This document contains excerpts from the recently issued FTC report:

"Protecting Consumer Privacy in an Era of Rapid Change" March 2012

http://ftc.gov/os/2012/03/120326privacyreport.pdf

Protecting Consumer Privacy in an Era of Rapid Change

RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS

FTC REPORT

FEDERAL TRADE COMMISSION | MARCH 2012

EXECUTIVE SUMMARY

In today's world of smart phones, smart grids, and smart cars, companies are collecting, storing, and sharing more information about consumers than ever before. Although companies use this information to innovate and deliver better products and services to consumers, they should not do so at the expense of consumer privacy.

With this Report, the Commission calls on companies to act now to implement best practices to protect consumers' private information. These best practices include making privacy the "default setting" for commercial data practices and giving consumers greater control over the collection and use of their personal data through simplified choices and increased transparency. Implementing these best practices will enhance trust and stimulate commerce.

This Report follows a preliminary staff report that the Federal Trade Commission ("FTC" or "Commission") issued in December 2010. The preliminary report proposed a framework for protecting consumer privacy in the 21st Century. Like this Report, the framework urged companies to adopt the following practices, consistent with the Fair Information Practice Principles first articulated almost 40 years ago:

- **Privacy by Design:** Build in privacy at every stage of product development;
- **Simplified Choice for Businesses and Consumers:** Give consumers the ability to make decisions about their data at a relevant time and context, including through a Do Not Track mechanism, while reducing the burden on businesses of providing unnecessary choices; and
- **Greater Transparency:** Make information collection and use practices transparent.

The Commission received more than 450 public comments in response to the preliminary report from various stakeholders, including businesses, privacy advocates, technologists and individual consumers. A wide range of stakeholders, including industry, supported the principles underlying the framework, and many companies said they were already following them. At the same time, many commenters criticized the slow pace of self-regulation, and argued that it is time for Congress to enact baseline privacy legislation. In this Report, the Commission addresses the comments and sets forth a revised, final privacy framework that adheres to, but also clarifies and fine-tunes, the basic principles laid out in the preliminary report.

Since the Commission issued the preliminary staff report, Congress has introduced both general privacy bills and more focused bills, including ones addressing Do Not Track and the privacy of teens. Industry has made some progress in certain areas, most notably, in responding to the preliminary report's call for Do Not Track. In other areas, however, industry progress has been far slower. Thus, overall, consumers do not yet enjoy the privacy protections proposed in the preliminary staff report.

The Administration and certain Members of Congress have called for enactment of baseline privacy legislation. The Commission now also calls on Congress to consider enacting baseline privacy legislation and reiterates its call for data security legislation. The Commission is prepared to work with Congress and other stakeholders to craft such legislation. At the same time, the Commission urges industry to accelerate the pace of self-regulation.

The remainder of this Executive Summary describes key developments since the issuance of the preliminary report, discusses the most significant revisions to the proposed framework, and lays out several next steps.

DEVELOPMENTS SINCE ISSUANCE OF THE PRELIMINARY REPORT

In the last 40 years, the Commission has taken numerous actions to shape the consumer privacy landscape. For example, the Commission has sued dozens of companies that broke their privacy and security promises, scores of telemarketers that called consumers on the Do Not Call registry, and more than a hundred scammers peddling unwanted spam and spyware. Since it issued the initial staff report, the Commission has redoubled its efforts to protect consumer privacy, including through law enforcement, policy advocacy, and consumer and business education. It has also vigorously promoted self-regulatory efforts.

On the law enforcement front, since December 2010, the Commission:

- Brought enforcement actions against Google and Facebook. The orders obtained in these cases require the companies to obtain consumers' affirmative express consent before materially changing certain of their data practices and to adopt strong, company-wide privacy programs that outside auditors will assess for 20 years. These orders will protect the more than one billion Google and Facebook users worldwide.
- Brought enforcement actions against online advertising networks that failed to honor opt outs. The orders in these cases are designed to ensure that when consumers choose to opt out of tracking by advertisers, their choice is effective.
- Brought enforcement actions against mobile applications that violated the Children's Online Privacy Protection Act as well as applications that set default privacy settings in a way that caused consumers to unwittingly share their personal data.
- Brought enforcement actions against entities that sold consumer lists to marketers in violation of the Fair Credit Reporting Act.
- Brought actions against companies for failure to maintain reasonable data security.

