Protecting Consumer Privacy in an Era of Rapid Change A Dynamic Policy Framework

A Proposed Framework for Business and Policymakers

Preliminary FTC Staff Report

Federal Trade Commission

Originally Published December 2010[*†‡]

[*] http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

[†] Reprinted with permission exclusively for the *Journal of Privacy and Confidentiality*

[‡] Public comments on original report available at http://www.ftc.gov/os/comments/privacyreportframework/index.shtm

Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*

Table of Contents

*U.S. Department of Commerce Internet Policy Task Force (Dec. 2010), available at `http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf`.

Journal of Privacy and Confidentiality (2011) **3**, Number 1, 67–140

Protecting Consumer Privacy in an Era of Rapid Change—A Proposed Framework for Businesses and Policymakers; Preliminary FTC Staff Report

Federal Trade Commission

Executive Summary

In todays digital economy, consumer information is more important than ever. Companies are using this information in innovative ways to provide consumers with new and better products and services. Although many of these companies manage consumer information responsibly, some appear to treat it in an irresponsible or even reckless manner. And while recent announcements of privacy innovations by a range of companies are encouraging, many companies—both online and offline—do not adequately address consumer privacy interests.

Industry must do better. For every business, privacy should be a basic consideration similar to keeping track of costs and revenues, or strategic planning. To further this goal, this report proposes a normative framework for how companies should protect consumers privacy. This proposal is intended to inform policymakers, including Congress, as they develop solutions, policies, and potential laws governing privacy, and guide and motivate industry as it develops more robust and effective best practices and self-regulatory guidelines. The framework is designed to serve as a policy vehicle for approaching privacy, but it includes elements that reflect longstanding Federal Trade Commission ("FTC" or "Commission") law.

Although privacy often has been said to mean "the right to be let alone,"[1] the application of this concept in modern times is by no means straightforward. Consumers live in a world where information about their purchasing behavior, online browsing habits, and other online and offline activity is collected, analyzed, combined, used, and shared, often instantaneously and invisibly. For example:

- if you browse for products and services online, advertisers might collect and share information about your activities, including your searches, the websites you visit, and the content you view;
- if you participate in a social networking site, third-party applications are likely to have access to the information you or your friends post on the site;
- if you use location-enabled smartphone applications, multiple entities might have

[1] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 193 (1890).

access to your precise whereabouts;

- if you use loyalty cards at a grocery store or send in a product warranty card, your name, address, and information about your purchase may be shared with data brokers and combined with other data.

Some consumers are troubled by the collection and sharing of their information. Others have no idea that any of this information collection and sharing is taking place. Still others may be aware of this collection and use of their personal information but view it as a worthwhile trade-off for innovative products and services, convenience, and personalization. And some consumers—some teens for example—may be aware of the sharing that takes place, but may not appreciate the risks it poses. In addition, consumers level of comfort might depend on the context and amount of sharing that is occurring. For example, some consumers may be unconcerned about the collection and sharing of discrete pieces of information about them because that information, by itself, may seem innocuous. However, they may find the compilation of vast quantities of data about them surprising and disturbing. Because of these differences in consumer understanding, attitudes and behavior, as well as the rapid pace of change in technology, policymaking on privacy issues presents significant challenges.

The FTCs efforts to protect consumer privacy date back to the 1970s, when it began enforcing one of the first federal privacy laws—the Fair Credit Reporting Act ("FCRA").[2] Since then, the Commission has sought to protect consumer privacy through law enforcement, policy initiatives, and consumer and business education. Using these tools, the Commission's goal in the privacy arena has remained constant: to protect consumers' personal information and ensure that they have the confidence to take advantage of the many benefits of the ever-changing marketplace. In recent years, the FTC has sought to advance this objective using two primary models: the "notice-and-choice model," which encourages companies to develop privacy notices describing their information collection and use practices to consumers, so that consumers can make informed choices, and the "harm-based model," which focuses on protecting consumers from specific harms physical security, economic injury, and unwanted intrusions into their daily lives. Each model has significantly advanced the goal of protecting consumer privacy; at the same time, each has been subject to certain criticisms.

Specifically, the notice-and-choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand. Likewise, the harm-based model has been criticized for failing to recognize a wider range of privacy-related concerns, including reputational harm or the fear of being monitored. In addition, both models have struggled to keep pace with the rapid growth of technologies and business models that enable companies to collect and use consumers information in ways that often are invisible to consumers. Meanwhile, industry efforts to address privacy through self-regulation have been too slow, and up to now have failed to provide adequate and meaningful protection.

[2] 15 U.S.C. § 1681 (2010). The Commission currently enforces a number of other sector-specific privacy laws, as well as the Federal Trade Commission Act's broad prohibition on "unfair or deceptive" acts or practices. 15 U.S.C. § 45 (2010).

In light of these concerns, last year the Commission announced that it would host a series of roundtables to explore the privacy issues and challenges associated with 21st century technology and business practices to determine how best to protect consumer privacy while supporting beneficial uses of information and technological innovation. Roundtable participants reflected a wide range of perspectives and included academics, technologists, privacy experts, consumer advocates, representatives from industry, and regulators.

Several major themes emerged from these discussions, including:

- the ubiquitous collection and use of consumer data;
- consumers' lack of understanding and ability to make informed choices about the collection and use of their data;
- the importance of privacy to many consumers;
- the significant benefits enabled by the increasing flow of information; and
- the blurring of the distinction between personally identifiable information and supposedly anonymous or de-identified information.

Stakeholders emphasized the need to improve transparency, simplify the ability of consumers to exercise choices about how their information is collected and used, and ensure that businesses take privacy-protective measures as they develop and implement systems. At the same time, commenters and participants urged regulators to be cautious about restricting the exchange and use of consumer data in order to preserve the substantial consumer benefits made possible through the flow of information. Participants noted, for example, that the acquisition, exchange, and use of consumer data not only helps to fund a variety of personalized content and services, but also allows businesses to innovate and develop new products and services that offer consumers convenience and cost savings.

Based upon the major themes and concepts developed through the roundtables, Commission staff is proposing a new framework for addressing the commercial use of consumer data. This framework builds upon the notice-and-choice and harm-based models, the FTCs law enforcement experience, and the record from the roundtables. Commission staff encourages all interested parties to submit written comments to help guide further development and refinement of the proposal.

The proposed framework would apply broadly to online and offline commercial entities that collect, maintain, share, or otherwise use consumer data that can be reasonably linked to a specific consumer, computer or device. It contains three main components.

First, companies should adopt a "privacy by design"[3] approach by building privacy protections into their everyday business practices. Such protections include providing reasonable security for consumer data, collecting only the data needed for a specific business purpose, retaining data only as long as necessary to fulfill that purpose, safely

disposing of data no longer being used, and implementing reasonable procedures to promote data accuracy. Companies also should implement and enforce procedurally sound privacy practices throughout their organizations, including, for instance, assigning personnel to oversee privacy issues, training employees on privacy issues, and conducting privacy reviews when developing new products and services. Such concepts are not new, but the time has come for industry to implement them systematically. Implementation can be scaled to each company's business operations. Companies that collect and use small amounts of non-sensitive consumer data should not have to devote the same level of resources to implementing privacy programs as companies that collect vast amounts of consumer data, collect data of a sensitive nature, or engage in the business of selling consumer data.

Second, Commission staff proposes that companies provide choices to consumers about their data practices in a simpler, more streamlined way than has been used in the past. Under this approach, consumer choice would not be necessary for a limited set of "commonly accepted" data practices, thus allowing clearer, more meaningful choice with respect to practices of greater concern. This component of the proposed framework reflects the concept that it is reasonable for companies to engage in certain commonly accepted practices—namely, product and service fulfillment, internal operations such as improving services offered, fraud prevention, legal compliance, and first-party marketing. Some of these practices, such as where a retailer collects a consumer's address solely to deliver a product the consumer ordered, are obvious from the context of the transaction, and therefore, consent for them is inferred. Others are sufficiently accepted—or necessary for public policy reasons—that companies need not request consent to engage in them. By clarifying those practices for which consumer consent is unnecessary, companies will be able to streamline their communications with consumers, reducing the burden and confusion on consumers and businesses alike.

For data practices that are not "commonly accepted," consumers should be able to make informed and meaningful choices. To be most effective, choices should be clearly and concisely described and offered when—and in a context in which—the consumer is making a decision about his or her data. Depending upon the particular business model, this may entail a "just-in-time" approach, in which the company provides the consumer with a choice at the point the consumer enters his personal data or before he accepts a product or service.

One way to facilitate consumer choice is to provide it in a uniform and comprehensive way. Such an approach has been proposed for behavioral advertising, whereby consumers would be able to choose whether to allow the collection and use of data regarding their online searching and browsing activities. The most practical method of providing such universal choice would likely involve the placement of a persistent setting, similar to a cookie, on the consumer's browser signaling the consumer's choices about being tracked and receiving targeted ads. Commission staff supports this approach, sometimes referred to as "Do Not Track."

[3]Privacy By Design is an approach that Ann Cavoukian, Ph.D., Information and Privacy Commissioner of Ontario, has advocated. *See Privacy by Design*, Information & Privacy Commissioner of Ontario, `http://www.privacybydesign.ca`.

Third, staff proposes a number of measures that companies should take to make their data practices more transparent to consumers. For instance, although privacy policies may not be a good tool for communicating with most consumers, they still could play an important role in promoting transparency, accountability, and competition among companies on privacy issues—but only if the policies are clear, concise, and easy-to-read. Thus, companies should improve their privacy policies so that interested parties can compare data practices and choices across companies.

Staff also proposes providing consumers with reasonable access to the data that companies maintain about them, particularly for companies that do not interact with consumers directly, such as data brokers. Because of the significant costs associated with access, staff believes that the extent of access should be proportional to both the sensitivity of the data and its intended use. In addition, all entities must provide robust notice and obtain affirmative consent for material, retroactive changes to data policies.

Finally, staff proposes that stakeholders undertake a broad effort to educate consumers about commercial data practices and the choices available to them. Increasing consumer understanding of the commercial collection and use of their information is important to facilitating competition on privacy across companies.

Commission staff seeks comment by January 31, 2011, on each component of the proposed framework and how it might apply in the real world. Interested parties are encouraged to raise, and comment upon, related issues. Based on comments received, the Commission will issue a final report in 2011. In the meantime, the Commission plans to continue its vigorous law enforcement in the privacy area, using its existing authority under Section 5 of the Federal Trade Commission Act and the other consumer privacy laws it enforces.

Protecting Consumer Privacy in an Era of Rapid Change:
A Proposed Framework for Businesses and Policymakers

Scope: The framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device.

Principles:

PRIVACY BY DESIGN

Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services.

- Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention practices, and data accuracy.
- Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.

SIMPLIFIED CHOICE

Companies should simplify consumer choice.

- Companies do not need to provide choice before collecting and using consumers' data for commonly accepted practices, such as product fulfillment.
- For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data.

GREATER TRANSPARENCY

Companies should increase the transparency of their data practices.

- Privacy notices should be clearer, shorter, and more standardized, to enable better comprehension and comparison of privacy practices.
- Companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use.
- Companies must provide prominent disclosures and obtain affirmative express consent before using consumer data in a materially different manner than claimed when the data was collected.
- All stakeholders should work to educate consumers about commercial data privacy practices.

1 Introduction

The FTC has long been at the forefront of consumer privacy issues. It has engaged in aggressive law enforcement, hosted workshops on technology and other issues, promoted industry self-regulation, and conducted substantial outreach on privacy issues. With this report, the Commission reaffirms its long-standing commitment to this important area.

On December 7, 2009, the Commission launched a series of public roundtables to explore the privacy issues and challenges associated with 21st century technology and business practices that collect and use consumer data.[4] The decision to host the privacy roundtables reflected a growing sense that the Commission's existing approaches to protecting consumer privacy must continue to keep pace with changes in the marketplace. These changes include the development of new technologies and business models, such as social media services, cloud computing, mobile services, and increasingly powerful behavioral advertising techniques. On the one hand, these innovations provide tremendous benefits for consumers in the form of new products and services. On the other hand, they facilitate unprecedented levels of data collection, which often are invisible to consumers. In hosting the roundtables, the Commission sought to evaluate how best to protect consumer privacy, while also preserving the ability of companies to innovate, compete, and offer consumer benefits. In advance of each roundtable, the Commission posed a number of key questions and solicited public comment, academic papers, consumer surveys, and other relevant research.

Roundtable discussions covered a range of topics, such as the risks and benefits of data collection, consumers' expectations about data practices and privacy, the adequacy of existing legislation and self-regulatory regimes, the use of privacy-enhancing technologies, and the treatment of health and sensitive information. In addition, the roundtables explored the privacy implications of a number of business models including online behavioral advertising, social networking, mobile services, cloud computing, and information brokers. Roundtable participants included a broad range of stakeholders—industry representatives, academics, technologists, consumer and privacy advocates, and government officials—and the Commission received over 100 written submissions from interested parties.

This report begins by providing brief background on the Commission's leadership in the privacy arena. Next, it outlines the themes, concepts, and areas of discussion that emerged from the privacy roundtables. The report then sets forth a proposed framework to inform policymakers as they develop solutions, policies, and potential laws governing privacy, and to guide and motivate industry as it develops and refines best practices and self-regulatory guidelines. The proposed framework builds upon the record from the roundtables and the foundation of the Commissions law enforcement and policy work protecting consumer privacy. In discussing the proposed framework, the report raises a number of issues and questions for public comment.[5] Commission staff will consider comments it receives as it further develops and refines the proposed framework for its

[4] *See FTC, Exploring Privacy—A Roundtable Series*, (Dec. 7, 2009), `http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml`. The second and third roundtable events took place on January 28, 2010, and March 17, 2010. *Id.*

final report.

2 Background

2.1 Privacy and the FTC [6]

The FTC's focus on privacy issues dates back to enactment of the Fair Credit Reporting Act ("FCRA") in 1970.[7] The FTC has been the primary enforcer of this law, which protects sensitive consumer information—used for decisions involving credit, employment and insurance—from disclosure to unauthorized persons.[8] Through its implementation and enforcement of the FCRA over the last few decades, the FTC has developed unique expertise in consumer privacy issues. Beginning in the mid-1990s, aided by the enactment of new consumer privacy laws discussed below, the FTC began to examine privacy issues extending beyond the concerns embodied by the FCRA. Since then, privacy has been one of the FTC's highest consumer protection priorities, which it has addressed through law enforcement, policy initiatives, and consumer and business education. Through this work, the Commission has sought to identify and understand existing and emerging threats to consumer privacy, while also preserving the benefits that technological advances offer. The FTC has balanced these two objectives by taking a flexible and evolving approach to privacy protection, designed to keep pace with a dynamic marketplace.

The Commission's primary source of legal authority is Section 5 of the FTC Act, which empowers the Commission to take action against deceptive or unfair acts or practices.[9] The Commission also enforces numerous sector-specific statutes, including the Gramm-Leach-Bliley Act ("GLB Act"), the Children's Online Privacy Protection Act ("COPPA"), the CAN-SPAM Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act ("Do Not Call Rule").[10] As described below, the Commission has brought scores of consumer privacy cases under these laws.

In addition to its enforcement work, the FTC has conducted studies and held public events regarding the privacy and security implications of various technologies and business practices. For example, the Commission has held public workshops on the privacy implications of online behavioral advertising and mobile marketing, as well as

[5] The questions for comment appear throughout the report and also separately in Appendix A. In addition to these specific questions, interested parties may provide comments on any of the issues raised by the report.

[6] This report addresses the FTC's approach to consumers' privacy in commercial transactions. For a more comprehensive discussion of the history of privacy law, see Daniel J. Solove & Paul M. Schwartz, *Information Privacy Law* (3d. ed. 2009).

[7] Attached as Appendix B is a timeline of some of the FTC's major consumer privacy actions since 1970, including law enforcement, policy initiatives, and consumer and business education.

[8] 15 U.S.C. § 1681.

[9] 15 U.S.C. § 45.

[10] *See* GLB Act, 15 U.S.C. §§ 6801-6809 (2010) (consumer financial data); COPPA, 15 U.S.C. §§ 6501-6506 (2010) (information about children); CAN-SPAM Act, 15 U.S.C. §§ 7701-7713 (2010) (unsolicited electronic messages); and Do Not Call Rule, 15 U.S.C. §§ 6101-6108 (2010) (telemarketing calls).

radio frequency identification ("RFID") and authentication technologies.[11] The FTC has also testified before Congress on a variety of privacy and data security issues.[12] Finally, the Commission has published educational materials to inform consumers and businesses about different privacy issues and how businesses can comply with statutory requirements.[13]

Although the FTC's commitment to consumer privacy has remained constant, the Commission has employed different, though complementary, approaches to privacy over

[11] *See, e.g., FTC International Conference: Securing Personal Data in the Global Economy*, FTC (Mar. 16-17, 2009), `http://www.ftc.gov/bcp/workshops/personaldataglobal/index.shtm`; *FTC Public Workshop: Transatlantic RFID Workshop on Consumer Privacy and Data Security*, FTC (Sept. 23, 2008), `http://www.ftc.gov/bcp/workshops/transatlantic/index.shtml`; *FTC Town Hall: Pay on the Go* (July 24, 2008), `http://www.ftc.gov/bcp/workshops/payonthego/index.shtml`; *FTC Town Hall, Beyond Voice: Mapping the Mobile Marketplace*, FTC (May 6-7, 2008), `http://www.ftc.gov/bcp/workshops/mobilemarket/index.shtml`; *FTC Town Hall: Behavioral Advertising: Tracking, Targeting, & Technology*, FTC (Nov. 1-2, 2007), `http://www.ftc.gov/bcp/workshops/ehavioral/index.shtml`; *FTC Public Workshop: Spam Summit, The Next Generation of Threats and Solutions*, FTC (July 11-12, 2007), `http://www.ftc.gov/bcp/workshops/spamsummit/index.shtml`; *FTC Public Workshop: Proof Positive, New Directions for ID Authentication*, FTC (Apr. 23-24, 2007), `http://www.ftc.gov/bcp/workshops/proofpositive/index.shtml`; *FTC Public Workshop: Peer-to-Peer File-Sharing Technology, Consumer Protection and Competition Issues*, FTC (Dec. 15-16, 2004), `http://www.ftc.gov/bcp/workshops/filesharing/index.htm`; *FTC Public Workshop: Radio Frequency IDentification, Applications and Implications for Consumers*, FTC (June 21, 2004), `http://www.ftc.gov/bcp/workshops/rfid/index.shtm`; *FTC Public Workshop: Monitoring Software on Your PC, Spyware, Adware, and Other Software*, FTC (Apr. 19, 2004), `http://www.ftc.gov/bcp/workshops/spyware/index.shtm` [hereinafter FTC Public Workshops].

[12] *See, e.g., Consumer Privacy: Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 111th Cong. (July 27, 2010), *available at* `http://www.ftc.gov/os/testimony/100727consumerprivacy.pdf` (prepared statement of the FTC); *Consumer Privacy: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Prot. of the H. Comm. on Energy and Commerce*, 111th Cong. (July 22, 2010), *available at* `http://www.ftc.gov/os/testimony/100722consumerprivacyhouse.pdf` (prepared statement of the FTC); *Protecting Youths in an Online World: Hearing Before the Subcomm. on Consumer Prot., Prod. Safety, and Ins. of the S. Comm. on Commerce, Sci., and Transp.*, 111th Cong. (July 15, 2010), *available at* `http://www.ftc.gov/os/testimony/100715toopatestimony.pdf` (prepared statement of the FTC); *An Examination of Children's Privacy: Hearing Before the Subcomm. on Consumer Prot., Prod. Safety, and Ins. of the S. Comm. on Commerce, Sci., and Transp.*, 111th Cong. (Apr. 29, 2010), *available at* `http://www.ftc.gov/os/testimony/100429coppastatement.pdf` (prepared statement of the FTC); *Hearing on H.R. 2221, the Data Accountability and Protection Act, and H.R. 1319, the Informed P2P User Act Before the Subcomm. on Commerce, Trade and Consumer Prot. of the H. Comm. on Energy and Commerce*, 111th Cong. (May 5, 2009), available at `http://www.ftc.gov/os/2009/05/P064504peertopeertestimony.pdf` (prepared statement of the FTC); *Data Breaches and Identity Theft: Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 109th Cong. (June 16, 2005), *available at* `http://www.ftc.gov/os/2005/06/050616databreaches.pdf` (prepared statement of the FTC).

[13] For example, the Commission's well-known OnGuard Online website educates consumers about threats such as spyware, phishing, laptop security, and identity theft. *See OnGuard Online*, FTC, `http://www.onguardonline.gov`. The FTC also developed a guide to help small and medium-sized businesses implement appropriate data security for the personal information they collect and maintain. *See Protecting Personal Information: A Guide For Business*, FTC, `http://www.ftc.gov/infosecurity`. In addition, the FTC has developed a brochure, *Net Cetera: Chatting with Kids About Being Online*, specifically for children, parents, and teachers to help kids stay safe online. *See* Press Release, FTC, OnGuardOnline.gov Off to a Fast Start with Online Child Safety Campaign (Mar. 31, 2010), `http://www.ftc.gov/opa/2010/03/netcetera.shtm`. Further, the Commission offers specific guidance for certain types of Internet services, including, for example, social networking and peer-to-peer file sharing. *See Topics: OnGuard Online*, FTC, `http://www.onguardonline.gov/topics/overview.aspx`.

time, in part to account for changes in the marketplace. In the mid-to-late 1990s, the FTC encouraged companies to implement the fair information practice principles of notice, choice, access, and security and undertook enforcement efforts related to claims companies made in their privacy notices. Thereafter, in the early 2000s, the Commission began focusing on the specific harms associated with the misuse of consumers' data, such as risks to physical security, economic injury, and unwanted intrusions into consumers' daily lives. During this period, the Commission brought aggressive enforcement against, for example, purveyors of spam and spyware, as well as companies that inadequately protected the security of consumer data. Each of the Commission's approaches has enhanced the effectiveness of its consumer protection efforts, and the agency has continued to use both approaches as appropriate.

2.1.1 The FTC Approach to Fair Information Practice Principles

With the emergence of online commerce in the mid-1990s, the Commission began to examine online privacy and consumers' developing concerns about the information they provided through the Internet. As a starting point, the Commission drew upon a set of widely accepted "Fair Information Practice Principles," which embodied the important underlying concepts of transparency, consumer autonomy, and accountability. The Commission noted that, since the 1970s, government agencies in the United States, Canada, and Europe, as well as multilateral international organizations, had issued a series of reports, guidelines, and model codes, the core of which contained these fair information principles.[14]

The Commission's early online privacy work focused on four key elements of the overall fair information practices approach: (1) businesses should provide **notice** of what information they collect from consumers and how they use it; (2) consumers should be given **choice** about how information collected from them may be used; (3) consumers should have **access** to data collected about them; and (4) businesses should take reasonable steps to ensure the **security** of the information they collect from consumers. The

[14] *See* U.S. Dep't of Health, Ed. and Welfare, *Records, Computers and the Rights of Citizens: Report of The Secretary's Advisory Committee on Automated Personal Data Systems* (July 1973), *available at* `http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm`. In 1980, the Organisation for Economic Co-operation and Development ("OECD") adopted privacy guidelines in response to the growth of automatic data processing, which enabled increased transfers of personal data across national borders. The OECD privacy guidelines included the following principles: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. See Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, [hereinafter OECD Guidelines] *available at* `http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html`. These principles are reflected in laws such as the European Union's 1995 Data Protection Directive and Canada's Personal Information Protection and Electronic Documents Act. *See* Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, 1995 O.J. (L 281) 31, [hereinafter Directive 95/46/EC] *available at* `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML`; Canada's Personal Information Protection and Electronic Documents Act, S.C. 2000, c.5 (2008) [hereinafter PIPEDA] *available at* `http://laws-lois.justice.gc.ca/eng/acts/P-8.6/`.

