the system when designing notice. They can identify points in the system where the most useful, appropriate information can be conveyed to the user. Since the time at which a user encounters a notice can affect how effective the notice is, developing the notice throughout the design process can allow designers to provide users notice and information at different times depending on context. It can allow for delivery of visual or auditory notices, depending on the device or

[258] This process is referred to as *privacy-by-design,* an approach to protecting privacy by embedding it into the design specifications of technologies, business practices, and physical infrastructures. *See Introduction to PbD*, Information and Privacy Commissioner of Ontario (last visited Apr. 5, 2016) https://www.ipc.on.ca/english/privacy/introduction-to-pbd/.

data environment. It can also allow developers to take advantage of a variety of channels by which notices can be delivered, depending on the audience, and the constraints and opportunities of the system.[259]

D. *Contextual expectations should serve as a key consideration for improving consumer notices.*

Individual privacy expectations have been defined in terms of social norms within a particular context. These norms define what information practices are acceptable and do not raise privacy concerns in a given context. A recent national public opinion survey found that eighty-seven percent of individuals were concerned about the sharing of their information with others without their knowledge and consent, suggesting this practice violates social norms.[260] Reusing information in a way that is related to the original purpose of the collection generally does not raise privacy concerns because such use conforms to established social norms.[261] These can include sharing an address with a carrier who will deliver a purchase, providing a credit card number to a bank for payment processing, internal operations, fraud prevention or first-party marketing.[262] Because these uses are obvious and/or widely accepted and often do not involve choice, they may need only a brief or even no mention in the consumer notice. On the other hand, heightened attention to

---

[259] *See* Florian Schaub, Rebecca Balebako, Adam L. Durity, Lorrie Faith Cranor*, Symposium on Usable Privacy and Security (SOUPS): A Design Space for Effective Privacy Notices*, (July 22–24, 2015), Ottawa, Canada (Unpublished and on file with SOUPS).

[260] *See* National Cyber Security Alliance, *Results of Consumer Data Privacy Survey Reveal Critical Need for All Digital Citizens to Participate in Data Privacy Day (*Jan. 28, 2015), https://staysafeonline.org/about-us/news/results-of-consumer-data-privacy-survey-reveal-critical-need-for-all-digital-citizens-to-participate-in-data-privacy-day.

[261] *See generally* Helen Nissenbaum, *Privacy in Context* (Stanford Law Books 2010); *see also* Kirsten Martin, *Privacy Notices as Tabula Rasa: An Empirical Investigation into how Complying with a Privacy Notice is Related to Meeting Privacy Expectations Online*, 34 J. OF PUB. POL'Y AND MKTG. 2, 210–27 (2015).

[262] *See Protecting Consumer Privacy in an Era of Rapid Change*, Federal Trade Commission (Mar. 2012), www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

transparency is needed for information processing which is not reasonable in light of the context and violates consumer expectations.[263] Potential contextual issues can be assessed as part of privacy-by-design or during a separate review such as a privacy impact assessment.

E. *Technology should promote transparency by supporting the availability and utility of notice.*

While initial efforts at technological solutions have enjoyed limited success, technology may still play a significant role in fostering better transparency. Just as developments in technology and data processing have enabled powerful new offerings in products and services, such advances arguably should also enable more effective transparency that empowers individuals.

One example of such work is the Usable Privacy Policy Project at Carnegie Mellon University.[264] The project responds to the limitations of natural language, privacy notices, and other obstacles by addressing the problem using machine implementable standards, the project builds on recent advances in natural language processing, privacy preference modeling, crowdsourcing, formal methods, and privacy interfaces.[265] The goal of the project is to develop a technological approach that would (1) semi-automatically extract key privacy policy elements from natural language notices posted on websites and (2) present these elements to users in a format that is easy to read and understand.[266] For users, the project holds out the possibility of access to notices that would inform privacy decision-making. For website operators, it promises a way to overcome the limitations of existing natural language notices without imposing new requirements.

In addition to machine-readable notices, technology can also provide alternatives to traditional text notices. These can include

---

[263] For example, the Obama Administration's 2015 discussion draft of its 2015 Consumer Privacy Bill of Rights Act calls for a risk analysis and specifies notice requirements for data practices that are not reasonable in light of context.

[264] *See generally* The Usable Privacy Policy Project, http://www.usableprivacy.org/learn_more (last visited Apr. 5, 2016).