On the policy front, since December 2010, the FTC and staff:

- Hosted two privacy-related workshops, one on child identity theft and one on the privacy implications of facial recognition technology.
- Testified before Congress ten times on privacy and data security issues.
- Consulted with other federal agencies, including the Federal Communications Commission, the Department of Health and Human Services, and the Department of Commerce, on their privacy initiatives. The Commission has supported the Department of Commerce's initiative to convene stakeholders to develop privacy-related codes of conduct for different industry sectors.
- Released a survey of data collection disclosures by mobile applications directed to children.
- Proposed amendments to the Children's Online Privacy Protection Act Rule.

On the education front, since December 2010, the Commission:

- Continued outreach efforts through the FTC's consumer online safety portal, OnGuardOnline.gov, which provides information in a variety of formats – articles, games, quizzes, and videos – to help consumers secure their computers and protect their personal information. It attracts approximately 100,000 unique visitors per month.
- Published new consumer education materials on identity theft, Wi-Fi hot spots, cookies, and mobile devices.
- Sent warning letters to marketers of mobile apps that do background checks on individuals, educating them about the requirements of the Fair Credit Reporting Act.

To promote self-regulation, since December 2010, the Commission:

- Continued its call for improved privacy disclosures and choices, particularly in the area of online behavioral tracking. In response to this call, as well as to Congressional interest:
  - A number of Internet browser vendors developed browser-based tools for consumers to request that websites not track their online activities.
  - The World Wide Web Consortium, an Internet standard setting organization, is developing a universal web protocol for Do Not Track.
  - The Digital Advertising Alliance ("DAA"), a coalition of media and marketing organizations, has developed a mechanism, accessed through an icon that consumers can click, to obtain information about and opt out of online behavioral advertising. Additionally, the DAA has committed to preventing the use of consumers' data for secondary purposes like credit and employment and honoring the choices about tracking that consumers make through the settings on their browsers.
- Participated in the development of enforceable cross-border privacy rules for businesses to harmonize and enhance privacy protection of consumer data that moves between member countries of the forum on Asia Pacific Economic Cooperation.

THE FINAL REPORT

Based upon its analysis of the comments filed on the proposed privacy framework, as well as commercial and technological developments, the Commission is issuing this final Report. The final framework is intended to articulate best practices for companies that collect and use consumer data. These best practices can be useful to companies as they develop and maintain processes and systems to operationalize privacy and data security practices within their businesses. The final privacy framework contained in this Report is also intended to assist Congress as it considers privacy legislation. To the extent the framework goes beyond existing legal requirements, the framework is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC. While retaining the proposed framework's fundamental best practices of privacy by design, simplified choice, and greater transparency, the Commission makes revised recommendations in three key areas in response to the comments.

First, the Commission makes changes to the framework's scope. The preliminary report proposed that the privacy framework apply to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device. To address concerns about undue burdens on small businesses, the final framework does not apply to companies that collect only non-sensitive data from fewer than 5,000 consumers a year, provided they do not share the data with third parties. Commenters also expressed concern that, with improvements in technology and the ubiquity of public information, more and more data could be "reasonably linked" to a consumer, computer or device, and that the proposed framework provided less incentive for a business to try to de-identify the data it maintains. To address this issue, the Report clarifies that data is not "reasonably linkable" to the extent that a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data.

Second, the Commission revises its approach to how companies should provide consumers with privacy choices. To simplify choice for both consumers and businesses, the proposed framework set forth a list of five categories of "commonly accepted" information collection and use practices for which companies need not provide consumers with choice (product fulfillment, internal operations, fraud prevention, legal compliance and public purpose, and first-party marketing). Several business commenters expressed concern that setting these "commonly accepted practices" in stone would stifle innovation. Other commenters expressed the concern that the "commonly accepted practices" delineated in the proposed framework were too broad and would allow a variety of practices to take place without consumer consent.