Commission also identified **enforcement**—the use of a reliable mechanism to impose sanctions for noncompliance as a critical component of any regulatory or self-regulatory program.

To promote these practices in the context of emerging business models, the Commission undertook a number of policy initiatives. Among other things, the Commission conducted surveys of online privacy policies, hosted workshops, and issued reports to Congress on the subject, and commented on self-regulatory and technological developments intended to enhance consumer privacy.

In 2000, the Commission reported to Congress that, although there had been improvement in industry self-regulatory efforts to develop and post privacy policies online, only about one-quarter of the privacy policies surveyed addressed the four fair information practice principles of notice, choice, access, and security.[15] Accordingly, a majority of the Commission concluded that legislation requiring online businesses to comply with these principles, in conjunction with self-regulation, would allow the electronic marketplace to reach its full potential and give consumers the confidence they need to participate fully in that marketplace.[16] Although Congress did not enact the recommended legislation, the Commission's work during this time—particularly its surveys, reports, and workshops—raised public awareness about consumer privacy and led companies to examine their information collection practices and to post privacy policies. It also encouraged self-regulatory efforts designed to benefit consumers, improvements in privacy-enhancing technologies, and the creation of online privacy certification programs.

During this period, the Commission also used its Section 5 authority to bring actions against companies that engaged in unfair or deceptive information practices. Most of these early cases involved deceptive statements in companies' privacy notices about their collection and use of consumers' data.[17] The legal theories in these early enforcement actions highlighted, in particular, the fair information practice principles of notice and choice (the "notice-and-choice approach"). Collectively, the Commission's policy and enforcement efforts underscored its emphasis on the concepts of transparency and accountability for information practices.

---

[15] *See* FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace* 12-13 (2000), *available at* `http://www.ftc.gov/reports/privacy2000/privacy2000.pdf`.

[16] *Id.* at 36-38 (Commissioner Swindle dissenting, Commissioner Leary concurring in part and dissenting in part).

[17] *See, e.g., In re GeoCities, Inc.*, 127 F.T.C. 94 (1999) (consent order) (settling charges that website had misrepresented the purposes for which it was collecting personally identifiable information from children and adults); FTC v. *Toysmart.com, LLC*, No. 00-11341-RGS, 2000 WL 34016434 (D. Mass. July 21, 2000) (consent order) (challenging website's attempts to sell children's personal information, despite a promise in its privacy policy that such information would never be disclosed); *see also In re Liberty Fin. Cos.*, 128 F.T.C. 240 (1999) (consent order) (alleging that site falsely represented that personal information collected from children, including information about family finances, would be maintained anonymously); *FTC v. ReverseAuction.com Inc.*, No. 00-0032 (D.D.C. Jan. 6, 2000), `http://www.ftc.gov/os/2000/01/reverseconsent.htm` (consent order) (settling charges that an online auction site allegedly obtained consumers' personal identifying information from a competitor site and then sent deceptive, unsolicited email messages to those consumers seeking their business); FTC v. Sandra Rennert, No. CV-S-00-0861-JBR (D. Nev. July 6,

2.1.2 Harm-Based Approach

In the early 2000s, prompted by concern over offline data privacy threats and the increasing convergence of online and offline data systems, the Commission's privacy approach evolved to include a focus on specific consumer harms as the primary means of addressing consumer privacy issues. Rather than emphasizing potentially costly notice-and-choice requirements for all uses of information, the harm-based model targeted practices that caused or were likely to cause physical or economic harm, or "unwarranted intrusions in [consumers'] daily lives."[18]

The harm-based model successfully advanced consumer protection in a number of contexts, including data security, identity theft, children's privacy, spam, spyware, and unwanted telemarketing. For example, since 2001, the FTC has used its authority under a number of statutes—including the FCRA, the GLB Act, and Section 5 of the FTC Act—to bring 29 cases against businesses that allegedly failed to protect consumers' personal information.[19] These cases, against well-known companies such as Microsoft, ChoicePoint, TJX, and LexisNexis, involved such practices as the alleged failure to: (1) comply with posted privacy policies;[20] (2) take appropriate steps to protect against common vulnerabilities;[21] (3) dispose of data properly;[22] and (4) take reasonable steps to ensure that they do not share customer data with unauthorized third parties.[23] The orders obtained in these cases have required companies to implement comprehensive information security programs and to obtain third-party audits of the effectiveness of those programs. In some cases, the Commission also obtained significant monetary relief—for example, in *ChoicePoint*, the Commission received a $10 million civil penalty for alleged violations of the FCRA and $5 million in redress for consumers.[24] The Commission also has brought 96 cases involving unwanted spam;[25] 15 spyware cases;[26] and 15 cases against companies that violated COPPA by collecting personal information

2000), `http://www.ftc.gov/os/caselist/9923245/9923245.shtm` (consent order) (alleging that defendants misrepresented the security and encryption used to protect consumers' information and used the information in a manner contrary to their stated purpose).

[18] In announcing the Commission's expanded privacy agenda, then FTC Chairman Muris noted that "[m]any consumers are troubled by the extent to which their information is collected and used . . . [but that] what probably worries consumers most are the significant consequences that can result when their personal information is misused." *See* Remarks of FTC Chairman Tim Muris at the Privacy 2001 Conference (Oct. 4, 2001), *available at* `http://www.ftc.gov/speeches/muris/privisp1002.shtm`. Chairman Muris then identified various harms caused by the misuse of consumer data—for example, risks to physical security from stalking; economic injury resulting from identity theft; and commercial intrusions into daily life by unwanted solicitations.

from children without parental consent.[27]

Perhaps the Commission's most well-known privacy initiative during this period is the Do Not Call Rule. Since its inception in 2003, Do Not Call has been highly successful in protecting consumers from unwanted telemarketing calls. The Do Not Call Rule's registry currently includes over 200 million telephone numbers. The Commission actively enforces the requirements of the Do Not Call Rule to ensure its ongoing effectiveness. It has brought 64 cases alleging violations of the Do Not Call Rule, resulting in almost $60 million in monetary relief.[28] Do Not Call demonstrates that a thoughtful privacy initiative can have almost universal support.

2.2 Recent Privacy Initiatives

In recent years, the Commission has continued to employ a range of tools—including law enforcement, consumer and business education, policymaking, and international outreach—in pursuing its consumer privacy initiatives. Many of these initiatives have highlighted the distinct challenges that new technologies and the changing marketplace

[19] *See Privacy Initiatives, Enforcement*, FTC, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

[20] *See, e.g., In re Premier Capital Lending, Inc.*, No. C-4241, 2008 WL 5266769 (F.T.C. Dec. 10, 2008) (consent order); *In re Life Is Good, Inc.*, No. C-4218, 2008 WL 1839971 (F.T.C. Apr. 16, 2008) (consent order); *In re Petco Animal Supplies, Inc.*, 139 F.T.C. 102 (2005); MTS, Inc., 137 F.T.C. 444 (2004) (consent order); *In re Microsoft Corp.*, 134 F.T.C. 709 (2002) (consent order).

[21] *See, e.g., In re TJX Cos.*, No. C-4227, 2008 WL 3150421 (F.T.C. July 29, 2008) (consent order); *In re Guidance Software, Inc.*, No. C-4187, 2007 WL 1183340 (F.T.C. Mar. 30, 2007) (consent order); *In re Petco Animal Supplies, Inc.*, 139 F.T.C. 102 (2005) (consent order); *In re Guess?, Inc.*, 136 F.T.C. 507 (2003) (consent order).

[22] *See, e.g., FTC v. Navone*, No. 2:08-CV-001842 (D. Nev. Dec. 30, 2008), http://www.ftc.gov/os/caselist/0723067/100120navonestip.pdf (consent order); *United States v. Am. United Mortg. Co.*, No. 1:07-CV-07064 (N.D. Ill. Dec. 18, 2007), http://www.ftc.gov/os/caselist/0623103/071217americanunitedmrtgstipfinal.pdf (consent order); *In re CVS Caremark Corp.*, No. C-4259, 2009 WL 1892185 (F.T.C. June 18, 2009) (consent order).

[23] *See, e.g., United States v. Rental Research Serv.*, No. 09 CV 524 (D. Minn. Mar. 5, 2009), http://www.ftc.gov/os/caselist/0723228/090305rrsorder.pdf (consent order); *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198 (N.D. Ga. Feb. 15, 2006), http://www.ftc.gov/os/caselist/choicepoint/stipfinaljudgement.pdf (consent order).

[24] *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198 (N.D. Ga. Feb. 15, 2006), http://www.ftc.gov/os/caselist/choicepoint/stipfinaljudgement.pdf (stipulated order imposing $15 million judgment); *United States v. ChoicePoint, Inc.,* No. 1:06-CV-0198-JTC (N.D. Ga. Oct. 14, 2009), http://www.ftc.gov/os/caselist/choicepoint/100902choicepointstip.pdf (stipulated order imposing additional $275,000 civil penalty). Beginning in 2003, numerous states passed data breach notification laws, which required companies to notify affected consumers in the event of a data breach. See, e.g., Cal. Civ. Code §§ 1798.29, 1798.82-1789.84 (West 2003). These laws further increased consumers' awareness of data security issues and related harms, as well as the FTCs awareness of data security issues at specific companies.

[25] *See Spam Introduction*, FTC, http://www.ftc.gov/bcp/edu/microsites/spam/index.html.

[26] *See Spyware Enforcement Actions*, FTC, http://www.ftc.gov/bcp/edu/microsites/spyware/law_enfor.htm.

[27] *See Children's Privacy Enforcement*, FTC, http://business.ftc.gov/privacy-and-security/childrens-online-privacy

[28] *See Do Not Call Enforcement Action Announcements*, FTC, http://www.ftc.gov/bcp/edu/microsites/donotcall/cases.html.

raise for consumer privacy.

2.2.1 Enforcement

A number of the Commission's recent cases have focused on emerging technologies that permit new ways of collecting and using consumer data. For example, in a complaint against the retailer Sears, the Commission claimed that the company had violated Section 5 of the FTC Act by deceiving consumers about the extent to which it tracked their online activities.[29] The FTC alleged that Sears paid $10 to consumers who visited its websites and agreed to download "research" software that the company said would confidentially track their "online browsing." The complaint charged that the software in fact collected vast amounts of information, such as the contents of consumers' shopping carts, online bank statements, drug prescription records, video rental records, and library borrowing histories. Only in the middle of a lengthy user license agreement, available to consumers at the end of a multi-step registration process, did Sears disclose the full extent of the information the software tracked. The Commission alleged that this did not constitute adequate notice to consumers of the company's tracking activities and thus violated Section 5 of the FTC Act. The Commission's resulting consent order against Sears requires the company to stop collecting data from the consumers who downloaded the software and to destroy all data it had previously collected.

Additionally, the Commission has brought cases involving the privacy implications of social networking services. For example, the FTC challenged the social media service Twitter, alleging that it deceived customers by failing to honor their choices to designate certain "tweets" as private.[30] The FTC also alleged that imbee.com, a social networking website directed to young people, violated COPPA by collecting personal information from children under the age of 13 without obtaining verifiable parental consent.[31]

2.2.2 Consumer and Business Education

The FTC has done groundbreaking work to educate consumers and businesses in the area of consumer privacy and data security. For example, the Commission's well-known OnGuard Online website educates consumers about such threats as spyware and online phishing, as well as security measures consumers can take to avoid them.[32] Other outreach includes a guide to help small and medium-sized businesses implement appropriate data security for personal information,[33] and guidance for businesses to respond

[29] *See In re Sears Holdings Mgmt. Corp.*, No. C-4264 (Aug. 31, 2009), `http://www.ftc.gov/os/caselist/0823099/090604searsdo.pdf` (consent order).

[30] *See In re Twitter, Inc.*, No. 092-3093, 2010 WL 2638509 (F.T.C. June 24, 2010) (proposed consent order).

[31] *See United States v. Industrious Kid, Inc.*, CV No.08-0639 (N.D. Cal. 2008), available at `http://www.ftc.gov/os/caselist/0723082/080730cons.pdf` (consent order).

to specific threats, such as those posed by peer-to-peer file sharing.[34]

Additionally, the FTC has developed resources specifically for children, parents, and teachers to help kids stay safe online. Among other materials, the FTC produced the booklet *Net Cetera: Chatting with Kids About Being Online* to give adults practical tips to help children navigate the online world.[35] In less than 10 months, the Commission already has distributed more than 6 million copies of *Net Cetera* to schools and communities nationwide.

2.2.3 Policymaking and Research

The Commission's privacy work also includes public workshops to examine the implications of new technologies on consumer privacy and security.[36] For instance, in 2008 Commission staff hosted a workshop examining online behavioral advertising and subsequently released principles to guide self-regulatory efforts in this area. These principles include: (1) transparency and consumer control; (2) reasonable security and limited retention for consumer data; (3) affirmative express consent for material retroactive changes to privacy policies; and (4) affirmative express consent for the use of sensitive data.[37] This report prompted industry to launch a number of self-regulatory initiatives, including the development of new codes of conduct and online tools to allow consumers more control over the receipt of targeted advertising. As discussed further below, these efforts have not yet been fully implemented and their effectiveness has yet to be demonstrated.

The Commission also has focused on privacy and technology issues as they affect children and teens. In 2010, the Commission hosted a workshop to examine the impact of technological innovation on children's privacy in connection with its review of COPPA and its implementing Rule, which the Commission enforces.[38] The COPPA statute and Rule require website operators to provide notice to, and receive explicit

[32] *See OnGuard Online, supra* note 13. Since its launch in 2005, OnGuard Online and its Spanish-language counterpart Alerta en Lnea have attracted nearly 14 million unique visits.

[33] *See Protecting Personal Information: A Guide for Business, supra note 13.*

[34] *See FTC, Peer-to-Peer File Sharing: A Guide For Business,* `http://business.ftc.gov/documents/bus46-peer-peer-file-sharing-guide-business`. In February 2010, the Commission informed nearly 100 companies that sensitive personal data from their networks had been shared and was available on peer-to-peer networks, where it could be used to commit identity theft or fraud. *See* Press Release, FTC, Widespread Data Breaches Uncovered by FTC Probe (Feb. 22, 2010), `http://www.ftc.gov/opa/2010/02/p2palert.shtm`. The Commission sent business education materials to those businesses explaining how to secure any peer to peer programs on their systems.

[35] *See* OnGuardonline.gov Off to a Fast Start with Online Child Safety Campaign, *supra* note 13.

[36] *See FTC Public Workshops, supra* note 11.

[37] FTC Staff, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* (2009) [hereinafter *OBA Report*], `http://www.ftc.gov/os/2009/02/P0085400behavadreport.pdf`.

[38] *See FTC Roundtable: Protecting Kids' Privacy Online* (June 2, 2010), FTC, `http://www.ftc.gov/bcp/workshops/coppa/index.shtml`. The COPPA roundtable followed the Commission's Federal Register notice calling for public comment on whether technological changes warranted changes to the Commissions implementation of COPPA. *See* Request for Public Comment on the Federal Trade Commissions Implementation of the Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2010), *available at* `http://www.ftc.gov/os/fedreg/2010/april/P104503coppa-rule.pdf`.

consent from, parents of children under age 13 prior to the collection, use, or disclosure of such children's personal information on web sites or online services. With changes in technology—such as the increased use of smartphones to access the Internet—the Commission is exploring whether an update to the Rule is warranted. At the workshop, participants examined, among other things, whether the Rule should apply to emerging media, including mobile devices, interactive television, and interactive gaming; whether the Rule's definition of personally identifiable information should be expanded; and whether technological advances dictate changes to the methods for verification of parental consent. The Commission will announce the results of its review in the coming months.

With respect to teens, the Commission recently testified before Congress on whether COPPA should be expanded to cover children between the ages of 13 and 17.[39] The Commission recognized the fact that teens are heavy users of digital technology and new media applications but also noted concerns that teens may not be fully aware of the consequences of what they do.[40] As a result, teens may voluntarily disclose more information than they should, which could leave them vulnerable to identity theft or adversely affect future opportunities, such as employment. While acknowledging these concerns, the Commission noted difficulties in applying COPPA to teens citing, among other things, the potential ineffectiveness of relying on teens to provide accurate information about their age, and the ability of teens to access the Internet outside their homes, such as at libraries and friends' homes, without their parents' supervision.

2.2.4 International Activities

International enforcement and policy cooperation also has become more important with the proliferation of complex cross-border data flows and cloud computing. To protect consumers in this rapidly changing environment, the FTC participates in various international policy initiatives, including those in multilateral organizations such as the OECD and the Asia-Pacific Economic Cooperation forum ("APEC").

Within the OECD, the FTC has participated in the Working Party on Information Security and Privacy, which led the development of the 2007 OECD Council's Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (the "Recommendation").[41] In APEC, the FTC has been actively involved in an initiative to establish a self-regulatory framework governing the privacy of data transfers throughout the APEC region.[42]

[39] *See Protecting Youths in an Online World: Hearing Before the Subcomm. on Consumer Prot., Prod. Safety, and Ins. of the S. Comm. on Commerce, Sci., and Transp.*, 111th Cong. (July 15, 2010) (prepared statement of the FTC), available at `http://www.ftc.gov/os/testimony/100715toopatestimony.pdf`.

[40] *Id.* at 3.

[41] The Recommendation provided that OECD member countries should foster the establishment of an informal network of privacy enforcement authorities and should cooperate with each other to address cross-boarder issues arising from enforcement of privacy laws. *See* OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, `http://www.oecd.org/document/14/0,3343,en_2649_34255_38771516_1_1_1_1,00.html`.

[42] The FTC recently became one of the first participants in the APEC Cross-Border Privacy Enforce-

The Commission also is using its expanded powers under the U.S. SAFE WEB Act of 2006 to cooperate with foreign counterparts on cross-border law enforcement actions, including in the privacy area.[43] In addition, recognizing the need for expanded international cooperation in enforcing privacy laws, the Commission, joined by a number of its international counterparts, launched the Global Privacy Enforcement Network ("GPEN") in March of 2010.[44] GPEN, a network of privacy enforcement agencies across the globe, is designed to facilitate cooperation among its members. Further, the Commission has brought a number of cases relating to the U.S.-EU Safe Harbor Framework, a self-regulatory program that enables U.S. companies that abide by certain privacy principles to transfer personal data from Europe to the United States, consistent with European privacy law.[45]

In recognition of the Commission's role in protecting consumer privacy, the FTC was recently admitted as a full member of the International Data Protection Commissioners' Conference.[46]

3 Re-examination of the Commission's Privacy Approach

The FTC's experience with consumer privacy issues, including its use of different enforcement models and its ongoing examination of new technologies, led to the Commission's decision to re-examine privacy through the roundtables series. Among other things, Commission staff recognized certain limitations in the notice-and-choice and harm-based models. It also questioned whether these models were keeping pace with the rapid growth of technologies and business models that allow companies to collect and use consumers' information in new ways.

---

ment Arrangement, a multilateral cooperation network for APEC privacy enforcement authorities. *See* Press Release, FTC, FTC Joins New Asia-Pacific Multinational Network of Privacy Enforcement Authorities (July 19, 2010), `http://www.ftc.gov/opa/2010/07/apec.shtm`.

[43]Pub. L. No. 109-455, 120 Stat. 3372 (2006) (codified at 12 U.S.C. § 3412(e) and scattered sections of 15 U.S.C.).

[44]*See* Press Release, FTC, FTC and International Privacy Enforcement Authorities Launch Global Privacy Cooperation Network and Website (Sept. 21, 2010), `http://www.ftc.gov/opa/2010/09/worldprivacy.shtm` (unveiling the organization's public website); Press Release, GPEN, Global Privacy Enforcement Network Launches Website (Sept. 21, 2010), `http://www.privacyenforcement.net`.

[45]In these cases, the Commission alleged that companies falsely claimed to be part of the Safe Harbor Framework when their self-certifications had, in fact, lapsed. The consent orders against six of the companies prohibit them from misrepresenting their participation in any privacy, security, or other compliance program. *See In re Dirs. Desk LLC*, No. C-4281, 2010 WL 326896 (F.T.C. Jan. 12, 2010) (consent order); *In re World Innovators, Inc.*, No. C-4282, 2010 WL 326892 (F.T.C. Jan. 12, 2010) (consent order); *In re Collectify LLC*, No. C-4272, 2009 WL 5576194 (F.T.C. Nov. 9, 2009) (consent order); *In re ExpatEdge Partners, LLC*, No. C-4269, 2009 WL 5576191 (F.T.C. Nov. 9, 2009) (consent order); *In re Onyx Graphics, Inc.*, No. C-4270 2009 WL 5576192 (F.T.C. Nov. 9, 2009) (consent order); *In re Progressive Gaitways LLC*, No. C-4271, 2009 WL 5576193 (F.T.C. Nov. 9, 2009) (consent order). A seventh case is still in litigation. *See FTC v. Karnani*, No. 09-CV-5276 (C.D. Cal. filed July 31, 2009), *available at* `http://www.ftc.gov/os/caselist/0923081/090806karnanicmpt.pdf`.

3.1 Limitations of the FTC's Existing Privacy Models

In recent years, the limitations of the notice-and-choice model have become increasingly apparent. Privacy policies have become longer, more complex, and, in too many instances, incomprehensible to consumers. Too often, privacy policies appear designed more to limit companies' liability than to inform consumers about how their information will be used. Moreover, while many companies disclose their practices, a smaller number actually offer consumers the ability to control these practices. Consequently, consumers face a substantial burden in reading and understanding privacy policies and exercising the limited choices offered to them.[47] This difficulty is illustrated by the recent Sears case, in which the Commission charged that the company's buried disclosures were inadequate to inform consumers about its data collection practices. Additionally, the emphasis on notice and choice alone has not sufficiently accounted for other widely recognized fair information practices, such as access, collection limitation, purpose specification, and assuring data quality and integrity.

The FTC's harm-based approach also has limitations. In general, it focuses on a narrow set of privacy-related harms—those that cause physical or economic injury or unwarranted intrusion into consumers' daily lives. But, for some consumers, the actual range of privacy-related harms is much wider and includes reputational harm, as well as the fear of being monitored or simply having private information "out there."[48] Consumers may feel harmed when their personal information particularly sensitive health or financial information is collected, used, or shared without their knowledge or consent or in a manner that is contrary to their expectations.[49] For instance, the Commission's online behavioral advertising work has highlighted consumers' discomfort with the tracking of their online searches and browsing activities, which they believe to be private.