[265] *Id.*

[266] *Id.*

images, icons, LEDs, or even auditory notices in the form of sounds or spoken word.[267] The mode by which a notice is delivered is best selected to attract the individual's attention given the context. Further, independent of how disclosures are delivered, notice design is most effective when developed as part of the overall system design and subjected to consumer testing prior to rollout.

F. *Public education should work at the core of efforts to promote transparency.*

In addition to the issues discussed above, transparency requires the public be broadly informed about data collection and use – not only on an application-by-application basis, but also as a foundation for navigating the data ecosystem at large. This public awareness fosters greater understanding about data uses, their benefits to the individual and to society, and the risks that they raise. It also enhances understanding of when individual choice is available and when it is not, and the rationale behind the distinction. It provides clear guidance about an individual's rights in her data, how she can exercise her rights, and where she can go to correct mistakes or obtain recourse when a company misuses data or fails to meet its obligations as articulated in law or the policies in its notice. Because privacy notices cannot both educate individuals about these issues and be timely, succinct, and clear; public education must be a separate and ongoing initiative. For example, the success of the nutrition label is due in part because the label was accompanied by an extensive, distinct consumer education effort.[268] This effort continues in the form of ongoing media coverage of nutrition as an element of health. As the experience with the nutrition label demonstrated, public education is not a one-time event and it is a responsibility that should be shared by the public and private sectors.[269]

---

[267] Michael S. Wogalter et al., *supra* note 247.

[268] *See* FRONT-OF-PACKAGE NUTRITION RATING SYSTEMS AND SYMBOLS: PROMOTING HEALTHIER CHOICES, (Ellen A. Wartella et al. eds. 2011); Archon Fung, Mary Graham, & David Weil, *Full Disclosure, The Perils and Promise of Transparency* 96 (2007).

[269] The FTC has engaged in public education around emerging privacy risks, complying with FTC regulations and best practices. While some of the most

To make notice work as a vehicle for transparency, education must not only become the norm but should also be made more visible and easily accessible to the public. Brief, one-time attempts at public education prompted by some event or the release of some product or application will not be sufficient. Data collection that is ubiquitous, invisible, and integrated into infrastructures, requires that the public be apprised of how the ecosystem works and how it is evolving, particularly when these forms of data use are new, unexpected, and possibly violate current contextual norms. But while public education is critical, it does not obviate the need for the comprehensive notice and the consumer-focused notice we described earlier. Nor does it relieve companies of the responsibility to engage in responsible, ethical data practices. Rather, education is an essential complement to notice as it enables the public to make rational choices about data use, when available, based on a full understanding of a particular data ecosystem. Moreover, if individuals are educated, abbreviated notices or notification icons are more likely to effectively provide them with needed information.[270]

notable instances of public education have been in the area of identity theft, which were targeted at consumers, many are focused on the business community. *See* Maureen K. Ohlhausen, *Privacy Challenges and Opportunities: The Role of the Federal Trade Commission,* 33 J. PUB. POL'Y & MKTG. 4, 4–9 (2014).

[270] The use of sensors and beacons in retail environments provides a useful example. Here, the retailer contracts with a third party analytics firm to track customer behavior using their mobile devices. Transparency in this environment poses a challenge because a third party tracks the mobile devices, consumers may not be aware of the tracking, and it is difficult to provide useful in-store notice. Transparency would be improved if the retailer developed an icon to provide notice when tracking was occurring, the stores agreed to display the icon, and consumers were educated about the benefits and risks of these technologies, the icon, and their available choices, if they had any, to limit the tracking if they objected. While such an approach would not eliminate the need for the vendor to provide the tracking service *and* the retailer to provide traditional notice, it would make the tracking transparent. *See About Smart Places,* FUTURE OF PRIVACY FORUM, http://www.futureofprivacy.org/issues/smart-places/.