In response to these concerns, the Commission sets forth a modified approach that focuses on the context of the consumer's interaction with the business. Under this approach, companies do not need to provide choice before collecting and using consumers' data for practices that are consistent with the context of the transaction, consistent with the company's relationship with the consumer, or as required or specifically authorized by law. Although many of the five "commonly accepted practices" identified in the preliminary report would generally meet this standard, there may be exceptions. The Report provides examples of how this new "context of the interaction" standard would apply in various circumstances.

Third, the Commission recommends that Congress consider enacting targeted legislation to provide greater transparency for, and control over, the practices of information brokers. The proposed framework recommended that companies provide consumers with reasonable access to the data the companies maintain about them, proportionate to the sensitivity of the data and the nature of its use. Several commenters discussed in particular the importance of consumers' ability to access information that information brokers have about them. These commenters noted the lack of transparency about the practices of information brokers, who often buy, compile, and sell a wealth of highly personal information about consumers but never interact directly with them. Consumers are often unaware of the existence of these entities, as well as the purposes for which they collect and use data.

The Commission agrees that consumers should have more control over the practices of information brokers and believes that appropriate legislation could help address this goal. Any such legislation could be

modeled on a bill that the House passed on a bipartisan basis during the 111th Congress, which included a procedure for consumers to access and dispute personal data held by information brokers.

IMPLEMENTATION OF THE PRIVACY FRAMEWORK

While Congress considers privacy legislation, the Commission urges industry to accelerate the pace of its self-regulatory measures to implement the Commission's final privacy framework. Although some companies have excellent privacy and data security practices, industry as a whole must do better. Over the course of the next year, Commission staff will promote the framework's implementation by focusing its policymaking efforts on five main action items, which are highlighted here and discussed further throughout the report.

- **Do Not Track:** As discussed above, industry has made significant progress in implementing Do Not Track. The browser vendors have developed tools that consumers can use to signal that they do not want to be tracked; the Digital Advertising Alliance ("DAA") has developed its own icon-based tool and has committed to honor the browser tools; and the World Wide Web Consortium ("W3C") has made substantial progress in creating an international standard for Do Not Track. However, the work is not done. The Commission will work with these groups to complete implementation of an easy-to use, persistent, and effective Do Not Track system.
- **Mobile:** The Commission calls on companies providing mobile services to work toward improved privacy protections, including the development of short, meaningful disclosures. To this end, FTC staff has initiated a project to update its business guidance about online advertising disclosures. As part of this project, staff will host a workshop on May 30, 2012 and will address, among other issues, mobile privacy disclosures and how these disclosures can be short, effective, and accessible to consumers on small screens. The Commission hopes that the workshop will spur further industry self-regulation in this area.
- **Data Brokers:** To address the invisibility of, and consumers' lack of control over, data brokers' collection and use of consumer information, the Commission supports targeted legislation – similar to that contained in several of the data security bills introduced in the 112th Congress – that would provide consumers with access to information about them held by a data broker. To further increase transparency, the Commission calls on data brokers that compile data for marketing purposes to explore creating a centralized website where data brokers could (1) identify themselves to consumers and describe how they collect and use consumer data and (2) detail the access rights and other choices they provide with respect to the consumer data they maintain.
- **Large Platform Providers:** To the extent that large platforms, such as Internet Service Providers, operating systems, browsers, and social media seek, to comprehensively track consumers' online activities, it raises heightened privacy concerns. To further explore privacy and other issues related to this type of comprehensive tracking, FTC staff intends to host a public workshop in the second half of 2012.

- **Promoting Enforceable Self-Regulatory Codes:** The Department of Commerce, with the support of key industry stakeholders, is undertaking a project to facilitate the development of sector-specific codes of conduct. FTC staff will participate in that project. To the extent that strong privacy codes are developed, the Commission will view adherence to such codes favorably in connection with its law enforcement work. The Commission will also continue to enforce the FTC Act to take action against companies that engage in unfair or deceptive practices, including the failure to abide by self-regulatory programs they join.

FINAL FTC PRIVACY FRAMEWORK AND IMPLEMENTATION RECOMMENDATIONS

The final privacy framework is intended to articulate best practices for companies that collect and use consumer data. These best practices can be useful to companies as they develop and maintain processes and systems to operationalize privacy and data security practices within their businesses. The final privacy framework contained in this report is also intended to assist Congress as it considers privacy legislation. To the extent the framework goes beyond existing legal requirements, the framework is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC.