3.2 Technological Changes and New Business Models

Changes in technology and the emergence of new business models also have new implications for consumer privacy. For example, technological advancements and increased

[46] Edouard Goodman, *America Joins the Global Privacy Club*, Creditbloggers (Nov. 17, 2010), `http://www.credit.com/blog/2010/11/america-joins-the-global-privacy-club`; *Live Coverage from Jerusalem: FTC Admitted as a Member of the International Group of Data Protection Commissioners*, Hunton & Williams Privacy and Information Security Law Blog (Oct. 29, 2010), `http://www.huntonprivacyblog.com/2010/10/articles/enforcement-1/live-coverage-from-jerusalem-ftc-admitted-as-a-member-of-the-international-group-of-data-protection-commissioners/`.

[47] *See* Felicia Williams, *Internet Privacy Policies: A Composite Index for Measuring Compliance to the Fair Information Principles* 17-18 (2006), *available at* (examined privacy policies of Fortune 500 companies; found that only one percent of the privacy policies were understandable for those with a high school education or less and thirty percent required a post-graduate education to be fully understood).

[48] As discussed below, this concern is heightened by the myriad ways in which information is collected, combined, and used without consumers' knowledge.

[49] Fordham University School of Law Professor Joel Reidenberg has characterized the "misuse of personal information" as a "significant privacy wrong. When data is collected for one purpose and then treated differently, the failure to respect the original expectation constitutes a cognizable harm." Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 Hastings L.J. 877, 881 (2003).

computing power have allowed companies to collect, store, manipulate, and share ever-increasing amounts of consumer data at very little cost. This has led to an explosion of new business models that depend upon capturing consumer data at a specific and individual level and over time, including online behavioral advertising, social media services, and location-based mobile services.[50] The effects of this trend have not been confined to the online environment; technological advances also have enabled traditionally offline businesses, such as brick-and-mortar retailers and information brokers, to access, aggregate, and process vast amounts of consumer data. As described further below, many of these activities are invisible to consumers.

These developments can provide enormous benefits to consumers, including instant, around-the-clock access to products and services, more choices, lower prices, personalized content, and the ability to communicate and interact with family, friends, and colleagues located around the globe. Consumers are using these new products and services at remarkable rates. The growth in mobile and social networking services in particular is striking, and is funded, in part, by the growth of targeted advertising that relies on use of consumer data. At the same time, the enhanced ability to collect and store consumer data has increased the risks that data will be shared more broadly than understood or intended by consumers or used for purposes not contemplated or disclosed at the time of collection.

4 Privacy Roundtables

4.1 Description

In light of these considerations, in September 2009, Commission staff announced a series of three public roundtables to explore the effectiveness of current privacy approaches in addressing the challenges of the rapidly evolving market for consumer data. To better frame the issues and guide the discussions, staff published a number of questions in advance of each roundtable and requested comments from stakeholders.[51] The Commission received a total of 116 submissions, which included responses to the questions as well as original research papers and studies relevant to the issues.[52]

The roundtables generated significant public participation from industry representatives, academics, technologists, consumer and privacy advocates, and government officials. Hundreds of interested parties attended the event, with many more accessing the webcasts, and 94 panelists participated in the discussions.

[50] Electronic collection and compilation of data poses different and more substantial privacy risks than collection of information regarding a discrete incident, because it offers the ability to obtain an intimate picture of an individual's life. *See United States v. Maynard*, 615 F.3d 544, 556-64 (D.C. Cir. 2010).

[51] *See FTC, Exploring Privacy—A Roundtable Series, supra* note 4.

[52] The public comments filed in connection with the privacy roundtables are available online. See FTC, *Roundtables to Address Evolving Consumer Privacy Issues: Public Comments* [hereinafter *Written Comment*], `http://www.ftc.gov/os/comments/privacyroundtable/index.shtm`.

4.2 Major Themes and Concepts from the Roundtables

Several recurring themes emerged from the roundtable series. Set forth below is a summary of the major concepts from the comments and roundtable discussions.

4.2.1 Increased Collection and Use of Consumer Data

Commenters and roundtable panelists addressed the increasing collection and use of consumer data and the extent to which multiple, diverse entities gather, maintain, and share the data for a vast array of purposes.[53] For example, the presentation by technologist Richard Smith on the "personal data ecosystem" during the first roundtable highlighted the immense scope of current data collection and use. The presentation outlined the virtually ubiquitous collection of consumer data that occurs in multiple contexts and at numerous points throughout a given day—for instance, when consumers browse websites, purchase items with payment cards, or use a geolocation application on a mobile device. In addition, the presentation depicted how companies that collect data through such activities share the data with multiple entities, including affiliated companies, as well as third parties that are many layers removed from, and typically do not interact with, consumers.[54]

Participants cited a number of factors that have led to this increased collection and use of consumer data. These include the enormous growth in data processing and storage capabilities, advances in online profiling, and the aggregation of information from online and offline sources.[55] In addition, participants discussed how economic incentives drive the collection and use of more and more information about consumers.[56] For example, the more information that is known about a consumer, the more a company will pay to

[53] *See, e.g.*, Leslie Harris, *Written Comment of Center for Democracy & Technology*, cmt. #544506-00026, at 9; *see also* FTC, *Transcript of December 7, 2009, Privacy Roundtable, Remarks of Leslie Harris, Center for Democracy & Technology*, at 36-38 [hereinafter *1st Roundtable*], `http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Dec2009_Transcript.pdf`; FTC, *Transcript of January 28, 2010, Privacy Roundtable, Remarks of Nicole Ozer, American Civil Liberties Union ("ACLU") of Northern California*, at 193-94 [hereinafter *2nd Roundtable*], `http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Jan2010_Transcript.pdf`; FTC, *Transcript of March 17, 2010, Privacy Roundtable, Remarks of Deven McGraw, Center for Democracy & Technology*, at 119-21 [hereinafter *3rd Roundtable*], `http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_March2010_Transcript.pdf`.

[54] *See 1st Roundtable, Remarks of Richard Smith*, at 16-27 (Smith also presented a "Personal Data Ecosystem" chart which is attached to this report as Appendix C); *see also* Julia Angwin & Tom McGinty, *Sites Feed Personal Details to New Tracking Industry*, Wall St. J., July 30, 2010, *available at* `http://online.wsj.com/article/SB10001424052748703977004575393173432219064.html` (discussing a *Wall Street Journal* study that found that the 50 largest U.S. websites on average installed 64 tracking devices onto the computers of visitors, usually with no warning; a dozen such sites each installed over 100 pieces of tracking technology).

deliver a precisely-targeted advertisement to him.[57]

Many participants expressed concern that this growth in data collection and use was occurring without adequate concern for consumer privacy. They stated that these activities frequently are invisible to consumers and thus beyond their control. (See also Section 4.2.2, below). Others raised concerns that the increase in low-cost data storage capability will lead companies to retain the data they collect indefinitely, which creates the incentives and opportunity to find new uses for it.[58] As a result, consumers' data may be subject to future uses that were not disclosed—and may not even have been contemplated at the time of collection.[59] Some participants stated that companies should address this concern by incorporating privacy protection measures into their everyday business practices—for example, collecting data only if there is a legitimate need to do so and implementing reasonable data retention periods.[60]

4.2.2 Lack of Understanding Undermines Informed Consent

Another major theme that emerged from the roundtables was consumers' lack of understanding about the collection and use of their personal data, and the corresponding inability to make informed choices. As noted above, many data collection and use practices are invisible to consumers. Participants stated that, because of this, consumers often are unaware of when their data is being collected or for what purposes it will be used.[61] Adding to this confusion is the lack of clarity in the terminology companies

[55] *See* Williams, *supra* note 47, at 49; *see also Written Comment of Center for Digital Democracy and U.S. PIRG*, cmt. #544506-00013, at 2; Pam Dixon, *Written Comment of World Privacy Forum*, cmt. #544506-00024, at 10-11 (discussing the volume of profiling data and the merging of offline and online data sources).

[56] *See, e.g., 1st Roundtable, Remarks of Joel Kelsey, Consumers Union*, at 119; *2nd Roundtable, Remarks of Nicole Ozer, ACLU of Northern California*, at 186-87.

[57] See Berin Szoka, *Written Comment of The Progress & Freedom Foundation*, cmt. #544506-00035, at 4-5 (describing greater rates publishers can charge for more targeted advertisements); *Written Comment of Network Advertising Initiative*, cmt. #544506-00117 (submitting J. Howard Beales, III, *The Value of Behavioral Targeting*) (report sponsored by the Network Advertising Initiative).

Consumer groups recently filed a complaint with the FTC discussing the practice of conducting realtime online auctions to micro-target ads to consumers without their knowledge. The complaint alleges the existence of a "vast ecosystem of online advertising data auctions and exchanges, demand and supply-side platforms, and the increasing use of third-party data providers that bring offline information to online profiling and targeting." The complaint further alleges that these businesses operate without the awareness or consent of users. The result, the complaint claims, is the creation of consumer profiles that can be used for purposes other than serving targeted advertisements that consumers may not expect or want. *See* Complaint, Request for Investigation, Injunction, and Other Relief of Center for Digital Democracy, U.S. PIRG, and World Privacy Forum, In the Matter of Real-time Targeting and Auctioning, Data Profiling Optimization, and Economic Loss to Consumers and Privacy (2010), *available at* `http://www.uspirg.org/uploads/eb/6c/eb6c038a1fb114be75ecabab05b4b90b/FTCfiling_Apr7_10.pdf`. *See also* Angwin & McGinty, *supra* note 54 (discussing realtime online auctions for detailed information about a Web surfer's activity).

[58] *See, e.g., 2nd Roundtable, Remarks of Nicole Ozer, ACLU of Northern California, at* 186.

[59] *See, e.g.*, Miyo Yamashita, *Written Comment of Anzen Consulting*, cmt. #544506-00032, at 12; Pam Dixon, *Written Comment of World Privacy Forum*, cmt. #544506-00024, at 3; *see also 1st Roundtable, Remarks of Leslie Harris, Center for Democracy & Technology*, at 36-37.

[60] *See, e.g.*, Kristin Van Dillen, *Written Comment of The Business Forum for Consumer Privacy*, cmt. #544506-00058, at 16.

employ to discuss their data collection and use practices. Indeed, one survey shows that consumers believe the term "privacy policy" on a website means that the site protects their privacy.[62]

In addition, commenters noted that consumers often do not understand the extent to which their data is shared with third parties. For instance, consumers may not appreciate that when a company discloses that it shares information with "affiliates," the company could have hundreds of affiliates.[63] Also, consumers may not be aware that third parties combine their data with additional information obtained from other sources. This practice further undercuts consumers' understanding and, to the extent choices are offered, their ability to exercise control.

Through its notice-and-choice approach, the FTC attempted to promote transparency for these otherwise invisible practices. As developed, however, privacy policies have become long and incomprehensible, placing too high a burden on consumers to read, understand, and then exercise meaningful choices based on them.[64] This challenge increases where consumers are expected to interrupt an ongoing transaction to locate and click on a privacy policy link to obtain relevant information. It is unlikely that busy consumers, intent on buying a product or service, will consider how the data they provide to complete the transaction will be shared and used for other purposes, potentially at a later date.

Participants also noted that even when consumers locate privacy policies, they cannot understand them or the choices they provide. Further, overloading privacy policies with too much detail can confuse consumers or cause them to ignore the policies altogether.[65]

---

[61] *See, e.g., 3rd Roundtable, Remarks of Kathryn Montgomery, American University School of Communication*, at 200-01; *2nd Roundtable, Remarks of Kevin Bankston, Electronic Frontier Foundation*, at 277.

[62] *See 1st Roundtable, Remarks of Joseph Turow, University of Pennsylvania*, at 126 (citing surveys showing that most respondents believe incorrectly that the existence of a privacy policy means that a company protects privacy by not sharing consumer information); *see also Written Comment of Lorrie Faith Cranor, Timing is Everything? The Efforts of Timing and Placement of Online Privacy Indicators*, cmt. #544506-00039, at 2 ("[m]any Internet users erroneously believe that websites with seals have adopted consumer-friendly privacy practices.").

[63] *See, e.g., 3rd Roundtable, Remarks of Chris Jay Hoofnagle, University of California, Berkeley School of Law*, at 291-92; *see also* Joshua Gomez, Travis Pinnick & Ashkan Soltani, *KnowPrivacy* (UC Berkeley, School of Information, 2009), *available at* `http://knowprivacy.org/report/KnowPrivacy_Final_Report.pdf`.

[64] *See, e.g, 1st Roundtable, Remarks of Fred Cate, Indiana University Maurer School of Law*, at 280-81; see also Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print?: Testing a Law and Economics Approach to Standard Form Contracts* (CELS 2009 4th Annual Conference on Empirical Legal Studies Paper, NYU Law and Economics Research, Paper No. 09-40 2009) (Oct. 6, 2009) (showing that few retail software shoppers access and read standard license agreements), *available at* `http://ssrn.com/abstract=1443256`; Williams, *supra* note 47, at 17 (examined privacy policies of Fortune 500 companies and found that only one percent of the privacy policies were understandable for those with a high school education or less and thirty percent required a postgraduate education to be fully understood).

[65] *See, e.g., 1st Roundtable, Remarks of Lorrie Cranor, Carnegie Mellon University*, at 129; *see also Written Comment of Fred Cate, Consumer Protection in the Age of the 'Information Economy,'* cmt. #544506-00057, at 343-79. Even the Chief Justice of the United States Supreme Court admitted that

Panelists discussed ways to address this problem. Most notably, they suggested simplifying consumers' ability to exercise choices about their privacy.[66] In addition, panelists suggested improving the transparency of privacy practices by, for example, developing standardized privacy notices and increasing consumer education efforts.[67]

4.2.3 Consumer Interest in Privacy

A number of roundtable participants cited evidence that, notwithstanding consumers' lack of understanding about how companies collect and use consumer data, consumers care about their privacy. For example, a representative from the social networking service Facebook noted that a significant percentage of the company's users chose to revise their account settings when Facebook released new privacy controls in December of 2009.[68] In addition, another participant pointed to the large number of Mozilla Firefox users who have downloaded NoScript, a privacy and security-enhancing tool that blocks Javascript commands.[69] Other popular privacy mechanisms include the Targeted Advertising Cookie Opt-Out tool ("TACO"), which allows consumers to prevent online advertising networks from serving targeted ads based on web browsing activities, and PrivacyChoice, which allows consumers to manage privacy choices for online marketing.[70] One panelist also discussed how consumers often try to protect their anonymity by providing false information about themselves or deleting cookies from their computers.[71]

Such actions suggest that significant numbers of consumers care enough about their privacy that, when given the opportunity, they will take active steps to protect it. Whether consumers take such steps, however, may depend on the nature of the information and how easily those steps are understood. For example, someone who takes the time to change his settings on a social networking site, or check that his online shopping is secure, may not be willing to devote comparable time and effort to figure out how to protect his online browsing activity, which may expose details of online purchases or

---

he does not read fine-print terms of service disclosures on websites. *See* Mike Masnick, *Supreme Court Chief Justice Admits He Doesnt Read Online EULAS or Other "Fine Print,"* Techdirt (Oct. 22, 2010 9:48 AM), `http://www.techdirt.com/articles/20101021/02145811519/supreme-court-chief-justice-admits-he-doesn-t-read-online-eulas-or-other-fine-print.shtml`.

[66] *See, e.g., 1st Roundtable, Remarks of Marc Rotenberg, Electronic Privacy Information Center*, at 322.

[67] *See Written Comment of Lorrie Faith Cranor, Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach*, cmt. #544506-00037, at 1-2 (describing the "nutrition label approach" to privacy notices); *see also 1st Roundtable, Remarks of Joel Kelsey, Consumers Union*, at 135-36.

[68] *See 2nd Roundtable, Remarks of Tim Sparapani, Facebook*, at 121-23 (indicating that almost 35% of Facebook's 350 million users customized their settings).

[69] *See 1st Roundtable, Remarks of Adam Thierer, The Progress & Freedom Foundation*, at 122. As of November 29, 2010, there were over 77,000,000 downloads of NoScript. *See* Giorgio Maone, *NoScript 2.0.3.5*, Add-ons for Firefox, `https://addons.mozilla.org/en-US/firefox/addon/722/`.

[70] As of November 29, 2010, TACO had been downloaded more than 820,000 times by Mozilla Firefox users while over 250,000 consumers had used PrivacyChoice to set their privacy preferences. *See* Abine, *Targeted Advertising Cookie Opt-Out (TACO)*, Add-ons for Firefox, `https://addons.mozilla.org/en-US/firefox/addon/11073/`; *see also The Easiest Way to Choose Privacy*, `http://www.privacychoice.org/`.

[71] *See 1st Roundtable, Remarks of Joel Kelsey, Consumers Union*, at 106.

web surfing, even if he would prefer to keep those purchase details private.

Consumer survey data discussed during roundtable panels and in comments also evidences consumer interest in privacy.[72] For instance, consumer surveys have shown that a majority of consumers are uncomfortable with being tracked online, although the surveys provide little or no information about the degree of such discomfort or the proportion of consumers who would be willing to forego the benefits of targeted advertising to avoid being tracked.[73] In addition, the public outcry and backlash in response to the rollout of new services, such as Facebook Beacon and Google's social networking service "Buzz," further evidence consumer interest in the privacy of their information.[74]

The special concerns raised by sensitive data and sensitive users such as children was a recurring theme among panelists. For example, one panelist noted that some consumers refuse to seek early treatment for cancer for fear that information about their condition will be disclosed.[75] Another panelist and commenter cited a *Wall Street Journal* article indicating that some data brokers maintain lists of elderly patients who suffer from Alzheimer's disease and similar maladies as "perfect prospects for holistic remedies, financial services, subscriptions and insurance."[76] Another panelist remarked that HIV status is almost always extremely sensitive and is extremely damaging if disclosed.[77]

---

[72] Staff recognizes that consumer survey evidence, by itself, has limitations. For instance, the way questions are presented may affect survey results. Also, while survey evidence may reveal a consumer's stated attitudes about privacy, survey evidence does not necessarily reveal what actions a consumer will take in real-world situations. Commission staff welcomes additional academic contributions in this area.

[73] *See, e.g., 1st Roundtable, Remarks of Alan Westin, Columbia University, at 93-94; Written Comment of Berkeley Center for Law & Technology, Americans Reject Tailored Advertising and Three Activities that Enable It*, cmt. #544506-00113, at 3; *Written Comment of Craig Wills & Mihajlo Zeljkovic, A Personalized Approach to Web Privacy Awareness, Attitudes and Actions*, cmt. #544506-00119, at 1; *Written Comment of Alan Westin, How Online Users Feel About Behavioral Marketing and How Adoption of Privacy and Security Policies Could Affect Their Feelings*, cmt. #544506-00052, at 3; *see also Press Release*, Consumer Reports, Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy (Sept. 25, 2008), `http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html`.

One laboratory study demonstrates that consumers are willing to pay more to shop at websites that have better privacy policies. Serge Egelman, Janice Tsai, Lorrie Faith Cranor & Alessandro Acquisti, *Timing is Everything? The Effects of Timing and Placement of Online Privacy Indicators, available at* `http://www.guanotronic.com/~serge/papers/chi09a.pdf`. Although the study included only consumers who stated they had privacy concerns about shopping online, it showed that these consumers were willing to pay more for privacy.

[74] *See, e.g.*, Brad Stone, *Facebook Executive Discusses Beacon Brouhaha*, N.Y. Times, Nov. 29, 2007, *available at* `http://bits.blogs.nytimes.com/2007/11/29/facebook-responds-to-beacon-brouhaha/`; *see also* Miguel Helft, *Critics Say Google Invades Privacy with New Service*, N.Y. Times, Feb. 12, 2010, *available at* `http://www.nytimes.com/2010/02/13/technology/internet/13google.html`.

[75] *See 3rd Roundtable, Remarks of Deborah Peel, Patient Privacy Rights*, at 126.

[76] *See Written Comment of Chris Jay Hoofnagle, University of California, Berkeley School of Law*, cmt. #544506-00012, at 5 (quoting Karen Blumenthal, *How Banks, Marketers Aid Scams*, Wall St. J., July 1, 2009).

[77] *See 3rd Roundtable, Remarks of Lior Jacob Strahilevitz, University of Chicago School of Law*, at 178.

At the same time, panelists discussed the fact that disagreement exists regarding the sensitivity of certain classes of data and certain users. For instance, can personal data that a user posts on a social networking site be sensitive? Further, some participants argued strongly that teens should be considered sensitive users because they often act impulsively and do not appreciate the consequences of their actions.[78] Because of the difficulty in determining whether certain data is "sensitive," some panelists supported substantive protections for all data rather than special protections only for sensitive data.[79]

Finally, several participants indicated that the FTC's harm-based approach is too narrow to fully address consumers' privacy interests.[80] They called on the Commission to support a more expansive view of privacy harm that takes into account reputational and other intangible privacy interests.[81] For example, one panelist noted that a consumer simply may not want information about his medical condition to be available to third-party marketers.[82] Another noted that the disclosure of a consumer's health or other sensitive information could lead to embarrassment, stigmatization, or simply needing to explain oneself.[83] Other panelists cited privacy harms such as the chilling effect that monitoring might have on consumers' willingness to participate in certain activities or research certain topics online;[84] and the offer of different media content, or different prices for products and services, based upon what companies know or infer about individual consumers.[85] New types of harm may also emerge as technology develops. For example, a consumer who "walks away" from a social networking site because of privacy concerns loses the time and effort invested in building a profile and connecting with friends.

In addition, others have criticized the Commission's harm-based model for being too reactive.[86] The success of the harm-based model depends upon the ability to identify and remedy harm. However, consumers may not know when they have suffered harm or the risk of harm. By their nature, privacy harms are often hidden from view. For example, consumers ordinarily will be unaware that their data has been disclosed or sold without their knowledge or consent. Further, even if they become aware, it can be challenging to identify the responsible party.[87] It also is often difficult to provide restitution to injured consumers, particularly if the harm involves non-monetary injury. Thus, some have argued that a more systemic approach to consumer privacy issues is

[78] *See, e.g., 3rd Roundtable, Remarks of Lee Peeler, National Advertising Review Council*, at 186; *3rd Roundtable, Remarks of Kathryn Montgomery, American University School of Law*, at 211-12.

[79] *See, e.g., 3rd Roundtable, Remarks of Parry Aftab, WiredTrust*, at 227.

[80] Some panelists noted, however, that the FTC's harm-based approach to privacy is capable of broad application. *See, e.g., 1st Roundtable, Remarks of J. Howard Beales III, George Washington University, at 296-97.*

[81] *See, e.g., Written Comment of Center for Democracy & Technology*, cmt. #544506-00026, at 7; *Written Comment of Electronic Frontier Foundation*, cmt. #544506-00047, at 1.

[82] *See 1st Roundtable, Remarks of Marc Rotenberg, Electronic Privacy Information Center*, at 301.

[83] *See, e.g., 1st Roundtable, Remarks of Leslie Harris, Center for Democracy & Technology*, at 36-38.