G. *Better transparency will depend on regulatory guidance 1and business buy-in.*

Proposals for providing consumers with an alternative notice that provides selected information absent a safe harbor have in the past raised concerns about opening companies to liability for failing to provide comprehensive descriptions of their data practices. Requiring both an abbreviated and a comprehensive notice would eliminate such liability concerns. However, this approach may call for legislation or regulation to provide organizations with clarity and assurances about their legal responsibilities and to reduce industry concerns about risk of exposure to regulatory action. While this occurred for the GLB model notice, developing guidance that is sufficiently specific yet applies across industries to a wide variety of business models and information practices is challenging. However, if regulators are unable or unwilling to offer a safe harbor for adopting a consumer notice that fulfills certain conditions provided, or to provide other motivation for business to act, the business community will likely resist this proposal. For example, Smith found that given the ambiguous external environment, executives rarely take active steps to develop new privacy practices absent some external event that forces them to act.[271] Recent events continue to provide support for his findings. The FTC content analysis of websites and its 2009 report on online behavioral advertising resulted in adoption of online privacy notices and the development of the AdChoices icon without new legislation.[272] Regulators could advance transparency for consumers, for example, by conducting web surveys to assess whether firms are complying with existing regulations related to notice visibility and usability. Further, where appropriate, the FTC should decline to endorse any

---

[271] *See* H. Jeff Smith, *Privacy Policies and Practices: Inside the Organizational Maze,* 36 COMMUNICATIONS OF THE ACM 104, 105–22 (1993).

[272] *Protecting Consumer Privacy in an Era of Rapid Change,* FEDERAL TRADE COMMISSION, (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf. In the Preliminary Staff Report, the FTC recognized the increase in privacy notices after the initial web sweeps; however, it also stated that a large number of the notices analyzed in the study were incomplete in terms of the basic elements of fair information practices. *Id.*

solution resulting from either an industry-developed self-regulatory program or a government-led multi-stakeholder process that has not been subjected to rigorous consumer testing to demonstrate its effectiveness. Absent pressure from government, business community leadership, and collaboration with consumer and privacy advocates, notices will fail to provide individuals with the usable information they need about data practices.

Transparency should not pose a threat to organizations, and in fact, for responsible companies, transparency will enhance their relationship with consumers and customers. One study found that when privacy information is made more salient, some consumers are willing to pay a premium to purchase from privacy protective websites. What is particularly interesting about this study is that the participants in the experiment used their own credit cards to make actual purchases rather than just stating their intentions. The authors hypothesize that where there is transparency and privacy protections, privacy may serve as a selling point. [273] Where companies provide value in exchange for the use of their data, transparency enables consumers to evaluate the risk-benefit tradeoff for disclosure.[274] Therefore, transparency does not pose a threat; rather, it promotes consumer trust and the innovative, responsible use of data.

IX. CONCLUSION

Notices currently serve many purposes, including to provide a basis for individual choice; serve as the basis for regulation, promote public awareness of data practices, and enable oversight by privacy experts and advocates of issues related to the collection, processing, and protection of information about individuals. The process of creating notices also provides an opportunity for organizations to review and understand their data collection practices and make

[273] *See* Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study,* 22 INF. SYS. RES. 254, 254–68 (2011).

[274] *See* Naveen F. Awad & M.S. Krishan, *The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization,* 30 MIS QUARTERLY 13, 13–28 (2006).

responsible decisions about internal data flows and external data uses. This Article discussed the shortcomings of traditional notices as a tool for promoting individual choice. It described the results of efforts to improve them through the use of layered or short notices and reviewed attempts to develop technological alternatives to traditional notice. Finally, it identified the challenges that new technologies such as big data, mobile environments, and the Internet of Things pose to notice.

This Article further argues that the way data is collected, used, processed, and stored in the emerging data eco-system requires not simply improved notices, but a multi-pronged approach to informing the individual about data and privacy practices that promotes an overall *environment of transparency*. As this Article notes in the opening sections, transparency is a condition of disclosure and awareness created by organizations that involves the use of an array of methods, notice among them. Whether transparency is achieved depends on the extent to which information is disclosed—its timeliness, its clarity, and its accuracy. The authors conclude that while notice is central to transparency, transparency involves far more than notice; they agree that notices as currently implemented must be fixed, however, even if improved, notices will not be sufficient to achieve transparency the evolving data ecosystem requires more.

Finally, this Article identifies the shortcomings of the current privacy regime as well as new challenges the twenty-first century data ecosystem poses for transparency. Further, while transparency is a necessary condition for fair data use, it alone is not sufficient, since all of the fair information principles contribute to fairness. While moving from notice to transparency poses its own challenges to both regulators and business, a combination of improved notices, attention to contextual norms, integration of the design of notices into the system development process as part of privacy-by-design, public education, and new technological solutions hold promise for addressing the current situation where there is agreement across a range of stakeholders that current privacy notices are simply not working.