SCOPE

Final 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, unless the entity collects only non-sensitive data from fewer than 5,000 consumers per year and does not share the data with third parties.

PRIVACY BY DESIGN

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

A. The Substantive Principles

Final Principle: Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy.

B. Procedural Protections to Implement the Substantive Principles

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

SIMPLIFIED CONSUMER CHOICE

Baseline Principle: Companies should simplify consumer choice.

A. Practices That Do Not Require Choice

Final Principle: Companies do not need to provide choice before collecting and using consumer data for practices that are consistent with the context of the transaction or the company's relationship with the consumer, or are required or specifically authorized by law.

To balance the desire for flexibility with the need to limit the types of practices for which choice is not required, the Commission has refined the final framework so that companies engaged in practices consistent with the context of their interaction with consumers need not provide choices for those practices.

B. Companies Should Provide Consumer Choice for Other Practices

Final Principle: 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. Companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes.

The Commission commends industry's efforts to improve consumer control over online behavioral tracking by developing a Do Not Track mechanism, and encourages continued improvements and full implementation of those mechanisms.

TRANSPARENCY

Baseline Principle: Companies should increase the transparency of their data practices.

A. Privacy notices

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

B. Access

Final Principle: 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.

The Commission has amplified its support for this principle by including specific recommendations governing the practices of information brokers.

C. Consumer Education

Final Principle: All stakeholders should expand their efforts to educate consumers about commercial data privacy practices.

LEGISLATIVE RECOMMENDATIONS

The Commission now also calls on Congress to consider enacting baseline privacy legislation and reiterates its call for data security and data broker legislation. The Commission is prepared to work with Congress and other stakeholders to craft such legislation. At the same time, the Commission urges industry to accelerate the pace of self-regulation.

FTC WILL ASSIST WITH IMPLEMENTATION IN FIVE KEY AREAS

As discussed throughout the Commission's final Report, there are a number of specific areas where policy makers have a role in assisting with the implementation of the self-regulatory principles that make up the final privacy framework. Areas where the FTC will be active over the course of the next year include the following:

1. Do Not Track

Industry has made significant progress in implementing Do Not Track. The browser vendors have developed tools that consumers can use to signal that they do not want to be tracked; the DAA has developed its own icon-based tool and has committed to honor the browser tools; and the W3C has made substantial progress in creating an international standard for Do Not Track. However, the work is not done. The Commission will work with these groups to complete implementation of an easy-to use, persistent, and effective Do Not Track system.

2. Mobile

The Commission calls on companies providing mobile services to work toward improved privacy protections, including the development of short, meaningful disclosures. To this end, FTC staff has initiated a project to update its business guidance about online advertising disclosures. As part of this project, staff will host a workshop on May 30, 2012 and will address, among other issues, mobile privacy disclosures and how these disclosures can be short, effective, and accessible to consumers on small screens. The Commission hopes that the workshop will spur further industry self-regulation in this area.

3. Data Brokers

To address the invisibility of, and consumers' lack of control over, data brokers' collection and use of consumer information, the Commission supports targeted legislation – similar to that contained in several of the data security bills introduced in the 112th Congress – that would provide consumers with access to information about them held by a data broker. To further increase transparency, the Commission calls on data brokers that compile data for marketing purposes to explore creating a centralized website where data brokers could (1) identify themselves to consumers and describe how they collect and use consumer data and (2) detail the access rights and other choices they provide with respect to the consumer data they maintain.

4. Large Platform Providers

To the extent that large platforms, such as Internet Service Providers, operating systems, browsers, and social media, seek to comprehensively track consumers' online activities, it raises heightened privacy concerns. To further explore privacy and other issues related to this type of comprehensive tracking, FTC staff intends to host a public workshop in the second half of 2012.

5. Promoting Enforceable Self-Regulatory Codes

The Department of Commerce, with the support of key industry stakeholders, is undertaking a project to facilitate the development of sector-specific codes of conduct. FTC staff will participate in that project. To the extent that strong privacy codes are developed, the Commission will view adherence to such codes favorably in connection with its law enforcement work. The Commission will also continue to enforce the FTC Act to take action against companies that engage in unfair or deceptive practices, including the failure to abide by self-regulatory programs they join.