[84] *See, e.g., 1st Roundtable, Remarks of Susan Grant, Consumer Federation of America*, at 38-39.

[85] *See, e.g., 1st Roundtable, Remarks of Joseph Turow, University of Pennsylvania*, at 141-42; *1st Roundtable, Remarks of Jeff Chester, Center for Digital Democracy*, at 173-77. *See* Complaint, Request for Investigation, Injunction, and Other Relief of Center for Digital Democracy, U.S. PIRG, and World Privacy Forum, supra note 57.

warranted.[88]

4.2.4 Benefits of Data Collection and Use

Another recurring theme from the roundtables was that the increasing flow of information provides important benefits to consumers and businesses. In particular, panelists discussed benefits specific to business models such as online search, online behavioral advertising, social networking, cloud computing, mobile technologies, and health services. Participants noted that search engines provide consumers with instant access to large amounts of information at no charge to the consumer.[89] Online advertising helps to support much of the content available to consumers online and allows personalized advertising that many consumers value.[90] Social networking services permit users to connect with friends and share experiences online, in real time. These platforms also facilitate broader types of civic engagement on political and social issues.[91]

Benefits associated with enterprises moving to cloud computing include cost savings for businesses, as well as positive environmental impacts because of the energy-saving effects of server consolidation.[92] Mobile device applications give consumers location-specific search results, access to information about local events, and more timely delivery of sales offers.[93] Finally, the disclosure and use of personal health information has facilitated advances in medical research.[94]

---

[86] George Washington University Law School Professor Daniel Solove has criticized the harm-based approach for being too "reactive" and called for an architectural approach to protecting privacy that involves "creating structures to prevent harms from arising rather than merely providing remedies when harms occur." Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 Hastings L.J. 1227, 1232-45 (2003).

[87] *See, e.g., Written Comment of Electronic Frontier Foundation*, cmt. #544506-00047, at 7.

[88] *See* Solove, *supra* note 86.

[89] *See, e.g., 1st Roundtable, Remarks of Michael Hintze, Microsoft Corp.*, at 44; *Written Comment of Technology Policy Institute*, cmt. #544506-00011, at 18-19. One consumer representative stated that consumers in fact "pay" for these services with their data. *See 1st Roundtable, Remarks of Susan Grant, Consumer Federation of America*, at 38-39 (noting that consumers should not have to trade their privacy to use things like search tools). Another roundtable participant noted, however, that new business models offer benefits that consumers want, and these benefits should be balanced with privacy interests. *See 1st Roundtable, Remarks of Berin Szoka, The Progress & Freedom Foundation*, at 167-68 (recognizing a trade-off between privacy and free content and suggesting that educated consumers can make choices about whether to engage in behavioral advertising or to pay for content or services).

[90] *See Written Comment of Microsoft Corp.*, cmt. #544506-00020, at 1 (stating that online advertising is the engine that drives the Internet economy, allowing thousands of websites to offer their content and services for free); *Written Comment of The Progress & Freedom Foundation*, cmt. #544506-00035, at 1, 5 (noting that tailored advertising offers significant benefits to users, including funding for content and services, improved information about products, and increased innovation); *Written Comment of Technology Policy Institute*, cmt. #544506-00011, at 2-4 (stating that targeted advertising gives consumers useful information and provides revenue that allows companies to develop innovative new services).

[91] *See, e.g., 2nd Roundtable, Remarks of Nicole Wong, Google*, at 107.

[92] *See, e.g., 2nd Roundtable, Remarks of Harriet Pearson, IBM*, at 216-17.

[93] *See, e.g., 2nd Roundtable, Remarks of Brian Knapp, Loopt*, at 263.

[94] *See, e.g., 3rd Roundtable, Remarks of Kimberly Gray, Americas Regions, IMS Health*, at 150-51.

To preserve the consumer benefits made possible through the flow of information, commenters and participants urged regulators to be circumspect and cautious about restricting the exchange and use of consumer data.[95] Panelists also argued for a flexible approach to privacy protection in order to allow companies to innovate in the area of privacy-enhancing technologies. Industry representatives argued that overly prescriptive regulations impair the ability of businesses to develop privacy solutions for consumers at the product level. These participants urged the FTC to maintain its flexible, technology-neutral approach in this area.[96]

4.2.5 Decreasing Relevance of Distinction Between PII and Non-PII

Finally, roundtable discussions addressed the diminishing distinction between personally identifiable information ("PII")—e.g., name, address, Social Security number—and supposedly anonymous or de-identified information ("non-PII"). Panelists representing industry, as well as academics and privacy advocates, acknowledged that the traditional distinction between the two categories of data has eroded and that information practices and restrictions that rely on this distinction are losing their relevance.[97]

Several factors have contributed to the breakdown of this dichotomy. Panelists cited the comprehensive scope of data collection and noted how businesses combine disparate bits of "anonymous" consumer data from numerous different online and offline sources into profiles that can be linked to a specific person.[98] Technological developments also have helped to blur the line between PII and non-PII. For example, using browser "fingerprinting" technology, websites can gather and combine information about a consumer's web browser configuration including the type of operating system used and installed browser plug-ins and fonts—to uniquely identify and track the consumer.[99] In the mobile context, Unique Device Identifiers—the unique serial number assigned to every smart phone—can be combined with location or other information provided to a third party mobile application to track a particular consumer's behavior or real-world

[95] *See, e.g., Written Comment of The Progress & Freedom Foundation*, cmt. #544506-00035, at 7-8.

[96] *See, e.g., 2nd Roundtable, Remarks of Ellen Blackler, AT&T, at 324-25; 2nd Roundtable, Remarks of Peter Cullen, Microsoft Corp., at 338-40; 2nd Roundtable, Remarks of Paul Schwartz, University of California, Berkeley School of Law, at 236.*

For example, some researchers have suggested that prescriptive and inconsistent privacy regulation may impede development and deployment of new health information technologies. See Amalia R. Miller & Catherine E. Tucker, Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records, 55 Mgmt. Sci. 1077 (2009).

[97] *See 3rd Roundtable, Remarks of David Hoffman, Intel*, at 247; *3rd Roundtable, Remarks of Jennifer Stoddart, Office of the Privacy Commissioner of Canada*, at 245-46; *1st Roundtable, Remarks of Alessandro Acquisti, Carnegie Mellon University*, at 40. This issue also was the focus of discussion at the Behavioral Advertising Town Hall and in the FTC Staff Report on Behavioral Advertising. *See OBA Report, supra* note 37.

whereabouts.[100]

Citing the value of personal data to advertisers, panelists discussed the growing incentives to link pieces of data to a particular person or device.[101] Indeed, in the context of behavioral advertising, as noted above, the more information that is known about a consumer, the more a company will pay to deliver a precisely-targeted advertisement to him.[102] Not surprisingly, in recent years, there has been a dramatic increase in the number of companies whose business depends on the collection of increasingly detailed information about consumers.[103]

Panelists discussed that even where companies take steps to "de-identify" data, technological advances and the widespread availability of publicly available information have fundamentally changed the notion of anonymity.[104] To illustrate this point, panelists pointed to incidents in which companies publicly released sets of consumer data that were supposedly "anonymized," only to have researchers and others re-identify the data and associate it with specific individuals. For example, in a 2006 incident involving the public release of data by AOL, the media was able to connect supposedly anonymized search data with particular consumers.[105] Similarly, in 2008, the video rental company Netflix publicly released certain anonymized data about its customers' movie viewing habits so that researchers could improve Netflix's algorithm for recommending films. Despite Netflix's efforts to de-identify the data set, researchers using other publicly available information were able to re-identify specific Netflix customers and associate information about the films they had rented.[106] In light of the increasing ease with which data can be linked to specific individuals, a number of panelists suggested that any data that relates to a person has privacy implications and, therefore, should be

[98] *See, e.g., 2nd Roundtable, Remarks of Scott Taylor, Hewlett-Packard*, at 58; *see also* Michael Barbaro & Tom Zeller, Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. Times, Aug. 9, 2006, *available at* http://www.nytimes.com/2006/08/09/technology/09aol.html.

A recent news report indicates that some businesses are developing services allowing customers to determine the identity of individuals who use pseudonyms to blog or use social networking sites. Julia Angwin & Steve Secklow, 'Scrapers' *Dig Deep for Data on Web*, Wall St. J., Oct. 12, 2010, *available at* http://online.wsj.com/public/page/what-they-know-digital-privacy.html?mod=quicklinks_whattheyknow.

[99] *See 3rd Roundtable, Remarks of Peter Eckersley, Electronic Frontier Foundation*, at 61-62; *see also* Claudine Beaumont, *Internet browsers track web history, warns privacy group*, The Telegraph (May 18, 2010 11:39 AM), http://www.telegraph.co.uk/technology/news/7736016/Internet-browsers-track-web-history-warns-privacy-group.html; Erik Larkin, *Browser Fingerprints: A Big Privacy Threat*, PCWorld (Mar. 26, 2010 9:00 PM), http://www.pcworld.com/article/192648/browser_fingerprints_a_big_privacy_threat.html.

[100] *See* Jacqui Cheng, *iPhone user privacy at risk from apps that transmit personal info*, Ars Technica, http://arstechnica.com/apple/news/2010/10/iphone-user-privacy-at-risk-from-apps-that-transmit-personal-info.ars.

[101] *See, e.g., 3rd Roundtable, Remarks of Richard Purcell, Corporate Privacy Group, at 244; 2nd Roundtable, Remarks of Scott Taylor, Hewlett-Packard*, at 58-59.

[102] *See Written Comment of The Progress & Freedom Foundation and Written Comment of Network Advertising Initiative, supra* note 57.

[103] *See, e.g.*, Emily Steel, *A Web Pioneer Profiles Users by Name*, Wall St. J., Oct. 25, 2010, *available at* http://online.wsj.com/article/SB10001424052702304410504575560243259416072.html (discussing company's sale of consumer profiles that have included information such as Facebook ID number, household income range, age, political leaning, gender, age of children in household as well as interests in religion, adult entertainment, "get rich quick" offers, and other topics).

appropriately protected.[107]

5 Proposed Framework

Drawing on the major themes and concepts developed through the roundtables, as well as the Commission's decades of experience in protecting consumers, Commission staff has developed, and is seeking comment on, a proposed new framework for consumer privacy. The framework is designed to serve as a forward-looking policy vehicle for approaching privacy in light of new practices and business models. However, it incorporates elements that reflect longstanding FTC law. For example, companies that fail to take reasonable steps to ensure the security of consumer data may violate Section 5 of the FTC Act and other laws.[108] Similarly, companies may not unilaterally change their data practices and use previously collected data in ways materially different than those communicated to consumers at the time of collection.[109] Many elements of the framework also parallel those in other federal and state laws, as well as international guidelines and laws governing privacy.[110]

In developing the proposed framework, staff was cognizant of the need to protect consumer privacy interests effectively, while also encouraging the development of innovative new products and services that consumers want. The framework is designed to establish certain common assumptions and bedrock protections on which both consumers and businesses can rely as they engage in commerce.

The framework includes three major elements that are based on discussions from the roundtables. First, to reduce the burden on consumers to seek out and "choose" privacy protective data practices, companies should integrate privacy into their regular

[104] *See, e.g., 2nd Roundtable, Remarks of Arvind Narayanan, Stanford University*, at 55- 56.

[105] *Id. See also* Michael Barbaro and Tom Zeller Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. Times, Aug. 9, 2006, available at `http://www.nytimes.com/2006/08/09/technology/09aol.html`.

[106] *See* Arvind Narayanan & Vitaly Shmatikov, *Robust De-Anonymization of Large Sparse Datasets*, The Univ. of Texas at Austin, `http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf`; *see also* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010); *see also* Letter from Maneesha Mithal, Assoc. Dir., Div. of Privacy and Identity Prot., FTC, to Reed Freeman, Morrison & Foerster LLP, Counsel for Netflix (Mar. 12, 2010), *available at* `http://www.ftc.gov/os/closings/100312netflixletter.pdf` (closing letter).

[107] *See, e.g., 3rd Roundtable, Remarks of Richard Purcell, Corporate Privacy Group*, at 244; *2nd Roundtable, Remarks of Sid Stamm, Mozilla*, at 60-61; *2nd Roundtable, Remarks of Pam Dixon, World Privacy Forum*, at 67-68.

[108] The Commission's Safeguards Rule promulgated under the GLB Act provides data security requirements for financial institutions. *See* 16 C.F.R. § 314 (implementing 15 U.S.C. § 6801(b)). The FCRA requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information, and imposes safe disposal obligations on entities that maintain consumer report information. *See* 15 U.S.C. §§ 1681e, 1681w.

[109] *See, e.g., Gateway Learning Corp.*, No. C-4120, 2004 WL 2618647 (F.T.C. Sept. 10, 2004); *OBA Report, supra* note 37, at 19; *see also In re Orkin Exterminating Co.*, 108 F.T.C. 263 (1986), *aff'd*, 849 F.2d 1354 (11th Cir.).

[110] *See, e.g.*, FCRA; GLB Act; COPPA; CAN-SPAM Act; Do Not Call Rule; *OECD Guidelines, supra* note 14; Directive 95/46/EC, *supra* note 14; PIPEDA, *supra* note 14.

business operations and at every stage of product development. Second, to give consumers meaningful privacy options while preserving beneficial uses of data, companies should provide choices to consumers in a simpler, more streamlined manner than has been used in the past. Thus, businesses should be able to engage in certain "commonly accepted practices" without seeking consumer consent, but should offer consumers clear and prominently disclosed choices for all other data practices. Third, to improve consumer understanding, companies should improve the transparency of all data practices, including those of non-consumer facing businesses.

The framework builds upon the FTC's notice-and-choice and harm-based privacy models while also addressing some of their limitations. For example, although the proposed framework provides for notice and choice, it aims to simplify how companies present such notice and choice and to reduce the degree to which privacy protection depends on them. The framework also takes consumer harm into account by allowing for the scalability of privacy practices based on the sensitivity of data and its intended use.[111]

The basic building blocks of the framework are:

- **Scope:** The framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device.
- **Privacy by Design:** Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services.[112]
  - Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention practices, and data accuracy.
  - Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.
- **Simplified Choice:** Companies should simplify consumer choice.
  - Companies do not need to provide choice before collecting and using consumers' data for commonly accepted practices, such as product fulfillment.
  - For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data.
- **Greater Transparency:** Companies should increase the transparency of their data practices.

[111] As noted, the Commission will also continue to bring enforcement actions against companies engaging in deceptive or unfair practices under the FTC Act—for example, those that make deceptive statements in their privacy policies or unfairly cause injury or reasonable likelihood of injury. In this sense, both the notice-and-choice and harm-based models will continue to inform the Commission's enforcement efforts.

- Privacy notices should be clearer, shorter, and more standardized, to enable better comprehension and comparison of privacy practices.
- Companies should provide consumers with reasonable access to data about themselves; the extent of access should depend on the sensitivity of the data and the nature of its use.
- Companies must provide prominent disclosures and obtain affirmative express consent before using consumer data in a materially different manner than claimed when the data was collected.
- All stakeholders should expand their efforts to educate consumers about commercial data privacy practices.

Commission staff encourages all interested parties to submit written comments to guide further development and refinement of the framework. Once the framework is finalized, Commission staff may conduct surveys or use other benchmarks to evaluate the extent to which industry is implementing the concepts in the framework. Commission staff will also continue to use its authority under Section 5 of the FTC Act, and other statutes it enforces, to investigate privacy or data security practices that may violate such laws.

5.1 Scope: The framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to specific consumer, computer, or other device.

The proposed framework applies broadly to commercial entities that collect, maintain, share, or otherwise use consumer data that can be reasonably linked to a specific consumer, computer, or other device. This proposed scope encompasses two main points. First, the framework would apply to all commercial entities that collect consumer data in both offline and online contexts, regardless of whether such entities interact directly with consumers. This broad scope is supported by the roundtable discussions and comments indicating that consumers are generally unaware of the number of online and offline entities that collect their data, the breadth of the data collected, and the extent to which data is shared with third parties that are often entirely unknown to consumers.

Second, the proposed framework is not limited to those who collect personally identifiable information ("PII"). Rather, it applies to those commercial entities that collect data that can be reasonably linked to a specific consumer, computer, or other device. This concept is supported by a wide cross section of roundtable participants who stated that the traditional distinction between PII and non-PII continues to lose significance due to changes in technology and the ability to re-identify consumers from supposedly anonymous data. Indeed, this standard encompasses a more modern approach that is reflected in recent Commission initiatives.[113]

[112] This is often referred to as Privacy By Design, an approach advocated by Ann Cavoukian, Ph.D., Information and Privacy Commissioner of Ontario. *See supra* note 3.

[113] *See OBA Report, supra* note 37, at 25 (companies should extend behavioral advertising protections

The framework's proposed scope raises a number of issues about which Commission staff seeks comment. One question is whether there are practical considerations that support excluding certain types of companies or businesses from the framework—for example, businesses that collect, maintain, or use a limited amount of non-sensitive consumer data. Another question is whether applying the framework to data that can be "reasonably linked to a specific consumer, computer, or other device" is feasible, particularly with respect to data that, while not currently considered "linkable," may become so in the future. If not feasible, what are some alternatives? Are there reliable methods for determining whether a particular data set is linkable or may become linkable? In addition, Commission staff seeks input on what technical measures exist to more effectively "anonymize" data, and whether industry norms are emerging in this area.

5.2 Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services.

Consistent with roundtable discussions, companies should incorporate substantive privacy and security protections into their everyday business practices and consider privacy issues systemically, at all stages of the design and development of their products and services. Such protections include providing reasonable security for consumer data, collecting only the data needed for a specific business purpose, retaining data only as long as necessary to fulfill that purpose, and implementing reasonable procedures to promote data accuracy. Companies also should implement and enforce procedurally sound privacy practices throughout their organizations. This may include, for example, assigning personnel to oversee privacy issues from the earliest stages of research and development, training employees on privacy, and conducting privacy reviews of new products and services.

These measures will provide consumers with privacy and security protections without forcing them to read long notices to determine whether basic privacy protections are offered. Commission staff notes that many companies already are providing these types of substantive and procedural protections as a matter of good business practice. However, more widespread adoption is needed to ensure adequate protections for consumers.

5.2.1 Companies should incorporate substantive privacy protection into their practices, such as data security, reasonable collection limits, sound retention practices, and data accuracy.

Four substantive protections are of critical importance to consumer privacy. First, companies that maintain information about consumers should employ reasonable safeguards—

to any data that can be reasonably linked to a specific consumer, computer, or other device); Health Breach Notification Rule, 16 C.F.R. § 318 (2009) (requiring entities to provide breach notification to an individual if they have a reasonable basis to believe the data can be linked to that individual).

including physical, technical, and administrative safeguards—to protect that information.[114] The level of security required should depend on the sensitivity of the data, the size and nature of a company's business operations, and the types of risks a company faces. The idea that companies should provide reasonable security for customer and employee data is well-settled. Failure to maintain such security can result in harm to consumers, negative publicity for businesses, and law enforcement action. Indeed, a number of federal and state laws also require this basic protection.[115] To date, the Commission has brought 29 cases against companies that failed to maintain reasonable security to protect customer and employee data.[116]

Recognizing the importance of this issue, many companies have taken positive steps to improve baseline security. Microsoft, for example, has called for data security standards for cloud computing services.[117] Google recently announced that it would use encryption by default for its email service.[118] Commission staff encourages companies to do more in this area.

Second, companies should collect only the information needed to fulfill a specific, legitimate business need. This protection will help ensure that companies give thought to their data collection practices on the front end and do not collect more information than necessary. This is particularly important in light of companies' increased ability to collect, aggregate, and match consumer data and to develop new ways of profiting from it. Good data collection practices also support good data security practices, as collecting and storing large amounts of data not only increases the risk of a data breach or other unauthorized access but also increases the potential harm that could be caused. Some examples of how this protection may work in practice include the following:

- If an advertising network is tracking consumers' online activities to serve targeted ads, there is no need for the network to use key loggers or other applications to capture all data a consumer inputs.

- If a company collects information about unsecured wireless networks for the purpose of providing location-based services, the company should implement reasonable procedures to prevent additional, unintended collection of consumer data, such as the contents of individuals' wireless communications.[119]

---

[114] *See Written Comment of the ACLU of Northern California*, cmt. #544506-00068, at 1-2 (referencing business education primer *Privacy and Free Speech: It's Good for Business, available at* `http://www.dotrights.org`).

[115] *See, e.g.*, Disposal of Consumer Report Information and Records, 16 C.F.R. § 682 (2005) [hereinafter FTC Disposal Rule]; FTC Standards for Safeguarding Customer Information Rule, 16 C.F.R. § 314 (2002); HIPAA Security Standards for the Protection of Electronic Personal Health Information, 45 C.F.R. §§ 160, 162, 164 (2003); Mass. Gen. Laws ch. 93H, § 2 (2007); Cal. Civil Code § 1798.81.5 (West 2010).

[116] *See Privacy Initiatives, Enforcement, supra* note 19.

[117] *See* Press Release, Microsoft Corp., Microsoft Urges Government and Industry to Work Together to Build Confidence in the Cloud (Jan. 20, 2010), `http://www.microsoft.com/presspass/press/2010/jan10/1-20brookingspr.mspx`.

[118] *See* Sam Schillace, *Default https access for Gmail*, The Official Gmail Blog (Jan. 12, 2010, 9:14 PM), `http://gmailblog.blogspot.com/2010/01/default-https-access-for-gmail.html`.

- If a mobile application is providing traffic and weather information to a consumer based on his or her location information, it does not need to collect contact lists or call logs from the consumer's device.

Third, companies should implement reasonable and appropriate data retention periods, retaining consumer data for only as long as they have a specific and legitimate business need to do so. As noted above, the falling cost of data storage enables companies to retain data for long periods of time, at limited cost. This may result in stored data finding new, secondary uses that consumers did not anticipate when they provided the data. Moreover, even if old data is not valuable to a particular company, it could be highly valuable to an identity thief. For these reasons, businesses should promptly and securely dispose of data, including paper and electronic records, for which they no longer have a specific business need. The Commission has long supported this principle in its data security cases.[120]

One example of information that companies should not retain longer than necessary is location-based data. Retention of such data, and its use to build consumer profiles, raises important privacy concerns. For instance, the retention of location information about a consumer's visits to a doctor's office or hospital over time could reveal something about that consumer's health that would otherwise be private.[121] As with basic data security, data retention is another area where companies are making progress to address consumer privacy concerns and, indeed, beginning to compete on privacy. Major search engines, for example, have shortened their retention periods for search data.[122]

Finally, companies should take reasonable steps to ensure the accuracy of the data they collect, particularly if such data could be used to deny consumers benefits or cause significant harm. For example, some data brokers sell identity verification services to

[119] *See* Letter from David C. Vladeck, Dir., Bur. of Consumer Prot., FTC, to Albert Gidari, Esq., Counsel for Google (Oct. 27, 2010), *available at* `http://www.ftc.gov/os/closings/101027googleletter.pdf` (closing letter).

[120] Indeed, at least three of the Commission's data security cases—against DSW Shoe Warehouse, BJ's Wholesale Club, and Card Systems—involved allegations that companies violated data security laws by retaining magnetic stripe information from customer credit cards, much longer than they had a business need to do so. *See CardSystems Solutions, Inc.*, No. C- 4168, 2006 WL 2709787 (F.T.C. Sept. 5, 2006) (consent order); *DSW, Inc.*, No. C-4157, 2006 WL 752215 (F.T.C. Mar. 7, 2006) (consent order); *BJ's Wholesale Club, Inc.*, 140 F.T.C. 465 (2005) (consent order). Moreover, in disposing of certain sensitive information, companies must do so securely. *See FTC Disposal Rule, supra* note 115 (credit reports); *see also CVS Caremark Corp.*, No. C-4259, 2009 WL 1892185 (F.T.C. June 18, 2009) (financial, medical and employment information) (consent order); *Rite Aid Corp.*, No. 072-3121, 2010 WL 3053863 (F.T.C. Nov. 12, 2010) (prescription and employment information) (consent order).

[121] *See 2nd Roundtable, Remarks of Amina Fazlullah, U.S. PIRG*, at 260; *see also 2nd Roundtable, Remarks of Brian Knapp*, at 265 (noting that location information becomes more sensitive if the information is stored over a period of time).

[122] *See* Herb Torrens, *Microsoft Reduces Bing Data Retention Times*, Redmond Channel Partner Online, Jan. 20, 2010, `http://rcpmag.com/articles/2010/01/21/microsoft-reduces-bing-data-retention-times.aspx`; Nate Anderson, *Yahoo Outdoes Google, Will Scrub Search Logs After 90 Days*, Ars Technica (Dec. 17, 2008 11:40 AM), `http://arstechnica.com/old/content/2008/12/yahoo-outdoes-google-will-scrub-search-logs-after-90-days.ars`; Kurt Opsahl, *Google Cuts IP Log Retention to Nine Months*, Electronic Frontier Foundation Blog (Sept. 9, 2008), `http://www.eff.org/deeplinks/2008/09/google-cuts-server-log-retention-nine-months`.

various public and private entities. If the information is erroneous and does not match the identifying information a consumer presents to gain a benefit—such as accessing funds or services—the consumer can suffer economic or other harm.[123]

Staff requests input on whether there are additional substantive protections that companies should provide and how to balance the costs and benefits of such protections. Further, staff requests comment on whether the concept of "specific business purpose" or "need" should be defined further, and if so, how? In addition, is there a way to prescribe a reasonable retention period? Should the retention period depend upon the type or the sensitivity of the data at issue? For example, does the value of information used for behavioral advertising decrease so quickly that retention periods for such data can be quite short?

In addition, staff requests comment on how to apply these substantive principles to companies with legacy data systems. Certainly, companies should consider updating legacy systems with newer systems that have more comprehensive privacy protection, when available. However, when updating legacy systems is not feasible, what administrative or technical procedures should companies follow to mitigate the risks posed by such systems? Can companies minimize or otherwise modify the data maintained in them to protect consumer privacy interests?

5.2.2 Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.

To ensure that the substantive principles enumerated above are properly incorporated into their business models, companies should develop and implement comprehensive privacy programs. Such programs should designate specific personnel who are responsible for training employees on privacy, as well as promoting accountability for privacy policies throughout the organization. Where appropriate, the programs also should direct companies to assess the privacy impact of specific practices, products, and services to evaluate risks and ensure that the company follows appropriate procedures to mitigate those risks.[124] The size and scope of these programs should be appropriate to the risks presented to the data. Thus, companies that collect and use small amounts of non-sensitive consumer data should not have to devote the same level of resources to implementing privacy programs as companies that collect vast amounts of consumer data or data of a sensitive nature.

The use of peer-to-peer ("P2P") file-sharing software provides one illustration of how incorporating privacy considerations up-front may work. News reports have indicated that sensitive personal information has been shared via P2P file-sharing net-

[123]The FCRA requires consumer reporting agencies to maintain the accuracy of consumer report information, in order to ensure that erroneous information is not used to deny consumers credit, employment, insurance, housing, or certain other rights. *See* 15 U.S.C. § 1681e. Many types of information and uses, however, fall outside the FCRA.

[124]These principles are well-settled in data security law (*see supra* note 115), as well as the laws regarding government privacy. *See, e.g.*, E-Government Act of 2002, 44 U.S.C. § 3501; Privacy Act of 1974, 5 U.S.C. § 522a (2006).

works, including documents disclosing non-public House Ethics Committee investigations, avionics details of the President's helicopter, and many thousands of tax returns and medical records of ordinary citizens.[125] Some of these documents became available because businesses allowed employees to download P2P file-sharing programs onto their work computers without proper controls or supervision. In response to this problem, the Commission sent letters to nearly 100 organizations whose customer or employee information was breached through P2P file-sharing software.[126]

Companies that experienced breaches could have avoided or mitigated the problem by considering privacy and data security issues *before* allowing the use of P2P file-sharing software on their networks. The Commission has made this point in its P2P file-sharing education materials, which encourages companies to engage in a "ground-up" review of the risks of allowing P2P programs on their networks particularly those programs that automatically designate certain files for sharing.[127] The materials urge companies to assess their need to use such programs; if they do decide to use such programs, the companies should segregate them from computers that maintain personal information, and train their employees about the risks associated with use of P2P file-sharing programs on their work computers. This type of review and training would be useful in many contexts, such as when a company purchases or accesses software or hardware that collects, stores, processes, or otherwise uses consumer data.

In addition, companies that develop P2P file-sharing programs should do a better job of designing their products to prevent disclosure of consumer data.[128] The early stage of product research and development is the right time to consider consumer privacy. Companies should not wait to consider privacy as an add-on after the launch of a product.

Other recent examples involving the unexpected collection, use, and sharing of consumer information similarly underscore the importance of conducting privacy reviews before launching new products. Earlier this year, consumer outcry caused companies such as Google and Facebook to change the privacy practices related to their social networking tools after launching new products and features.[129] A more thorough privacy review before product launch—at the research and development stage—may have better aligned these products and services with consumer expectations and avoided public backlash.

Companies also should conduct periodic reviews of internal policies to address changes

[125] *See* Greg Sandoval, *Congress to probe P2P sites over 'inadvertent sharing'*, CNET News (Apr. 21, 2009 10:41 AM), `http://news.cnet.com/8301-1023_3-10224080-93.html`.

[126] *See* Press Release, FTC, Widespread Data Breaches Uncovered by FTC Probe, *supra* note 34.

[127] FTC, *Peer-to-Peer File Sharing: A Guide For Business, supra* note 34.

[128] *See* Letter from Mark K. Engle, Assoc. Dir., Bureau of Adver. Practices, FTC, to George Searle, CEO, LimeWire, Inc. (Aug. 19, 2010), *available at* `http://ftc.gov/os/closings/100919limewireletter.pdf` (closing letter) (noting that distributors of P2P file sharing software should "act more responsibly and provide safeguards against inadvertent sharing").

[129] *See, e.g.*, Brad Stone, *Privacy Group Files Complaint on Facebook Privacy Changes*, N.Y. Times (Dec. 17, 2009 1:50 PM), `http://bits.blogs.nytimes.com/2009/12/17/privacy-group-files-complaint-on-facebook-privacy-changes/`; Molly Wood, *Google Buzz: Privacy Nightmare*, CNET New (Feb. 10, 2010 5:48 PM), `http://news.cnet.com/8301-31322_3-10451428-256.html`.

in data risks or other circumstances. For instance, given the incidents in which supposedly anonymous data has been re-identified, as described above, companies should exercise caution before releasing data presumed to be anonymous for research or other purposes.[130] Applying this principle more broadly, companies dealing with consumers' data should keep up-to-date on privacy-related developments and should modify their practices as necessary to maintain privacy and ensure that their practices comport with their representations to consumers.

Finally, Commission staff supports the use of privacy-enhancing technologies to establish and maintain strong privacy policies. Such technologies include identity management, data tagging tools, and the use of Transport Layer Security/Secure Sockets Layer ("TLS/SSL") or other encryption technologies. The use of such technologies should be proportionate to the size of the business and sensitivity of the data at issue.[131]

Staff requests comment on how the full range of stakeholders can be given an incentive to develop and deploy privacy-enhancing technologies. Staff also seeks comment on the roles that different industry participants—*e.g.*, browser vendors, website operators, advertising companies should play in addressing privacy concerns with more effective technologies for consumer control.

5.3 Companies should simplify consumer choice.

Consumers face considerable burdens in understanding lengthy privacy policies and effectively exercising any available choices based on those policies. Business and consumer representatives alike have called for a more simplified approach to offering and communicating privacy choices—one that reduces the burden on consumers, as well as businesses engaged in commonly understood and accepted data practices. Accordingly, the proposed framework calls on companies to provide consumers with meaningful choice, but sets forth a limited set of data practices for which choice is not necessary.

Staff notes that, under current law, many companies are not required to provide—and do not currently provide—choice to consumers. In proposing a streamlined choice model, staff's goal is to foster clearer expectations for consumers and businesses regarding the types of practices for which choice should be provided.

5.3.1 Companies do not need to provide choice before collecting and using consumers' data for commonly accepted practices, such as product fulfillment.

Based on roundtable discussions and comments, staff has identified a limited set of "commonly accepted practices" for which companies should not be required to seek

[130] *See supra* notes 104-106.

[131] Staff also urges companies that use technological tools to check and adjust default settings to ensure that these tools are operating in a privacy protective manner. For example, companies should check whether their systems routinely save data without a specific business need or for longer than is necessary to achieve that purpose.

consent once the consumer elects to use the product or service in question.[132] They are:

- **Product and service fulfillment:** Websites collect consumers' contact information so that they can ship requested products. They also collect credit card information for payment. Online tax calculators and financial analysis applications collect financial information to run their analyses for customers.
- **Internal operations:** Hotels and restaurants collect customer satisfaction surveys to improve their customer service. Websites collect information about visits and click-through rates to improve site navigation.
- **Fraud prevention:** Offline retailers check drivers' licenses when consumers pay by check to monitor against fraud. Online businesses also employ fraud detection services to prevent fraudulent transactions. In addition, online businesses may scan ordinary web server logs to detect fraud, deleting the logs when they are no longer necessary for this purpose. Stores use undercover employees and video cameras to monitor against theft.
- **Legal compliance and public purpose:** Search engines, mobile applications, and pawn shops share their customer data with law enforcement agencies in response to subpoenas. A business reports a consumer's delinquent account to a credit bureau.
- **First-party marketing:** Online retailers recommend products and services based upon consumers' prior purchases on the website. Offline retailers do the same and may, for example, offer frequent purchasers of diapers a coupon for baby formula at the cash register.

Some of these practices, such as where a retailer collects a consumer's address solely to deliver a product the consumer ordered, are obvious from the context of the transaction, and therefore, the consumer's consent to them can be inferred. Others, including the use of consumer data exclusively for fraud prevention, legal compliance, or internal operations, are sufficiently accepted—or necessary for public policy reasons—that companies do not need to request consent for them. Staff believes that requiring consumers to make a series of decisions whether to allow companies to engage in these obvious or necessary practices would impose significantly more burden than benefit on both consumers and businesses.[133] This is also true where companies share consumer information with service providers acting at their direction for the purposes enumerated above, provided there is no further use of the data.

[132] *See, e.g., 1st Roundtable, Remarks of Fred Cate, Indiana University Maurer School of Law*, at 305-06 (noting that certain activities, such as routine backing up of data, need not be subject to consumer choice); *1st Roundtable, Remarks of J. Howard Beales, III, George Washington University*, at 330; *1st Roundtable, Remarks of Marc Rotenberg, Electronic Privacy Information Center*, at 322; *3rd Roundtable, Remarks of David Hoffman, Intel*, at 283; *see also Written Comment of The Business Forum for Consumer Privacy*, cmt. #544506-00058; *Written Comment of Microsoft Corp.*, cmt. #544506-00020, at 4.

[133] Although the framework does not contemplate choice for these accepted practices, companies should still disclose these practices in their privacy policies in order to promote transparency and accountability.

Staff proposes that first-party marketing include only the collection of data from a consumer with whom the company interacts directly for purposes of marketing to that consumer.[134] If a company shares data with a third party other than a service provider acting on the company's behalf—including a business affiliate unless the affiliate relationship is clear to consumers through common branding or similar means—the company's practices would not be considered first-party marketing and thus they would fall outside of "commonly accepted practices," as discussed below. Similarly, if a website publisher allows a third party, other than a service provider, to collect data about consumers visiting the site, the practice would not be "commonly accepted."[135]

Data collection across websites, even if done by a single party and not shared with others, will in some cases take a data practice out of the category of "commonly accepted practices" for which companies do not need to provide choice. The tracking of a consumer's online activities by the consumer's Internet Service Provider ("ISP") through the use of "deep packet inspection" is a notable example.[136] Consumers may reasonably anticipate, and are likely to accept, that their ISP will monitor the transmission of data for reasons related to providing Internet service, such as to ensure that their service is not interrupted or to detect and block the transmission of computer viruses or malware. It is, however, unlikely that consumers would anticipate ISP monitoring of all of their online activity in order to create detailed profiles of them for marketing purposes.[137]

With this background, staff raises several specific questions for public comment. Is the list of proposed "commonly accepted practices" described above too broad or too narrow? Additionally, are there practices that should be considered "commonly accepted" in some business contexts but not in others?

As discussed below, however, companies should conduct research and take other steps to ensure that such privacy policies clearly and effectively communicate information to consumers and are not overly complex and likely to confuse. *See* discussion *infra* pp. 69-72.

[134]Staff also believes that online contextual advertising should fall within the "commonly accepted practices" category. Contextual advertising involves the delivery of advertisements based upon a consumer's current visit to a web page or a single search query, without the collection and retention of data about the consumer's online activities over time. As staff concluded in its 2009 online behavioral advertising report, contextual advertising is more transparent to consumers and presents minimal privacy intrusion as compared to other forms of online advertising. *See OBA Report, supra* note 37, at 26-27 (where a consumer has a direct interface with a particular company, the consumer is likely to understand, and to be in a position to control, the company's practice of collecting and using the consumer's data).

[135]*OBA Report, supra* note 37, at 28.

[136]Deep packet inspection refers generally to the ability of an ISP to inspect the contents of each Internet transmission it carries on its network, including email messages and websites visited. *See* Steve Stecklow & Paul Sonne, *Shunned Profiling Technology on the Verge of a Comeback*, Wall St. J., Nov. 24, 2010, *available at* `http://online.wsj.com/article/SB10001424052748704243904575630751094784516.html`.

[137]*See* Ellen Nakashima, *NebuAd Halts Plans for Web Tracking*, Wash. Post, Sept. 4, 2008, *available at* `http://www.washingtonpost.com/wp-dyn/content/article/2008/09/03/AR2008090303566.html`; Saul Hansell, *Phorm's All-Seeing Parasite Cookie*, N.Y. Times (Apr. 7, 2008 4:04 PM), `http://bits.blogs.nytimes.com/2008/04/07/phorms-all-seeing-parasite-cookie`. For a discussion of how choices should be provided in the context of deep packet inspection, see *infra* text accompanying note 146.

Staff also seeks comment on the scope of first-party marketing that should be considered a "commonly accepted practice." Even if first-party marketing in general may be a commonly accepted practice, should consumers be given a choice before sensitive data is used for such marketing? In addition, should first-party marketing be limited to the context in which the data is collected from the consumer? For instance, in the online behavioral advertising context, Commission staff has stated that where a website provides recommendations or offers to a consumer based on his or her prior purchases at that website, such practice constitutes first-party marketing.[138] An analogous offline example would include a retailer offering a coupon to a consumer at the cash register based upon the consumer's prior purchases in the store. Is there a distinction, however, if the owner of the website or the offline retailer sends offers to the consumer in another context—for example, via postal mail, email, or text message? Should consumers have an opportunity to decline solicitations delivered through such means, as provided by existing sectoral laws?[139] In addition, should marketing to consumers by commonly-branded affiliates be considered first-party marketing?

Finally, how should the proposed framework handle the practice of data "enhancement," whereby a company obtains data about its customers from other sources, both online and offline, to enrich its databases? Should companies provide choices about this practice?

5.3.2 For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data.

The proposed "commonly accepted practices" category is limited to a narrow set of data collection and use activities. With respect to all other commercial data collection and use, the framework would require companies to give consumers the ability to make informed and meaningful choices.

A variety of business models involve practices that fall outside the proposed "commonly accepted practices" category. These include, for example, a retailer collecting purchase information directly from a consumer and then selling it to a data broker or other third party that may be unknown to the consumer. Other examples include online behavioral advertising, in which an online publisher allows third parties to collect data about consumers' use of the website, as well as social media services, where the service or platform provider allows thirdparty applications to collect data about a consumer's use of the service. In addition, as noted above, using deep packet inspection to create marketing profiles of consumers would not be a commonly accepted practice.

To ensure that choice is meaningful and accessible to consumers, companies should

[138] *See OBA Report, supra* note 37, at 26-27.

[139] Consumers have the ability to decline certain solicitations delivered via email or telemarketing phone calls. *See* CAN-SPAM Act and Do Not Call Rule, *supra* note 10. In addition, consumers can chose to have their names removed from many direct marketing lists. *See* Direct Marketing Association, *Guidelines for Ethical Business Practice* 14-15 (Oct. 2007), *available at* `http://dmaccc.org/Files/EthicsGuidelines.pdf`.

describe consumer choices clearly and concisely, and offer easy-to-use choice mechanisms. To be most effective, companies should provide the choice mechanism at a time and in a context in which the consumer is making a decision about his or her data.

a. General considerations regarding how choice is presented

Where a company has a relationship with a consumer, the choice mechanism should be offered at the point when the consumer is providing data or otherwise engaging with the company. In the context of an online retailer, the disclosure and control mechanism should appear clearly and conspicuously on the page on which the consumer types in his or her personal information. For an offline retailer, the disclosure and consumer control should take place at the point of sale by, for example, having the cashier ask the customer whether he would like to receive marketing offers from other companies.

With respect to social media services, if consumer information will be conveyed to a third-party application developer, the notice-and-choice mechanism should appear at the time the consumer is deciding whether to use the application and in any event, before the application obtains the consumer's information. Where the information sharing occurs automatically, through a default setting, that fact should be disclosed clearly and conspicuously at the time the consumer becomes a member of the service, not merely buried in the privacy policy.

Similar issues arise with respect to mobile services. For example, when a consumer downloads an application to his smartphone, he may not know whether his wireless carrier shares his personal information with the application. He also may not know if the application shares his information with advertisers or other third parties. All companies involved in information collection and sharing on mobile devices—carriers, operating system vendors, applications, and advertisers—should provide meaningful choice mechanisms for consumers.

Regardless of the specific context, where the consumer elects not to have her information collected, used, or shared, that decision should be durable and not subject to repeated additional requests from the particular merchant.

The Commission staff believes that such a simplified approach to providing choices will not only help consumers make decisions during particular transactions, but also will facilitate consumers' ability to compare privacy options that different companies offer. Thus, the staff's approach could promote meaningful competition on privacy.

Commission staff recognizes that there are differing views as to what constitutes informed consent. Some roundtable participants recommended that the Commission mandate "opt-in" consent for data practices, while others advocated for "opt-out" consent.[140] Different mechanisms for obtaining opt-in and opt-out consent can vary in their effectiveness. Indeed, a clear, simple, and prominent opt-out mechanism may be more privacy protective than a confusing, opaque opt-in. Staff has already stated that, regardless of how they are described, choices buried within long privacy policies and pre-checked boxes are not effective means of obtaining meaningful, informed consent.[141] Further, the time and effort required for consumers to understand and exercise their options may be more relevant to the issue of informed consent than whether the

choice is technically opt-in or opt out.[142]

Staff seeks comment on the appropriate way to obtain consent for practices that do not fall within the "commonly accepted" category, including whether the method of consent should be different for different contexts. For example, what are effective ways to seek informed consent in the mobile context, given the multiple parties involved in data collection and the challenges presented by the small screen? Would a uniform icon or graphic for presenting options be feasible and effective in this and other contexts? Market research and academic studies focusing on the effectiveness of different choice mechanisms in different contexts would be particularly helpful to staff as it continues to explore this issue. Staff also requests comment on whether and in what circumstances it is appropriate to offer choice as a "take it or leave it" proposition, whereby a consumer's use of a website, product, or service constitutes consent to the companys information practices.[143] Further, staff requests comment on what types of disclosures and consent mechanisms would be most effective to inform consumers about the trade-offs they make when they share their data in exchange for services. In particular, how should companies communicate the "take it or leave it" nature of the transaction to consumers? Are there any circumstances in which a "take it or leave it" proposition would be inappropriate?

Moreover, staff notes that both sensitive information and sensitive users may require additional protection through enhanced consent.[144] The Commission staff has supported affirmative express consent where companies collect sensitive information for online behavioral advertising[145] and continues to believe that certain types of sensitive information warrant special protection, such as information about children, financial and medical information, and precise geolocation data. Thus, before any of this data is collected, used, or shared, staff believes that companies should seek affirmative express consent. Staff requests input on the scope of sensitive information and users and the most effective means of achieving affirmative consent in these contexts.

In addition, staff notes that deep packet inspection would likely warrant enhanced

---

[140] *See, e.g., 1st Roundtable, Remarks of Leslie Harris, Center for Democracy & Technology*, at 64-65 (opt-in); *1st Roundtable, Remarks of Berin Szoka, The Progress & Freedom Foundation*, at 169 (opt-out).

[141] *See OBA Report, supra* note 37, at 39-40, n.70.

[142] There also may be choice approaches other than opt-in or opt-out consent. For example, in the organ donor context, the state of Illinois uses "mandated choice," under which consumers are required to make a decision about whether to become a donor before obtaining a driver's license. *See* Richard Thaler, *Opting In vs. Opting Out*, N.Y. Times, Sept. 26, 2009, *available at* `http://www.nytimes.com/2009/09/27/business/economy/27view.html?_r=1`. *See also* Letter from Bruce Sewell, Gen. Counsel and Senior Vice President of Legal and Gov't Affairs, Apple Inc., to the Hon. Edward J. Markey and Hon. Joe Barton, U.S. House of Representatives (Jul. 12, 2010), at 5, *available at* `http://markey.house.gov/docs/applemarkeybarton7-12-10.pdf` (explaining that before a thirdparty application on the iPhone can use information about a consumer's location for the first time, a dialogue box tells the consumer the application would like to use the consumer's location and requires the consumer to indicate "OK" or "Don't Allow").

[143] For example, in many cases, consumers receive, without charge, services such as email or other online storage from companies that collect and share their information for marketing.

[144] *See, e.g., 1st Roundtable, Remarks of Leslie Harris, Center for Democracy & Technology*, at 64-65; *1st Roundtable, Remarks of Pam Dixon, World Privacy Forum*, at 229-31.