In all other areas, the Commission calls on individual companies, trade associations, and self-regulatory bodies to adopt the principles contained in the final privacy framework, to the extent they have not already done so. For its part, the FTC will focus its policy efforts on the five areas identified above, vigorously enforce existing laws, work with industry on self-regulation, and continue to target its education efforts on building awareness of existing data collection and use practices and the tools to control them.

B. PRIVACY BY DESIGN

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

The preliminary staff report called on companies to promote consumer privacy throughout their organizations and at every stage of the development of their products and services. Although many companies already incorporate substantive and procedural privacy protections into their business practices, industry should implement privacy by design more systematically. A number of commenters, including those representing industry, supported staff's call that companies "build in" privacy, with several of these commenters citing to the broad international recognition and adoption of privacy by design.[115] The Commission is encouraged to see broad support for this concept, particularly in light of the increasingly global nature of data transfers.

111 Letter from Maneesha Mithal, Assoc. Dir., Div. of Privacy & Identity Prot., FTC, to Reed Freeman, Morrison & Foerster LLP, Counsel for Netflix, 2 (Mar. 12, 2010), *available at* http://www.ftc.gov/os/closings/100312netflixletter.pdf (closing letter).

112 *Id.*

113 To the extent that a company maintains and uses both data that is identifiable and data that it has taken steps to de-identify as outlined here, the company should silo the data separately.

114 A company that violates its policy against re-identifying data could be subject to liability under the FTC Act or other laws.

115 *Comment of Office of the Information and Privacy Commissioner of Ontario*, cmt. #00239, at 2-3; *Comment of Intel Corp.*, cmt. #00246, at 12-13; *Comment of CNIL*, cmt. #00298, at 2-3.

In calling for privacy by design, staff advocated for the implementation of substantive privacy protections – such as data security, limitations on data collection and retention, and data accuracy – as well as procedural safeguards aimed at integrating the substantive principles into a company's everyday business operations. By shifting burdens away from consumers and placing obligations on businesses to treat consumer data in a responsible manner, these principles should afford consumers basic privacy protections without forcing them to read long, incomprehensible privacy notices to learn and make choices about a company's privacy practices. Although the Commission has not changed the proposed "privacy by design" principles, it responds to a number of comments, as discussed below.

1. THE SUBSTANTIVE PRINCIPLES: DATA SECURITY, REASONABLE COLLECTION LIMITS, SOUND RETENTION PRACTICES, AND DATA ACCURACY.

Proposed Principle: Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention practices, and data accuracy.

a. Should Additional Substantive Principles Be Identified?

Responding to a question about whether the final framework should identify additional substantive protections, several commenters suggested incorporating the additional principles articulated in the 1980 OECD Privacy Guidelines.[116] One commenter also proposed adding the "right to be forgotten," which would allow consumers to withdraw data posted online about themselves at any point.[117] This concept has gained importance as people post more information about themselves online without fully appreciating the implications of such data sharing or the persistence of online data over time.[118] In supporting an expansive view of privacy by design, a consumer advocacy group noted that the individual elements and principles of the proposed framework should work together holistically.[119]

In response, the Commission notes that the framework already embodies all the concepts in the 1980 OECD privacy guidelines, although with some updates and changes in emphasis. For example, privacy by design includes the collection limitation, data quality, and security principles. Additionally, the framework's simplified choice and transparency components, discussed below, encompass the OECD principles of purpose specification, use limitation, individual participation, and openness. The framework also adopts the

116 *Comment of CNIL*, cmt. #00298, at 2; *Comment of the Information Commissioner's Office of the UK*, cmt. #00249, at 2; *Comment of World Privacy Forum*, cmt. #00369, at 7; *Comment of Intel Corp.*, cmt. #00246, at 4; *see also* Organisation for Economic Co-operation & Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Sept. 1980), *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 include purpose specification, individual participation, accountability, and principles to govern cross-border data transfers). Another commenter called for baseline legislation based on the Fair Information Practice Principles and the principles outlined in the 1974 Privacy Act. *Comment of Electronic Privacy Information Center*, cmt. #00386, at 17-20.

117 *Comment of CNIL*, cmt. #00298, at 3.