[145] *See OBA Report, supra* note 37, at 42-44.

consent or even more heightened restrictions, because of the scope of the information collected about consumers and the inability of many consumers to discontinue broadband service. Indeed, deep packet inspection raises special concerns not only because of the extensive mining of consumer information it entails but also because of the limited level of competition among residential broadband ISPs. According to the Federal Communications Commission ("FCC"), approximately 96% of the U.S. population has at most two wireline broadband providers.[146] In addition, there may be barriers to switching ISPs, such as potential termination fees or costs and inconvenience associated with waiting for service personnel. In light of these concerns, staff requests comment on the appropriate level of protection for deep packet inspection.

Staff also seeks comment on the special issues raised with respect to teens. As noted above, teens are heavy users of digital technology and new media but may not always think clearly about the consequences of their actions. Are teens sensitive users, warranting enhanced consent procedures? Should additional protections be explored in the context of social media services? For example, Facebook has stated that it limits default settings such that teens are not allowed to share certain information with the category "Everyone."[147] What are the benefits and drawbacks of such an approach?

Finally, a topic of particular concern at the roundtables was how to ensure meaningful consumer choice with respect to the many companies that collect and use data without directly interacting with consumers. Information brokers, for instance, may acquire consumer data from a variety of sources and use it for purposes that consumers never anticipated. Although such practices generally would not fall within the "commonly accepted practices" category, staff recognizes that providing meaningful consumer choice is difficult in this context. Indeed, because these companies do not interact directly with consumers, they may not be in a position to provide consumer choice at the point of collection or use. Staff requests comment on choice mechanisms for data brokers, including whether some sort of universal, standardized mechanism would be feasible and beneficial. Another potential approach, which a number of roundtable panelists supported, is to provide additional transparency about data brokers, including by allowing consumers to access the data these entities maintain about them.[148] This idea is discussed further below.

b. A special choice mechanism for online behavioral advertising: Do Not Track

Companies engaged in behavioral advertising may be invisible to most consumers. The FTC repeatedly has called on stakeholders to create better tools to allow consumers to control the collection and use of their online browsing data. In response, several companies have developed new tools that allow consumers to control their receipt of targeted advertisements and to see and manipulate the information companies collect about them for targeting advertising.[149] TrustE, an online certification company, has launched a pilot program to display an icon on advertisements that links to additional

[146] *See* FCC, National Broadband Plan, at 37 (Mar. 15, 2010), *available at* `http://download.broadband.gov/plan/national-broadband-plan.pdf`.
[147] *See Controlling How You Share*, Facebook, `http://www.facebook.com/privacy/explanation.php`.
[148] *See infra* pp. 72-76.

information and choices about behavioral advertising.[150] An industry group comprised of media and marketing associations has developed self-regulatory guidelines and an opt-out mechanism for behavioral advertising.[151] This group has formed a coalition to develop an icon to display in or near targeted advertisements that links to more information and choices. The coalition has stated that providing consumers with choices about online advertising is essential to building the trust necessary for the marketplace to grow and has pledged to implement this effort industry-wide.[152]

In addition, each of the major browser vendors offers a mechanism to limit online tracking, with varying scope and ease of use. These browser vendors recognize the importance of offering consumers choices in this area.

While some industry members have taken positive steps toward improving consumer control, there are several concerns about existing consumer choice mechanisms. First, industry efforts to implement choice on a widespread basis have fallen short. The FTC has been calling on industry to implement innovations such as "just-in-time" choice for behavioral advertising since 2008. Although there have been developments in this area as described above, an effective mechanism has yet to be implemented on an industry-wide basis. Second, to the extent that choice mechanisms exist, consumers often are unaware of them, and click-through rates remain low.[153] For example, consumers are largely unaware of their ability to limit or block online tracking through their browsers, in part because these options may be difficult to find; further, those consumers who know about these options may be confused by the lack of clarity and uniformity among the browsers in how choices are presented and implemented.

Third, existing mechanisms may not make clear the scope of the choices being offered. It may not be clear whether these mechanisms allow consumers to choose not to be tracked, or to be tracked but not delivered targeted advertising. Also, consumers may believe that opting out at one company or website will prevent tracking or will block personalized advertising—or even all advertising—everywhere. Finally, consumers are not likely to be aware of the technical limitations of existing control mechanisms. For example, they may believe they have opted out of tracking if they block third-party cookies on their browsers; yet they may still be tracked through Flash cookies or other mechanisms.[154]

---

[149] *See, e.g., Google Ad Preferences*, `http://www.google.com/ads/preferences`; *Yahoo! Ad Interest Manager*, `http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/`.

[150] *See* Press Release, TRUSTe, TRUSTe Launches TRUSTed Ads Privacy Platform (Oct. 4, 2010), *available at* `http://www.truste.com/about_TRUSTe/press-room/news_truste_trustedads.html`.

[151] *See* Press Release, Interactive Advertising Bureau Press Release, Major Marketing / Media Trade Groups Launch Program to Give Consumers Enhanced Control over Collection and Use of Web Viewing Data for Online Behavioral Advertising (Oct. 4, 2010), *available at* `http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-100410`.

[152] *See id.*

[153] *1st Roundtable, Remarks of Alan Davidson, Google*, at 113.

[154] A Flash cookie, or a Flash local shared object, is a data file that is stored on a consumer's computer by a website that uses Adobe's Flash player technology. Like a regular http cookie, a Flash cookie can store information about a consumer's online activities. Unlike regular cookies, Flash cookies are stored in an area not controlled by the browser. Thus, when a consumer deletes or clears the cookies from his browser using tools provided through the browser, the consumer does not delete Flash cookies stored

Given these limitations, Commission staff supports a more uniform and comprehensive consumer choice mechanism for online behavioral advertising, sometimes referred to as "Do Not Track." Such a universal mechanism could be accomplished by legislation or potentially through robust, enforceable self-regulation. The most practical method of providing uniform choice for online behavioral advertising would likely involve placing a setting similar to a persistent cookie on a consumer's browser and conveying that setting to sites that the browser visits, to signal whether or not the consumer wants to be tracked or receive targeted advertisements. To be effective, there must be an enforceable requirement that sites honor those choices.[155]

Such a mechanism would ensure that consumers would not have to exercise choices on a company-by-company or industry-by-industry basis, and that such choices would be persistent. It should also address some of the concerns with the existing browser mechanisms, by being more clear, easy-to-locate, and effective, and by conveying directly to websites the user's choice to opt out of tracking.

Commission staff notes several important issues with respect to such a mechanism. First, any such mechanism should not undermine the benefits that online behavioral advertising has to offer, by funding online content and services and providing personalized advertisements that many consumers value.

Second, such a mechanism should be different from the Do Not Call program in that it should not require a "Registry" of unique identifiers. In the context of the Do Not Call program, each telephone already has a unique identifier in the form of a phone number. In contrast, there is no such persistent identifier for computers, as Internet Protocol ("IP") addresses[156] can change frequently. Rather than creating such an identifier in this context, which would raise significant privacy issues,[157] Commission staff recommends a browser-based mechanism through which consumers could make persistent choices.[158]

Third, some companies currently offer consumers a choice between opting out of

---

on his computer. Instead, the consumer must know that Flash cookies exist, go to the Adobe website, and follow the instructions provided there to have them removed.

Recently, a researcher released a software tool that demonstrates several technical mechanisms—in addition to Flash cookies—that websites can use to persistently track consumers, even if they have attempted to prevent such tracking through existing tools. *See* `http://samy.pl/evercookie`; *see also* Tanzina Vega, *New Web Code Draws Concerns Over Privacy Risks*, N.Y. Times, Oct. 10, 2010, *available at* `http://www.nytimes.com/2010/10/11/business/media/11privacy.html`.

[155]As with many high-tech areas, it may be difficult for consumers to ascertain which parties are not respecting their choices. However, technical methods exist that may reduce the ability of sites to track users, or that may identify parties that do not respect consumer choices not to be tracked for behavioral advertising. The Commission staff believes these tools could be effective to help monitor and enforce a uniform choice mechanism.

[156]An Internet Protocol address (IP address) is a number that is assigned to any device that is connected to the Internet.

[157]A new identifier would be yet another piece of personally identifiable information that companies could use to gather data about individual consumers.

[158]Although the practicalities of a proposed choice mechanism here would differ from Do Not Call, it would be similar in that it would allow consumers to express a single, persistent preference regarding advertising targeted to them.

online behavioral advertising altogether or affirmatively choosing the types of advertising they receive. For example, at the roundtables, one company described how it shows consumers the categories of advertising associated with them, and allows them to de-select those categories and select additional ones.[159] The panelist noted that, when given this option, rather than opting out of advertising entirely, consumers tend to choose to receive some types of advertising.

As this example illustrates, consumers may want more granular options. Thus, Commission staff seeks comment on whether a universal choice mechanism should include an option that enables consumers to control the types of advertising they want to receive and the types of data they are willing to have collected about them, in addition to providing the option to opt out completely.

Fourth, it is imperative that any universal choice mechanism be understandable and simple. In addition to being easy to find and use, such a mechanism should make it clear to consumers exactly what they are choosing and if there are limitations to that choice. Staff solicits comment on how to accomplish this goal.

Finally, staff seeks comment on the mechanics of a standardized choice mechanism. How should such a mechanism be offered to consumers and publicized? How can such mechanism be designed to be as clear and usable as possible for consumers? What are the potential costs and benefits of offering the mechanism? For instance, how many consumers would likely choose to avoid receiving targeted advertising? How many consumers, on an absolute and percentage basis, have utilized the opt-out tools currently provided? What is the likely impact if large numbers of consumers elect to opt out? How would it affect online publishers and advertisers, and how would it affect consumers? Should the concept of a universal choice mechanism be extended beyond online behavioral advertising and include, for example, behavioral advertising for mobile applications? If the private sector does not implement an effective uniform choice mechanism voluntarily, should the FTC recommend legislation requiring such a mechanism?

6 Companies should increase the transparency of their data practices.

As noted above, many data practices are invisible to consumers. Further, many consumers are unaware of how, and for what purposes, companies collect, use, and share data about them. In general, privacy policies do a poor job of informing consumers about companies' data practices or disclosing changes to their practices. And the aggregation of consumer data by information brokers and other non-consumer-facing entities raises significant policy issues.

To address these concerns, the proposed framework calls for a number of measures that companies should take to make their data practices more transparent to consumers.

[159] *1st Roundtable, Remarks of Alan Davidson, Google*, at 100-02.

One key measure, discussed above, is to simplify consumer choice and to provide choice mechanisms in a prominent, relevant, and easily accessible place for consumers. Other important transparency measures include improving consumers' ability to compare data practices across companies, thereby encouraging competition on privacy issues, and providing consumers with reasonable access to their data. In addition, before making material changes to their data policies, companies should make prominent disclosures that clearly describe such changes, and should obtain consumers' affirmative consent. Finally, additional consumer education efforts would increase transparency and improve consumers' understanding of data collection and use. Accordingly, all stakeholders should intensify their efforts to educate consumers about commercial data practices and the choices available to them.

6.1 Privacy notices should be clearer, shorter, and more standardized, to enable better comprehension and comparison of privacy practices.

An important legacy of the Commission's notice-and-choice approach to privacy is that most companies now disclose their data practices to consumers through privacy notices. Indeed, as a number of roundtable participants and commenters recognized, privacy notices continue to promote companies' accountability for their practices.[160] The public posting of privacy notices is especially valuable to consumer and privacy advocacy groups, regulators, and those consumers who want to learn more about a company's overall privacy practices. At the same time, however, privacy notices are often opaque, lack uniformity, and are too long and difficult to navigate. Too frequently they bury disclosures of important information. Staff agrees with those roundtable participants who asserted that these problems undermine the ability of consumers, regulators, and others to compare data practices from one company to another. In addition, participants cited evidence that consumers often misconstrue the meaning of privacy notices.[161]

A particularly strong illustration of where privacy notices have been ineffective is in the mobile context where, because of the small size of the device, a privacy notice can be spread out over 100 separate screens. Indeed, it is difficult to imagine consumers scrolling through each screen or making informed decisions based on the information contained in them.[162]

To address these concerns, privacy notices should provide clear, comparable, and concise descriptions of a company's overall data practices. They should clearly articulate who is collecting consumer data, why they are collecting it, and how such data will be used. Companies should standardize the format of their notices, as well as

[160] *See, e.g., 3rd Roundtable, Remarks of Fred Cate, Indiana University Maurer School of Law*, at 251-52; *3rd Roundtable, Remarks of Paula Bruening, Center for Information Policy Leadership*, at 256-57; *Written Comment of The Business Forum for Consumer Privacy*, cmt. #544506-00058, at 4.

[161] *See supra* note 62.

[162] *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 J.L. & Pol'y Info. Soc'y 543, 565 (2008) (estimating that it would take consumers hundreds of hours to read the privacy policies they might typically encounter in a year on the Internet).

the terminology used. This could allow consumers to make choices based on privacy and will potentially drive competition on privacy issues. In addition, companies and industry associations should undertake consumer testing of privacy notices to ensure comprehension. Companies that provide services on mobile and other "small screen" hand-held devices should determine how best to ensure that consumers can access and review pertinent information about data practices. The academic community may also offer valuable input on how best to ensure usability and comprehension of notices.

The financial privacy area offers useful guidance. In that context, the FTC worked with other agencies to develop shorter, standardized privacy notices. Under the GLB Act, financial institutions were required to send customers privacy notices beginning on July 1, 2001. The resulting notices were extremely long and complex legal documents with buried disclosures that consumers often could not find or understand. As a result, many consumers were unable to make meaningful choices. To address these concerns, eight agencies worked together to develop a model financial privacy notice using extensive research and consumer testing.[163] The consumer testing showed that consumers were more likely to read notices that were simple, provided key context up front, and had pleasing design elements, such as large amounts of white space. It also showed that the model notice—which uses a "layered approach" to simplify the presentation of information to consumers—is a significant improvement over the financial privacy notices that companies sent after Congress enacted the GLB Act.

The Commission staff requests comment on the feasibility of standardizing the format and terminology for describing data practices across industries, particularly given ongoing changes in technology. Further, how can companies present these notices effectively in the offline world or on mobile and similar devices? Should companies increase their use of machine-readable policies to allow consumers to more easily compare privacy practices across companies?

6.2 Companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use.

Information brokers or other companies entirely unknown to a consumer may collect consumer data, combine it with other information about them, and sell it to third parties. This practice is invisible to consumers, who do not know about these entities and do not know the identity of the third parties that purchase information about them or the purposes for which their data is being used.[164] This practice can result in the

[163] On October 13, 2006, President George W. Bush signed into law the Financial Services Regulatory Relief Act of 2006, which directed the Commission and other federal agencies to jointly develop a model financial privacy form. *See* Financial Services Regulatory Relief Act of 2006, Pub. L. 109-351, § 728, 120 Stat. 1966 (codified at 15 U.S.C. § 6803(e)). The form is a safe harbor for financial institutions that elect to use it. Earlier this year, the Commission and other agencies developed a simple, easy-to-understand form that consumers can use to compare privacy notices among institutions. *See* Final Model Privacy Form Under the Gramm-Leach-Bliley Act, 74 Fed. Reg. 62965 (codified by FTC at 16 C.F.R. Part 313) (2009), *available at* `http://www.ftc.gov/privacy/privacyinitiatives/PrivacyModelForm_FR.pdf`.

creation of individual consumer profiles or dossiers that consumers do not know about and cannot control, which raises privacy concerns.[165]

To address these concerns, some roundtable panelists stated that consumers should have access to their data as a means of improving transparency.[166] At the same time, other panelists expressed concerns about the cost of access to businesses, the ability of companies to authenticate the identity of consumers requesting access,[167] and the potential privacy threats of requiring access, which could force companies to assemble and store consumer data in profiles when they do not currently do so.[168] Yet other roundtable participants acknowledged that there were both costs and benefits to allowing consumers to access their own data, and proposed to reconcile these costs and benefits by creating a sliding scale for access, whereby the extent of access would depend on the sensitivity of data and its intended use.[169]

Commission staff recognizes that access raises significant policy issues, including questions about the costs relative to the benefits in various circumstances. However, if implemented properly, taking into account the costs and benefits of access in different situations, access could significantly increase the transparency of companies' data practices without imposing undue burden.[170] For example, where a company maintains data to be used for authentication or decision-making purposes, erroneous data could lead to significant consumer harm;[171] thus, it may be appropriate to provide the actual data regarding the consumer, along with the ability to correct or, if appropriate, delete the data. In such cases, the benefit of allowing the consumer to access and correct the data may outweigh the costs. On the other hand, companies that maintain marketing data might disclose the categories of consumer data they possess and provide a suppression right that allows consumers the ability to have their name removed from marketing lists.[172] Staff supports such a sliding scale approach.

---

[164] *See* Leslie Scism & Mark Maremont, *Insurers Test Data Profiles to Identify Risky Clients*, Wall St. J., Nov. 16, 2010, *available at* `http://online.wsj.com/article/SB10001424052748704648604575620750998072986.html`.

[165] *See, e.g., 1st Roundtable, Remarks of Pam Dixon, World Privacy Forum*, at 258-60; *3rd Roundtable, Remarks of Chris Jay Hoofnagle, University of California, Berkeley School of Law*, at 287-88.

[166] *See, e.g., 1st Roundtable, Remarks of Jim Adler, Intelius*, at 245; *3rd Roundtable, Remarks of Paula Bruening, Centre for Information Policy Leadership*, at 268-69;*1st Roundtable, Remarks of Evan Hendricks, Privacy Times*, at 288-89.

[167] *See, e.g., 3rd Roundtable, Remarks of David Hoffman, Intel*, at 271-72.

[168] *Id.*

[169] *See, e.g., 3rd Roundtable, Remarks of Paula Bruening, Centre for Information Policy Leadership*, at 268-69; *1st Roundtable, Remarks of Jennifer Barrett, Acxiom*, at 263-64; *1st Roundtable, Remarks of Rick Erwin, Experian*, at 264-65; *Written Comment of The Business Forum for Consumer Privacy*, cmt. #544506-00058 (discussing different levels of access depending on use of data).

[170] Additionally, access will provide an incentive for businesses to limit the data they collect and to reduce the amount of time they maintain it. *See, e.g., 3rd Roundtable, Remarks of Richard Purcell, Corporate Privacy Group*, at 269-70.

[171] Erroneous information from data brokers can be used to deny consumers access to funds, admission to an event, or membership in a group. Such uses may fall outside of the FCRA.

[172] This is consistent with the guidelines of the Direct Marketing Association, which require database compilers to provide consumers with access to the types of marketing information they hold about the consumer, along with an ability to opt out of the database compiler's marketing database. *See* Direct

Staff acknowledges that issues surrounding access have been controversial in the past. Indeed, a Commission-sponsored Advisory Committee convened in 1999 identified the many burdens imposed by access and was not able to develop workable solutions that would align costs of access with the benefits to consumers.[173] Since then, progress has been made in this regard. For example, in the 111th Congress, a bill providing for access to data broker information passed the House of Representatives on a bipartisan basis.[174] In addition to setting forth certain statutory requirements, the bill mandates that the Commission promulgate regulations to carry out the purpose of the Act and authorizes the Commission to impose additional limitations on the access provision as appropriate. Moreover, as discussed at the roundtables and expressed in comments, a number of companies have made progress in developing cost-effective approaches to access. Indeed, some companies currently allow consumers to see and, in appropriate cases, suppress, correct, or otherwise control data about them.[175] This progress is commendable and can serve as a model for how to implement access in a way that provides transparency, without imposing undue costs on businesses.

Access raises a number of issues about which Commission staff seeks comment. Should companies be able to charge a reasonable cost for certain types of access? Should companies inform consumers of the identity of those with whom the company has shared data about the consumer, as well as the source of the data? In addition, where companies do provide access, how should access apply to information maintained about teens? Should parents be able to access such data?

Another question is whether access to data should differ for consumer-facing and nonconsumer- facing entities. For non-consumer facing companies, how can consumers best discover which entities possess information about them and how to seek access to their data? Is it feasible for industry to develop a standardized means for providing consumer access to data maintained by non-consumer-facing entities? A related question concerns whether and how to notify consumers when data has been used to deny them benefits. One way is to require that entities that deny benefits to consumers based upon information obtained from information brokers provide notice to the affected consumer,

---

Marketing Association, *supra* note 139. It is also consistent with mechanisms offered by companies like Google and Yahoo, where consumers can access the categories of data these companies maintain about them and opt out of marketing based on some or all of these categories. *See* Erick Schonfeld, *Google Gives You a Privacy Dashboard to Show Just How Much It Knows About You*, TechCrunch (Nov. 5, 2009), `http://techcrunch.com/2009/11/05/google-gives-you-a-privacy-dashboard-to-show-just-how-much-it-knows-about-you/`; Rob Pegoraro, *Yahoo Adds Ad-Preferences Manager*, Wash. Post, Faster Forward Blog (Dec. 7, 2009 11:36 AM), `http://voices.washingtonpost.com/fasterforward/2009/12/yahoo_adds_ad-preferences_mana.html`.

[173] *See* FTC, *Final Report of the FTC Advisory Committee on Online Access and Security* (2000), *available at* `http://www.ftc.gov/acoas/papers/finalreport.htm`.

[174] *See* Data Accountability and Trust Act, H.R. 2221, 111th Congress (2009).

[175] For example, representatives from the data broker industry stated that for their marketing databases, they provide access to the types of information that a company holds about an individual, along with a right to suppress that information from those marketing databases. *See, e.g., 1st Roundtable, Remarks of Jennifer Barrett, Acxiom*, at 263-64;*see also 2nd Roundtable, Remarks of Scott Shipman, eBay*, at 229-30 (describing eBay's provision of access to consumers to comply with European Data Protection Directive); *1st Roundtable, Remarks of Alan Davidson, Google*, at 107-08 (describing Google Dashboard tool for improving transparency).

similar to an adverse action notice under the FCRA. This would allow the consumer to contact the information broker and access and potentially correct the data upon which the denial was based. Staff requests comment on the costs and benefits of providing such notice.

6.3 Companies must provide prominent disclosures and obtain affirmative express consent before using consumer data in a materially different manner than claimed when the data was collected.

Transparency and consumer choice are undermined when companies change their policies with respect to their use of previously-collected data. One example is where online social media services change their privacy setting defaults so that data that had been private at the time it was provided later becomes public or subject to use by third-party applications.[176] Commission staff recognizes the challenges of making changes to data practices more transparent, particularly in contexts such as social networking, where user expectations vary widely and may change over time.[177] However, if transparency and choice are to have any meaning, companies must honor the privacy promises they have made, even when they change their policies with respect to new transactions.

Under well-settled FTC case law and policy,[178] companies must provide prominent disclosures and obtain opt-in consent before using consumer data in a materially different manner than claimed when the data was collected, posted, or otherwise obtained. Thus, if a retailer changes its stated policy of not sharing customer data with third parties, it would need to prominently disclose the change and obtain affirmative express consent before sharing previously collected data. Similarly, if a social networking site changes its policy of keeping profile information private, it should make a prominent disclosure and seek affirmative express consent before retroactively applying the new policy.

Commission staff seeks comment on the types of changes companies make to their policies and practices and what types of changes they regard as material. Staff also seeks comment on the appropriate level of transparency and consent for prospective changes to datahandling practices.

6.4 All stakeholders should work to educate consumers about commercial data privacy practices.

Numerous participants, representing industry as well as consumer and privacy advocacy groups, discussed the need for greater consumer education to increase consumer aware-

[176] *See, e.g., 2nd Roundtable, Remarks of Chris Conley, ACLU of Northern California*, at 155-56.

[177] *See, e.g., 2nd Roundtable, Remarks of Erika Rottenberg, LinkedIn*, at 124-25; *2nd Roundtable, Remarks of Nicole Wong, Google*, at 126; *2nd Roundtable, Remarks of Chris Conley, ACLU of Northern California*, at 123.

[178] *See, e.g., Gateway Learning Corp.*, No. C-4120, 2004 WL 2618647 (F.T.C. Sept. 10, 2004); *OBA Report, supra* note 37; *see also In re Orkin Exterminating Co.*, 108 F.T.C. 263 (1986), *aff'd*, 849 F.2d 1354 (11th Cir.) (unilateral, retroactive change to material contract term found to violate Section 5 of the FTC Act).

ness and understanding of overall data collection and use practices and their privacy implications.[179] Similarly, participants supported increased education regarding the available tools for consumers to control the collection and use of their data.[180] Panelists also discussed the need for better consumer education about specific business models, including behavioral advertising, social networking, and location-based services, so that consumers can understand both the benefits and the privacy implications of these types of data uses.[181]

A number of companies and industry groups, as well as consumer advocates, academics, and others have undertaken efforts to educate consumers about various types of data practices. For instance, several non-profit organizations have launched campaigns and developed school curricula to educate young people about safe social networking and other online issues.[182]

The Commission staff encourages these initiatives but calls upon stakeholders toaccelerate efforts to raise consumer awareness about data practices and to provide additional transparency tools to consumers. As noted above, one of the major themes of the roundtables is that consumers lack understanding of various data practices and their privacy implications, and thus lack the ability to make informed decisions about the trade-offs involved. Increased consumer education—in conjunction with the clearer and stronger protections discussed above—will help alleviate these concerns. In addition, the Commission staff requests input on how individual businesses, industry associations, consumer groups, and government can do a better job of informing consumers about privacy. Also, what role should government and industry associations have in educating businesses?

7 Conclusion

This report represents Commission staff's efforts to distill the major themes discussed at the privacy roundtable series into a broad privacy framework to guide policymakers, including Congress and industry. To expand the record developed through the roundtables, and further inform the Commission and other policy makers, the report includes a number of preliminary recommendations, questions, and issues related to the proposed framework. Commission staff encourages interested parties to submit comments, which it will consider as it further develops and refines the proposed framework for its final

[179] *See, e.g., 1st Roundtable, Remarks of Linda Woolley, Direct Marketing Association*, at 172-73; *3rd Roundtable, Remarks of Deborah Peel, Patient Privacy Rights*, at 101-02; *1st Roundtable, Remarks of Jennifer Barrett, Acxiom*, at 257.

[180] *See, e.g., Written Comment of The Progress & Freedom Foundation*, cmt. #544506-00035, at 6; *2nd Roundtable, Remarks of Anne Toth, Yahoo! Inc.*, at 66.

[181] *See, e.g., 1st Roundtable, Remarks of Richard Purcell, Corporate Privacy Group*, at 54-55; *2nd Roundtable, Remarks of Darren Bowie, Nokia*, at 284-85; *2nd Roundtable, Remarks of Michael Altschul, CTIA - The Wireless Association*, at 289; *2nd Roundtable, Remarks of Nicole Wong, Google*, at 114-15.

[182] *See, e.g., Internet Keep Safe Coalition*, `http://www.ikeepsafe.org`; *ConnectSafely*, `http://www.connectsafely.org`; *Common Sense Education Programs*, Common Sense Media, `http://www.commonsensemedia.org/educators`.

report.

Appendix A- Questions for Comment on Proposed Framework

Scope

- Are there practical considerations that support excluding certain types of companies or businesses from the framework—for example, businesses that collect, maintain, or use a limited amount of non-sensitive consumer data?
- Is it feasible for the framework to apply to data that can be "reasonably linked to a specific consumer, computer, or other device"?
- How should the framework apply to data that, while not currently considered "linkable," may become so in the future?
- If it is not feasible for the framework to apply to data that can be "reasonably linked to a specific consumer, computer, or other device," what alternatives exist?
- Are there reliable methods for determining whether a particular data set is "linkable" or may become "linkable"?
- What technical measures exist to "anonymize" data and are any industry norms emerging in this area?

Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services

Incorporate substantive privacy protections

- Are there substantive protections, in addition to those set forth in Section V(B)(1) of the report, that companies should provide and how should the costs and benefits of such protections be balanced?
- Should the concept of "specific business purpose" or "need" be defined further and, if so, how?
- Is there a way to prescribe a reasonable retention period?
- Should the retention period depend upon the type or the sensitivity of the data at issue? For example, does the value of information used for behavioral advertising decrease so quickly that retention periods for such data can be quite short?
- How should the substantive principles set forth in Section V(B)(1) of the report apply to companies with legacy data systems?
- When it is not feasible to update legacy data systems, what administrative or technical procedures should companies follow to mitigate the risks posed by such systems?

- Can companies minimize or otherwise modify the data maintained in legacy data systems to protect consumer privacy interests?

Maintain comprehensive data management procedures

- How can the full range of stakeholders be given an incentive to develop and deploy privacy-enhancing technologies?
- What roles should different industry participants—e.g., browser vendors, website operators, advertising companies—play in addressing privacy concerns with more effective technologies for consumer control?

Companies should simplify consumer choice

Commonly accepted practices

- Is the list of proposed "commonly accepted practices" set forth in Section V(C)(1) of the report too broad or too narrow?
- Are there practices that should be considered "commonly accepted" in some business contexts but not in others?
- What types of first-party marketing should be considered "commonly accepted practices"?
- Even if first-party marketing in general may be a commonly accepted practice, should consumers be given a choice before sensitive data is used for such marketing?
- Should first-party marketing be limited to the context in which the data is collected from the consumer?
  - For instance, in the online behavioral advertising context, Commission staff has stated that where a website provides recommendations or offers to a consumer based on his or her prior purchases at that website, such practice constitutes firstparty marketing. An analogous offline example would include a retailer offering a coupon to a consumer at the cash register based upon the consumers prior purchases in the store. Is there a distinction, however, if the owner of the website or the offline retailer sends offers to the consumer in another context for example, via postal mail, email, or text message? Should consumers have an opportunity to decline solicitations delivered through such means, as provided by existing sectoral laws?
- Should marketing to consumers by commonly-branded affiliates be considered first-party marketing?
- How should the proposed framework handle the practice of data "enhancement," whereby a company obtains data about its customers from other sources, both

online and offline, to enrich its databases? Should companies provide choice about this practice?

Practices that require meaningful choice

General

- What is the most appropriate way to obtain consent for practices that do not fall within the "commonly accepted" category?
- Should the method of consent be different for different contexts?
  - For example, what are effective ways to seek informed consent in the mobile context, given the multiple parties involved in data collection and the challenges presented by the small screen?
  - Would a uniform icon or graphic for presenting options be feasible and effective in this and other contexts?
  - Is there market research or are there academic studies focusing on the effectiveness of different choice mechanisms in different contexts that could assist FTC staff as it continues to explore this issue?
- Under what circumstances (if any) is it appropriate to offer choice as a "take it or leave it" proposition, whereby a consumers use of a website, product, or service constitutes consent to the companys information practices?
- What types of disclosures and consent mechanisms would be most effective to inform consumers about the trade-offs they make when they share their data in exchange for services?
  - In particular, how should companies communicate the "take it or leave it" nature of a transaction to consumers?
  - Are there any circumstances in which a "take it or leave it" proposition would be inappropriate?
- How should the scope of sensitive information and sensitive users be defined and what is the most effective means of achieving affirmative consent in these contexts?
- What additional consumer protection measures, such as enhanced consent or heightened restrictions, are appropriate for the use of deep packet inspection?
- What (if any) special issues does the collection or the use of information about teens raise?
  - Are teens sensitive users, warranting enhanced consent procedures?

  - Should additional protections be explored in the context of social media services? For example, one social media service has stated that it limits default settings such that teens are not allowed to share certain information with the category "Everyone." What are the benefits and drawbacks of such an approach

- What choice mechanisms regarding the collection and use of consumer information should companies that do not directly interact with consumers provide?
- Is it feasible for data brokers to provide a standardized consumer choice mechanism and what would be the benefits of such a mechanism?

Special choice for online behavioral advertising: Do Not Track

- How should a universal choice mechanism be designed for consumers to control online behavioral advertising?
- How can such a mechanism be offered to consumers and publicized?
- How can such a mechanism be designed to be clear, easy-to-find, usable, and understandable to consumers?
- How can such a mechanism be designed so that it is clear to consumers what they are choosing and what the limitations of the choice are?
- What are the potential costs and benefits of offering a standardized uniform choice mechanism to control online behavioral advertising?
- How many consumers would likely choose to avoid receiving targeted advertising?
- How many consumers, on an absolute and percentage basis, have utilized the opt-out tools currently provided?
- What is the likely impact if large numbers of consumers elect to opt out? How would it affect online publishers and advertisers, and how would it affect consumers?
- In addition to providing the option to opt out of receiving ads completely, should a universal choice mechanism for online behavioral advertising include an option that allows consumers more granular control over the types of advertising they want to receive and the type of data they are willing to have collected about them?
- Should the concept of a universal choice mechanism be extended beyond online behavioral advertising and include, for example, behavioral advertising for mobile applications?
- If the private sector does not implement an effective uniform choice mechanism voluntarily, should the FTC recommend legislation requiring such a mechanism?

Companies should increase the transparency of their data practices

Improved privacy notices

- What is the feasibility of standardizing the format and terminology for describing data practices across industries, particularly given ongoing changes in technology?
- How can companies present these notices effectively in the offline world or on mobile and similar devices?
- Should companies increase their use of machine-readable policies to allow consumers to more easily compare privacy practices across companies?

Reasonable access to consumer data

- Should companies be able to charge a reasonable cost for certain types of access?
- Should companies inform consumers of the identity of those with whom the company has shared data about the consumer, as well as the source of the data?
- Where companies do provide access, how should access apply to information maintained about teens? Should parents be able to access such data?
- Should access to data differ for consumer-facing and non-consumer-facing entities?
- For non-consumer-facing companies, how can consumers best discover which entities possess information about them and how to seek access to their data?
- Is it feasible for industry to develop a standardized means for providing consumer access to data maintained by non-consumer-facing entities?
- Should consumers receive notice when data about them has been used to deny them benefits? How should such notice be provided? What are the costs and benefits of providing such notice?

Material changes

- What types of changes do companies make to their policies and practices and what types of changes do they regard as material?
- What is the appropriate level of transparency and consent for prospective changes to data-handling practices?

Consumer education

- How can individual businesses, industry associations, consumer groups, and government do a better job of informing consumers about privacy?
- What role should government and industry associations have in educating businesses?

Appendix B: FTC Privacy Milestones

FTC Privacy Milestones

Laws & Rules
Cases
Reports
Workshops
Education

1970	Fair Credit Reporting Act enacted
1972	First Fair Credit Reporting Act (FCRA) case: In the Matter of Credit Bureau of Lorain
1975	FTC sues tax preparer for improperly using customers' information to market its loans: FTC v. Beneficial Corporation
1970s	FTC brings 15 additional enforcement actions against credit bureaus and report users
1983	First FCRA case against a nationwide credit bureau: FTC v. TransUnion
1985	FCRA sweep against users of consumer reports
1990	Commission staff issues comprehensive commentary on the FCRA
1991	FTC sues TRW for FCRA violations: FTC v. TRW
1992	FCRA sweep against employers using credit reports
1995	FTC sues Equifax for FCRA violations: In the Matter of Equifax Credit Information Services
1996	First major revision of the Fair Credit Reporting Act
	FTC sponsors workshop: *Consumer Privacy on the Global Information Infrastructure*
1997	First spam case: FTC v. Nia Cano
	FTC hosts traveling workshops to discuss revisions of FCRA
	FTC sponsors workshop: *Consumer Information Privacy*
	FTC issues *Individual Reference Services: A Federal Trade Commission Report to Congress*
1998	FTC issues *Privacy Online: A Federal Trade Commission Report to Congress*
1999	First case involving children's privacy: In the Matter of Liberty Financial
	First consumer privacy case: In the Matter of GeoCities
	FTC issues *Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress*
	FTC sponsors workshop: *Online Profiling*
	FTC launches ID Theft website: consumer.gov/idtheft and ID Theft Online Complaint Form
	FTC's 877-ID-THEFT consumer helpline established
2000	Children's Online Privacy Protection Rule (COPPA) goes into effect
	Gramm-Leach-Bliley Financial Privacy Rule goes into effect
	Three nationwide consumer reporting agencies pay $2.5 million in civil penalties for FCRA violations: US v. Equifax Credit Information Services, US v. TransUnion, and US v. Experian Information Solutions
	First COPPA case: FTC v. Toysmart.com
	FTC issues *Online Profiling: A Federal Trade Commission Report to Congress*
	FTC issues *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress*

FTC Privacy Milestones
continued

	FTC sponsors workshop: *The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*
	FTC publishes ID Theft booklet for victims: *When Bad Things Happen to Your Good Name*
2001	COPPA Safe Harbor Program begins
	First civil penalty cases under COPPA: US v. Looksmart, US v. Monarch Services, US v. Bigmailbox
	FTC sponsors workshops: *The Information Marketplace: Merging and Exchanging Consumer Data; Gramm-Leach-Bliley Educational Program on Financial Privacy*; and *Get Noticed: Effective Financial Privacy Notices: An Interagency Workshop*
	FTC publishes ID Theft Affidavit
2002	First data security case: In the Matter of Eli Lilly & Company
	FTC settles data security charges related to Microsoft's Passport service: In the Matter of Microsoft
	FTC sponsors workshop: *Consumer Information Security Workshop*
	FTC issues report on *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*
	FTC launches 10-minute educational ID Theft video
	FTC distributes over 1 million ID Theft booklets for victms
2003	Fair and Accurate Credit Transactions Act (FACTA) passed
	National Do Not Call Registry goes into effect
	Gramm-Leach-Bliley Safeguards Rule goes into effect
	FTC sues companies for sharing students' survey data with commercial marketers: In the Matter of Education Research Center of America and Student Marketing Group
	Guess settles FTC data security charges: In the Matter of Guess?
	FTC issues *Technologies for Protecting Personal Information: A Staff Workshop Report*
	FTC sponsors workshops: *Technologies for Protecting Personal Information; Spam Forum*; and *Costs and Benefits Related To the Collection and Use of Consumer Information*
2004	CAN-SPAM Rule goes into effect
	CAN-SPAM Adult Labeling Rule goes into effect
	Free Annual Credit Report Rule goes into effect
	First spyware case: FTC v. Seismic Entertainment
	FTC charges company with exposing consumers' purchases: In the Matter of MTS (dba Tower Records)
	FTC charges company with renting consumer information it had pledged to keep private: In the Matter of Gateway Learning

	FTC issues *The CAN-SPAM Act of 2003: National Do Not Email Registy: A Federal Trade Commission Report to Congress*
	FTC sponsors workshops: *Monitoring Software on Your PC: Spyware, Adware and Other Software; Radio Frequency IDentification: Applications and Implications for Consumers*; and *Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues*
	FTC publishes *The CAN-SPAM Act: A Compliance Guide for Business*
2005	Disposal Rule goes into effect
	FACTA Disposal Rule goes into effect
	FACTA Pre-Screen Opt Out Rule goes into effect
	National Do Not Call Registry tops 100 million phone numbers
	First Do Not Call enforcement action: FTC v. National Consumer Council
	First Do Not Call civil penalty action: US v. Braglia Marketing
	Highest civil penalty in a Do Not Call case: US v. DirecTV ($5.3 million)
	First enforcement actions under Gramm-Leach-Bliley Safeguards Rule: In the Matter of Sunbelt Lending and In the Matter of Nationwide Mortgage Group
	First unfairness allegation in a data security case: In the Matter of BJ's Wholesale Club
	FTC issues *RFID: Radio Frequency IDentification: Applications and Implications for Consumers: A Workshop Report From the Staff of the Federal Trade Commission*
	FTC issues *Spyware Workshop: Monitoring Software On Your Personal Computer: Spyware, Adware, and Other Software: Report of the Federal Trade Commission Staff*
	FTC launches online safety website: OnGuardOnline.gov
2006	FACTA Rule Limiting Marketing Solicitations from Affiliates goes into effect
	Highest civil penalty in a consumer protection case: US v. ChoicePoint ($10 civil penalty for violations of FCRA as well as $5 million redress for victims)
	First adware case: In the Matter of Zango
	Highest civil penalty to date in a COPPA case: US v. Xanga ($1 million)
	FTC settles charges against a payment processor that had experienced the largest breach of financial data to date: In the Matter of CardSystems Solutions
	FTC issues *Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues: A Federal Trade Commission Staff Workshop Report*
	FTC sponsors workshop: *Protecting Consumers in the Next Tech-Ade*
	FTC launches national educational campaign on identity theft and publishes *Deter, Detect, Defend: Avoid ID Theft* brochure

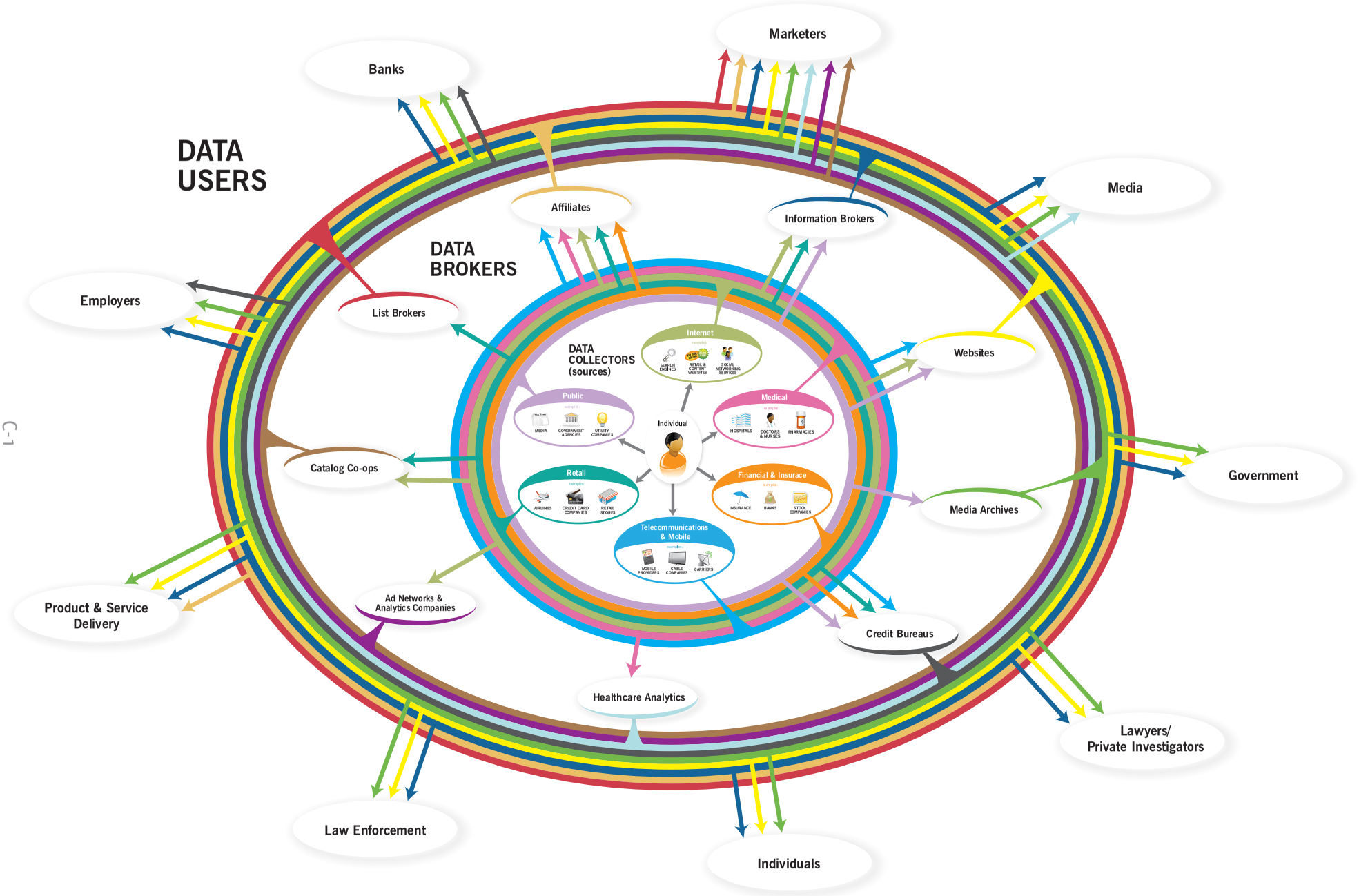
FTC Privacy Milestones
continued

2007	First Disposal Rule case: US v. American United Mortgage Company
	Adult-oriented online social networking operation settles FTC charges; unwitting consumers pelted with sexually graphic pop-ups: FTC v. Various (dba AdultFriendFinder)
	FTC issues *Spam Summit: The Next Generation of Threats and Solutions: A Staff Report by the Federal Trade Commission's Division of Marketing Practices*
	FTC issues *Implementing the Children's Online Privacy Protection Act: A Federal Trade Commission Report to Congress*
	FTC co-chairs President's Identity Theft Task Force (with DOJ) and issues Strategic Plan
	FTC sponsors workshops: *Security in Numbers: SSNs and ID Theft; Ehavioral Advertising: Tracking, Targeting, and Technology*; and *Spam Summit: The Next Generation of Threats and Solutions*
	FTC publishes *Protecting Personal Information: A Guide for Business* and launches interactive tutorial
2008	Highest civil penalty in a CAN-SPAM case: US v. ValueClick ($2.9 million)
	FTC settles charges against data broker Lexis Nexis and retailer TJX related to the compromise of hundreds of thousands of consumers' information: In the Matter of Reed Elsevier and Seisent and In the Matter of TJX Companies
	FTC issues *Protecting Consumers in the Next Tech-ade: A Report by the Staff of the Federal Trade Commission*
	FTC issues *Security In Numbers: Social Security Numbers and Identity Theft – A Federal Trade Commission Report Providing Recommendations On Social Security Number Use In the Private Sector*
	President's Identity Theft Task Force Report released
	FTC sponsors workshops: *Protecting Personal Information: Best Practices for Business* (Chicago, Dallas, and Los Angeles); *Pay on the Go: Consumers and Contactless Payment, Transatlantic RFID Workshop on Consumer Privacy and Data Security*; and *Beyond Voice: Mapping the Mobile Marketplace*
	U.S. Postal Service sends FTC ID Theft prevention brochure to every household in the country
2009	Robocall Rule goes into effect
	Health Breach Notification Rule goes into effect
	First case alleging failure to protect employee information: In the Matter of CVS Caremark
	First cases alleging six companies violated the EU-US Safe Harbor Agreement: In the Matter of World Innovators, In the Matter of ExpatEdge Partners, In the Matter of Onyx Graphics, In the Matter of Directors Desk, In the Matter of Progressive Gaitways, and In the Matter of Collectify
	Largest FTC-state coordinated settlement on privacy: FTC v. Lifelock
	FTC issues *Self-Regulatory Principles For Online Behavioral Advertising: Tracking, Targeting, and Technology*