118 The concept of the "right to be forgotten," and its importance to young consumers, is discussed in more detail below in the Transparency Section, *infra* at Section IV.D.2.b.

119 *Comment of Consumers Union*, cmt. #00362, at 1-2, 5-9, 18-19.

OECD principle that companies must be accountable for their privacy practices. Specifically, the framework calls on companies to implement procedures – such as designating a person responsible for privacy, training employees, and ensuring adequate oversight of third parties – to help ensure that they are implementing appropriate substantive privacy protections. The framework also calls on industry to increase efforts to educate consumers about the commercial collection and use of their data and the available privacy tools. In addition, there are aspects of the proposed "right to be forgotten" in the final framework, which calls on companies to (1) delete consumer data that they no longer need and (2) allow consumers to access their data and in appropriate cases suppress or delete it.[120]

All of the principles articulated in the preliminary staff report are intended to work together to shift the burden for protecting privacy away from consumers and to encourage companies to make strong privacy protections the default. Reasonable collection limits and data disposal policies work in tandem with streamlined notices and improved consumer choice mechanisms. Together, they function to provide substantive protections by placing reasonable limits on the collection, use, and retention of consumer data to more closely align with consumer expectations, while also raising consumer awareness about the nature and extent of data collection, use, and third-party sharing, and the choices available to them.

b. Data Security: Companies Must Provide Reasonable Security for Consumer Data.

It is well settled that companies must provide reasonable security for consumer data. The Commission has a long history of enforcing data security obligations under Section 5 of the FTC Act, the FCRA and the GLBA. Since 2001, the FTC has brought 36 cases under these laws, charging that businesses failed to appropriately protect consumers' personal information. Since issuance of the preliminary staff report alone, the Commission has resolved seven data security actions against resellers of sensitive consumer report information, service providers that process employee data, a college savings program, and a social media service.[121] In addition to the federal laws the FTC enforces, companies are subject to a variety of

120 *See In the Matter of Facebook, Inc.*, FTC File No. 092 3184 (Nov. 29, 2011) (proposed consent order), *available at* http://www.ftc.gov/os/caselist/0923184/index.shtm (requiring Facebook to make inaccessible within thirty days data that a user deletes); *see also* Do Not Track Kids Act of 2011, H.R. 1895, 112th Cong. (2011).

121 *In the Matter of Upromise, Inc.*, FTC File No. 102 3116 (Jan. 18, 2012) (proposed consent order), *available at* http://www.ftc.gov/os/caselist/1023116/index.shtm; *In the Matter of ACRAnet, Inc.*, FTC Docket No. C-4331(Aug. 17, 2011) (consent order), *available at* http://ftc.gov/os/caselist/0923088/index.shtm; *In the Matter of Fajilan & Assocs., Inc.*, FTC Docket No. C-4332 (Aug. 17, 2011) (consent order), *available at* http://ftc.gov/os/caselist/0923089/index.shtm; *In the Matter of SettlementOne Credit Corp.*, FTC Docket No. C-4330 (Aug. 17, 2011) (consent order), *available at* http://ftc.gov/os/caselist/0823208/index.shtm; *In the Matter of Lookout Servs., Inc.*, FTC Docket No. C-4326 (June 15, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/102376/index.shtm; *In the Matter of Ceridian Corp.*, FTC Docket No. C-4325 (June 8, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023160/index.shtm; *In the Matter of Twitter, Inc.*, FTC Docket No. C-4316 (Mar. 11, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/0923093/index.shtm.

other federal and state law obligations. In some industries, such as banking, federal regulators have given additional guidance on how to define reasonable security.[122]

The Commission also promotes better data security through consumer and business education. For example, the FTC sponsors OnGuard Online, a website to educate consumers about basic computer security.[123] Since the Commission issued the preliminary staff report there have been over 1.5 million unique visits to OnGuard Online and its Spanish-language counterpart Alerta en Línea. The Commission's business outreach includes general advice about data security as well as specific advice about emerging topics.[124]

The Commission also notes that the private sector has implemented a variety of initiatives in the security area, including the Payment Card Institute Data Security Standards for payment card data, the SANS Institute's security policy templates, and standards and best practices guidelines for the financial services industry provided by BITS, the technology policy division of the Financial Services Roundtable.[125] These standards can provide useful guidance on appropriate data security measures that organizations should implement for specific types of consumer data or in specific industries. The Commission further calls on industry to develop and implement best data security practices for additional industry sectors and other types of consumer data.