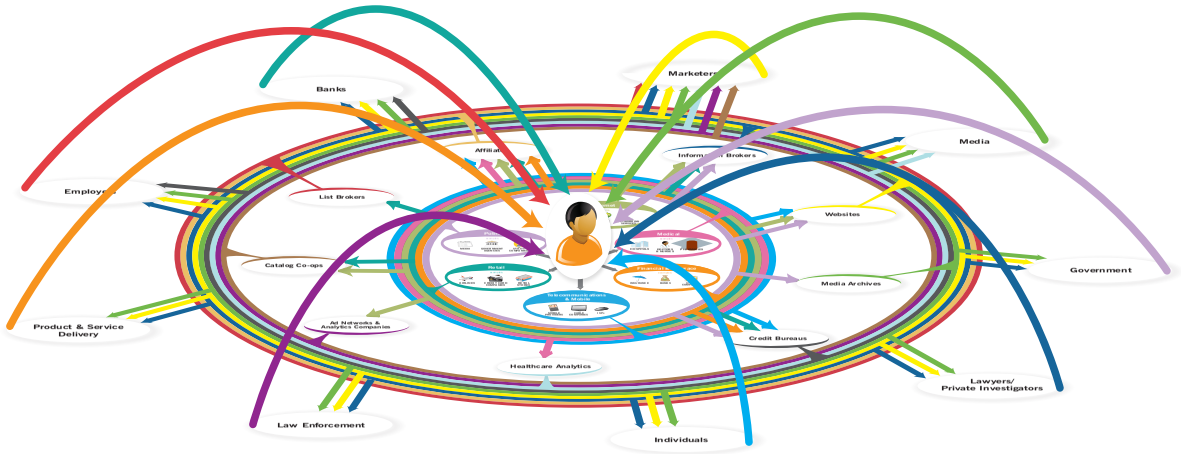
	FTC sponsors workshops: *Exploring Privacy: A Roundtable Series*; *Protecting Personal Information: Best Practices for Business* (New York); and *Securing Personal Data in the Global Economy*
	FTC publishes *Net Cetera: Chatting with Kids About Being Online*
2010	FTC jointly publishes Model Privacy Form under the Gramm-Leach-Bliley Act
	National Do Not Call Registry tops 200 million phone numbers
	First data security case involving social media: In the Matter of Twitter
	First case shutting down a rogue ISP: FTC v. Pricewert
	First data security case against an online seal provider: FTC v. ControlScan
	Highest judgment in a spyware case: FTC v. Innovative Marketing ($163 million)
	FTC conducts sweep against companies for exposure of employee and/or customer data on peer-to-peer (P2P) file-sharing networks
	FTC sponsors *COPPA Rule Review Roundtable*
	FTC publishes *Peer-to-Peer File Sharing: A Guide for Businesses*; *Medical Identity Theft: How to Minimize Your Risk*; and *Copier Data Security: A Guide for Businesses*
	FTC distributes 6+ million printed copies of *Deter, Detect, Defend: Avoid ID Theft* brochures and 5+ million printed copies of *Net Cetera: Chatting with Kids About Being Online*

Appendix C: Personal Data Ecosystem

Personal Data Ecosystem



DATA USES:



Examples of uses of consumer information in personally identifiable or aggregated form:

- Financial services, such as for banking or investment accounts
- Credit granting, such as for credit or debit cards; mortgage, automobile or specialty loans; automobile rentals; or telephone services
- Insurance granting, such as for health, automobile or life
- Retail coupons and special offers
- Catalog and magazine solicitations
- Web and mobile services, including content, e-mail, search, and social networking
- Product and service delivery, such as streaming video, package delivery, or a cable signal
- Attorneys, such as for case investigations
- Journalism, such as for fact checking
- Marketing, whether electronically, through direct mail, or by telephone
- Data brokers for aggregation and resale to companies and/or consumers
- Background investigations by employers or landlords
- Locating missing or lost persons, beneficiaries, or witnesses
- Law enforcement
- Research (e.g., health, financial, and online search data) by academic institutions, government agencies, and commercial companies
- Fraud detection and prevention
- Government benefits and services, such as licensing

Appendix D: Concurring Statement of Commissioner William E. Kovacic

Issuance of Preliminary FTC Staff Report *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*
December 1, 2010

I vote to issue this preliminary report by FTC staff for the purpose of stimulating further discussion. The report is the latest in a series of steps the agency has taken since the late 1960s to promote the development of sensible national and international policies involving data protection and privacy. This process of deliberation makes a valuable contribution by encouraging debate about the future framework of policy in these fields. By voting to issue the report as an element of the public consultation that will yield a further iteration of the document in 2011, I do not mean to endorse its content or perspective, as now presented.

In their current form, I regard some of staff's recommendations—notably, the proposal for a Do-Not-Track system—to be premature. I also would prefer that the report include more context about the existing framework for federal and state oversight of privacy; more context about legal concepts (including concepts from tort, property, and contract law) that underlie privacy policy and doctrine; and a fuller review of the modern literature (and the limits of that literature) on consumers' valuation of privacy.[1] The document also would benefit from more discussion of the relation of staffs proposed framework to earlier privacy frameworks. In 2000, a Commission majority recommended the adoption (through legislation) of Fair Information Practice Principles regarding notice, choice, access to data, and security.[2] Soon afterwards, the Commission shifted its focus to some degree and identified harm to consumers as its guiding principle.[3] This approach both contracted the 2000 framework (by imposing a harm screen) and expanded it (by including non-web based practices, and providing, for example, a conceptual framework for the Do-Not-Call rule).[4]

---

[1] The report cites one laboratory study for the proposition that consumers are willing to pay more to shop at websites that have better privacy policies. *See* Rep. at 30 n.73. In the cited study, the average measured privacy premiums ranged from $0.11 to $0.52 for a product costing $15.50, and varied according to when and where privacy indicators were visible during online purchasing experiences. Serge Egelman *et al., Timing is Everything? The Effects of Timing and Placement of Online Privacy Indicators, available at* `http://www.guanotronic.com/~serge/papers/chi09a.pdf`. Other research has also suggested that consumer willingness to pay for privacy may be small relative to self-reported values and varies across the population and settings. *See, e.g.*, Kai-Lung Hui et al., *The Economics of Privacy*, Chapter 9 *in* HANDBOOKS IN INFORMATION SYSTEMS, VOL. 1, at 19-22 (Terrence Hendershott, Ed., 2006) (reviewing the empirical literature and noting that "the key policy issue is not whether individuals value privacy. It is obvious that people value privacy. What is not know is *how much* people value privacy and the extent to which it varies.") (emphasis in original).

[2] *See* FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace* ii-iii (2000), *available at* `http://www.ftc.gov/reports/privacy2000/privacy2000.pdf`. [hereinafter 2000 Reprt]. Commissioner Swindle dissented and Commissioner Leary dissented in part and concurred in part.

[3] *See Protecting Consumers Privacy: 2002 and Beyond*, Remarks of FTC Chairman Timothy J. Muris at the Privacy 2001 Conference (Oct. 4, 2001) *available at* `http://www.ftc.gov/speeches/muris/privisp1002.shtm`.

[4] 16 C.F.R. § 310.4(b).

The current preliminary staff report does not reject the fundamental insight of the harmbased approach. Instead, the report appears to embrace a harm-based screen in reiterating and expanding principles covered by the 2000 report,[5] and in grouping those principles into new categories. It differs from earlier reports, though, in proposing an expanded concept of harm (although it does not address how the Commission's application of the harm test has developed in practice[6]).

One of the report's major premises is that "many companies . . . do not adequately address consumer privacy interests."[7] It would be useful to see greater support for the proposition that consumer expectations of privacy are largely going unmet. In its current form, the report understates the economic incentives that firms have today to meet consumers' demand for privacy. For example, large data breaches can have negative financial consequences for firms.[8] The increasingly widespread use of privacy controls such as NoScript and TACO—a development the report cites—might suggest that firms are working to meet consumer demands for privacy.

I am interested in comments to specific questions posed by staff. Additionally, I would be interested in any insights on the points I have noted above. Further, I would appreciate public comment on some additional or related questions, as follows:

- How should policy makers go about identifying mainstream consumer expectations for purposes of setting default terms with respect to data collection and use? When should such default terms be based on considerations other than consumer expectations? Should the chosen default terms be immutable? If not, what steps should consumers be required to take to override the defaults?

- The Do-Not-Track mechanism would share with the Do-Not-Call rule a basis in consumer sovereignty, insofar as it would implement individual consumers' choices. Are there any significant differences between the proposed Do-Not-Track mechanism and the Do-Not-Call rule? For example, the contemplated mechanism (similar to the Do-Not- Call registry) would merely convey a consumer's request not to be tracked, and would not actually prevent tracking. Would it be significant if, at the time the program was implemented, there was no legal mandate (at least for companies that did not *promise* to comply with such requests) requiring websites and others to comply? With or without new legislation, would there be an effective enforcement mechanism? Would consumers be able to detect violations? Would enforcement officials? Further, is there a risk that consumers will be

[5]The report does include components that were not within the 2000 report, such as separate principles addressing data collection and retention limits. Some of these were anticipated in a recent staff report. FTC, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* (2009), *available at* `http://www.ftc.gov/os/2009/02/P0085400behavadreport.pdf`.

[6]For example, in Eli Lilly and Co., 133 F.T.C. 763 (2002), the Commission accepted a consent order with a respondent that had disclosed personal information about individual consumers use of Prozac.

[7]Rep. at *i*.

[8]*See* Katherine Campbell et al., *The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market*, 11 J. COMPUTER. SECURITY 431 (2003) (an event study paper suggesting that firms that have confidential data breaches suffer significant negative market reactions).

harmed if they believe, mistakenly, that websites are incapable of tracking them (for purposes of behavioral advertising or otherwise)? How could the Commission minimize or avoid risks of over-promising?

- Staff has asked whether there are any circumstances where a take-it-or-leave it approach to tracking would be inappropriate. There is an extensive literature on the extent to which competition presses firms that use form contracts to offer a collection of attributes that best satisfy consumer tastes. Does that literature shed light on the significance of take-it-or-leave-it propositions related to the collection and use of data?

- In the case of Do-Not-Call, consumers fully internalize the costs and benefits of deciding to forego telemarketing; they are no longer annoyed by unwanted phone calls, but also forego any benefits associated with telemarketing. In the case of online behavioral advertising, however, consumers who opt out of tracking may externalize some of the costs of their decisions. Assuming a content provider continues to provide free content, consumers who opt-out of tracking contribute less to the provision of content than do consumers who do not opt out,[9] but enjoy the same content as those who agree to be tracked. It is possible that if online content providers can deny free access to those who opt out of tracking, they can prevent free riding. Setting prices is costly; if willingness to pay to avoid tracking varies substantially, the informational requirements to set access prices will be large. For a number of content providers, a price-for-content model is likely to provide less revenue than monetization via advertising; that most websites choose an ad-driven model rather than a direct fee model suggests that the former is a more efficient means than the latter to monetize content in most circumstances.[10] At the margin—which may be large—forcing firms away from their revealed-preferred method of monetization may reduce revenue and hence degrade quality. In discussing whether website content might be degraded by consumers choosing not to be tracked, how, if at all, should such risks impact the Commission's analysis?

- What is the optimal design of public institutions that will be responsible for making privacy policy?

[9] Because the ads will be random, rather than targeted based on user preferences, the price that content providers can charge advertisers to display ads on their websites is likely to fall, reducing the revenue generated. *See* Avi Goldfarb & Catherine Tucker, *Privacy Regulation and Online Advertising*, forthcoming in MGMT. SCI. (2011) (finding empirical evidence to suggest that online advertising in Europe became less effective after the EUs Privacy Directive), *available at*: `http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259&`. Non-tracked consumers may also view more advertisements, which are less likely to match their preferences.

[10] *See* David S. Evans, *The Online Advertising Industry: Economics, Evolution, and Privacy*, 23 J. ECON. PERSP. 37, 37 (2009) (77 percent of all page views for the top 100 sites earn most of their revenue from advertising).

Appendix E: Concurring Statement of Commissioner J. Thomas Rosch

Issuance of Preliminary FTC Staff Report *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*
December 1, 2010

Introduction

The Commission issues this Report today in order to continue the dialogue on issues related to consumer privacy and to solicit comment on a proposed new framework for how companies should protect consumers' privacy. I concur in the decision to issue the Report and seek critical comment on the issues it raises, but write separately to explain my serious reservations about the proposal advanced in the Report.

As a guide to Congress about what privacy protection law should look like,[1] the Report is flawed. First, insofar as the Report suggests that a new framework for consumer privacy should replace "notice" (or "harm") as the basis for Commission challenges relating to consumer privacy protection, that is unnecessary. A privacy notice that is opaque or fails to disclose material facts (such as the fact that consumer information may be shared with third parties) is deceptive under Section 5. That is particularly true if the sharing of the information may cause tangible harm. Moreover, Section 5 liability could not be avoided by eschewing a privacy notice altogether both because that would generally be competitive suicide and because that course would be deceptive in that it would entail a failure to disclose material facts.[2]

Second, insofar as the Report suggests that "notice and choice" has ever been a basis for law enforcement at the Commission (*see* Report at iii, 8-11), that suggestion is unfounded. Although the Commission has on several occasions challenged privacy notices that it considered deceptive, it has never challenged a firm's failure to offer a particular kind of "choice." For example, the Commission has never challenged an opt-out mechanism on the ground that it should have been an opt-in mechanism. Indeed, if the notice has been adequate, consumers have generally not had any choice other than to "take or leave it," and that choice has never been considered to be a Section 5 violation unless what was represented in the notice was different than what was actually done in practice.[3]

---

[1]The Report acknowledges that it is intended to "inform policymakers, including Congress, as they develop solutions, policies, and potential laws governing privacy." *See* Report at i, 2.

[2]The duty to disclose "material" facts would be triggered when the information was collected, used, or shared in a manner that "is likely to affect the consumers conduct or decision with regard to a product or service." *See* FTC Policy Statement on Deception, *appended to Cliffdale Associates, Inc.*, 103 F.T.C. 110, 174, 175 (1984). In some cases, disclosure would not have to be express. For example, using consumer information to provide order fulfillment would be disclosed by virtue of the transaction itself. *See also* Report at vi, 41, 52-53.

[3]The Report mentions "access" and "security" as aspirational privacy goals. *See* Report at 7. However, with the possible exception of the Childrens Online Privacy Protection Act, the Report does not suggest that Congress has ever enacted a special statute mandating "access," and the Report does

In short, to the extent that privacy notices have been buried, incomplete, or otherwise ineffective—and they have been—the answer is to enhance efforts to enforce the " notice" model, not to replace it with a new framework.

As a hortatory exercise, the Report is less problematic.[4] Many, if not all, of the "best practices" suggested are desirable. However, I disagree with the Report insofar as it suggests that even when the privacy notice is inadequate, the defect may be cured if consumers are offered some "meaningful choice" mechanism—whether it be opt in or opt out. *See* Report at 41, 52, 56-68. If firms are offered that alternative, that might disincentivize them from adopting acceptable privacy notices in the first place. That would be undesirable. Moreover, the Report takes no position as to whether the choice mechanism should be an opt-in or opt-out mechanism. *Id.* Because that question is left open, the Report can be read to portend that the final Report will suggest an opt-in option. More fundamentally, the self-regulation that is championed in this area (*see* Report at 8) may constitute a way for a powerful, well-entrenched competitor to raise the bar so as to create an entry barrier to a rival that may constrain the exercise of undue power. See Report at 48 (respecting self regulation as applicable to a "legacy system"). That possibility may be blunted by insuring that smaller rivals participate in the adoption of self-regulatory rules, but that may not be practical.

Analysis

The Report repeatedly acknowledges that the increasing flow of information provides important benefits to consumers and businesses.[5] Report at i, iv, 21, 33-35. Yet, despite the acknowledgment of these benefits, the Report, as written, leaves room in any final report for a prohibition against dissemination to third parties of non-sensitive information generally, and of information collected through behavioral tracking specifically.

First, based on testimony by some workshop participants, the Report asserts that the use being made of online and offline consumer information is contrary to consumer

not cite any instance in which "lack of access" has been a basis for a Commission law enforcement action. Moreover, except for the special statutes identified, the Report does not identify any special statute enacted by Congress that mandates " security" as such. The Commission has brought cases under the "unfairness" prong of Section 5 for failure to have reasonable security measures in place, but there was financial harm threatened in those cases.

[4]The Report asserts that there are a number of "best practices" that private firms should adopt from the get-go in order to protect privacy. *See* Report at v, 39, 40-41, 43-52. Most of these practices are desirable in the abstract. But that does not mean that firms should be mandated *de jure* (*i.e.*, by legislation) to adopt them or that firms should be required to do so *de facto* (*i.e.*, that large, well-entrenched firms engaging in "self-regulation" should dictate what the privacy practices of their competitors should be).

[5] "In particular, [workshop] panelists discussed benefits specific to business models such as online search, online behavioral advertising, social networking, cloud computing, mobile technologies, and health services. Participants noted that search engines provide customers with instant access to tremendous amounts of information at no charge to the consumer. Online advertising helps to support much of the content available to consumers online and allows personalized advertising that many consumers value. Social networking services permit users to connect with friends and share experiences online, in real time. These platforms also facilitate broader types of civic engagement on political and social issues." *See* Report at 33-34.

understanding. *See* Report at 25-26, 29. The Report also alleges that "consumer surveys have shown that a majority of consumers are uncomfortable with being tracked online." *Id.* at 29. Although some consumers may hold that view (which would be sufficient to make the practice of behavioral tracking a "material" fact), as the Report itself acknowledges it is inaccurate to assert that consumer surveys establish that "a majority of consumers" feel that way. *Id.* at 29 n.72. As others have observed, consumer surveys vary considerably in this respect. Of course, many consumers do not opt in to behavioral tracking when asked. But an even higher percentage do not opt out when given the chance to do so (and there is no solid evidence that is because they have not been able to make an informed choice).[6]

Second, the Report asserts that the "notice" model that the Commission has used in the past no longer works (*see* Report at iii, 19-20) and that the Commission should instead adopt the new framework proposed in the Report. Although the Report repeatedly asserts that this new framework "builds upon" the traditional Commission law enforcement model (*see* Report at v, 38-39, 40), it in fact would replace that model. To be sure, many, if not most, privacy policy disclosures are prolix and incomprehensible. But the appropriate remedy for opacity is to require notices to be clear, conspicuous and effective. If a consumer is provided with clear and conspicuous notice prior to the collection of information, there is no basis for concluding that a consumer cannot generally make an informed choice.[7] In addition, to the extent that the Commission has used a "harm" model based on the potential for physical or financial harm, or intangible harm constituting a violation of a special statute, that model may be a useful and legitimate framework.[8] However, the Commission could overstep its bounds if it were to begin considering "reputational harm" or "the fear of being monitored" or "other intangible privacy interests" (*see* Report at iii, 20, 31), generally when analyzing consumer injury. The Commission has specifically advised Congress that absent deception, it will not enforce Section 5 against alleged intangible harm.[9]

---

[6] *See, e.g.*, Thomas M. Lenhard and Paul H. Rubin, *Privacy and the Commercial Use of Personal Information: The Case of Customer Proprietary Network Information*, Progress on Point, at 6 (Aug. 2007)("[I]n testimony before the FTC on the experience of one firm, a witness indicated that, when the default was opt-in, 85 percent of consumers chose not to provide their data. In contrast, 95 percent chose to provide their data when the default was opt-out"), available at `http://www.pff.org/issues-pubs/pops/pop14.15lenardrubinCPNIprivacy.pdf`.

[7] The Report asserts there has been an "enormous growth in data processing and storage capabilities" (*see* Report at 24), and that there has been a proliferation of affiliates, information brokers and other information aggregators. See Report at 21, 23-24, 45-46, 68. But the Report does not explain how or why this phenomenon cannot be addressed by clear and conspicuous disclosures to consumers that their information may be aggregated in that fashion.

[8] The Commission has challenged practices threatening physical harm under Section 5 of the FTC Act. *See In re Intl Harvester Co.*, 104 F.T.C. 949 (1984). Moreover, it has challenged practices threatening intangible harm under special statutes enacted by Congress, specifically the Fair Credit Reporting Act, Gramm-Leach-Bliley Act, the Childrens Online Privacy Protection Act, and the Do Not Call amendments to the Telemarketing Sales Rule. *See* Report at 10-12. However, the Commission has not challenged practices threatening intangible harm under Section 5.

[9] Letter from the Federal Trade Commission to Hon. Wendell Ford and Hon. John Danforth, Committee on Commerce, Science and Transportation, United States Senate, Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction, *reprinted in In re Intl Harvester Co.*, 104 F.T.C. 949, 1070 (1984).

Third, as stated, the Report takes the position that an opt-in requirement may be triggered whenever there is a "material" change in the handling of the "other" information, including the sharing of non-sensitive information like behavioral tracking information, with third parties. *See* Report at 75-76. The Report is ambiguous as to whether this requirement would apply no matter how clear and conspicuous the disclosure of the prospect of material change was. *Compare* Report at 15, 75-76 *with* Report at 39, 76. Arguably, there is no warrant for requiring more than an opt-out requirement if that was what was initially required, when the disclosure of the material change and the ability to opt out is made clearly and conspicuously and the consumer actually receives the disclosure.

Fourth, insofar as the Report could be read as suggesting a ban on "take it or leave it" options (*see* Report at 60), again, clear and conspicuous disclosure is the most appropriate way to deal with such an option. I question whether such a ban would be constitutional and am also concerned about the impact of a ban on innovation.

Finally, if the traditional "notice" law enforcement model is to be augmented by some "choice" mechanism, I support a Do Not Track mechanism if it is technically feasible. However, I think consumers should have to "opt in" to use such a mechanism just as they have opted in to get on the Do Not Call Registry. Making access to the Do Not Track mechanism depend upon consumers opting in would not only parallel the Do Not Call model: it would give the Commission a much more reliable estimate of the percentage of consumers who really wish to prevent this type of tracking.

Conclusion

To the extent we have exercised our authority under Section 5, the "notice" model for privacy law enforcement has served this Commission long and well. Not only is there no warrant for discarding it now in favor of a proposed new framework that is as yet theoretical and untested, but in my judgment it would also be bad public policy to do so. To the contrary, if there is anything wrong with the "notice" model, it is that we do not enforce it stringently enough. Moreover, as the Bureau of Consumer Protection concedes, there are many benefits to the sharing of non-sensitive consumer information, and they may be endangered by the aspirational proposals advanced in the Report, however hortatory they may be.