Because this issue is important to consumers and because businesses have existing legal and self-regulatory obligations, many individual companies have placed great emphasis and resources on maintaining reasonable security. For example, Google has cited certain security features in its products, including default SSL encryption for Gmail and security features in its Chrome browser.[126] Similarly, Mozilla has noted that

122 *See, e.g.*, Federal Financial Institutions Examination Council ("FFIEC"), *Information Society IT Examination Handbook* (July 2006), *available at* http://ithandbook.ffiec.gov/it-booklets/information-security.aspx; Letter from Richard Spillenkothen, Dir., Div. of Banking Supervision & Regulation, Bd. of Governors of the Fed. Reserve Sys., *SRO1-11: Identity Theft and Pretext Calling* (Apr. 26, 2011), *available at* http://www.federalreserve.gov/boarddocs/srletters/2001/sr0111.htm (guidance on pretexting and identity theft); Securities & Exchange Commission, *CF Disclosure Guidance: Topic No. 2, on Cybersecurity* (Oct. 13, 2011), *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm; U.S. Small Business Administration, Information Security Guidance, http://www.sba.gov/content/information-security; National Institute of Standards & Technology, Computer Security Division, *Computer Security Resource Center*, *available at* http://csrc.nist.gov/groups/SMA/sbc/index.html; HHS, Health Information Privacy, *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html (guidance and educational materials for entities required to comply with the HIPPA Privacy and Security Rules); Centers from Medicare and Medicaid Services, *Educational Materials*, *available at* http://www.cms.gov/EducationMaterials/ (educational materials for HIPPA compliance).

123 FTC, OnGuard Online, http://onguardonline.gov/.

124 *See* FTC, *Protecting Personal Information: A Guide for Business* (Nov. 2011), *available at* http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business; *see generally* FTC, Bureau of Consumer Protection Business Center, Data Security Guidance, *available at* http://business.ftc.gov/privacy-and-security/data-security.

125 *See* PCI Security Standards Council, *PCI SSC Data Security Standards Overview*, *available at* https://www.pcisecuritystandards.org/security_standards/; SANS Institute, *Information Security Policy Templates, available at* http://www.sans.org/security-resources/policies/; BITS, *Financial Services Roundtable BITS Publications*, *available at* http://www.bits.org/publications/index.php; *see also, e.g.*, Better Business Bureau, *Security and Privacy – Made Simpler: Manageable Guidelines to help You Protect Your Customers' Security & Privacy from Identity Theft & Fraud*, *available at* http://www.bbb.org/us/storage/16/documents/SecurityPrivacyMadeSimpler.pdf; National Cyber Security Alliance, *For Business*, http://www.staysafeonline.org/for-business (guidance for small and midsize businesses); Direct Marketing Association, *Information Security: Safeguarding Personal Data in Your Care* (May 2005), *available at* http://www.the-dma.org/privacy/InfoSecData.pdf; Messaging Anti-Abuse Working Group & Anti-Phishing Working Group, *Anti-Phishing Best Practices for ISPs and Mailbox Providers* (July 2006), *available at* http://www.antiphishing.org/reports/bestpracticesforisps.pdf.

126 *Comment of Google Inc.*, cmt. #00417, at 2-3.

its cloud storage system encrypts user data using SSL communication.[127] Likewise, Twitter has implemented encryption by default for users logged into its system.[128] The Commission commends these efforts and calls on companies to continue to look for additional ways to build data security into products and services from the design stage.

Finally, the Commission reiterates its call for Congress to enact data security and breach notification legislation. To help deter violations, such legislation should authorize the Commission to seek civil penalties.

c. Reasonable Collection Limitation: Companies Should Limit Their Collection of Data.

The preliminary staff report called on companies to collect only the data they need to accomplish a specific business purpose. Many commenters expressed support for the general principle that companies should limit the information they collect from consumers.[129] Despite the broad support for the concept, however, many companies argued for a flexible approach based on concerns that allowing companies to collect data only for existing business needs would harm innovation and deny consumers new products and services.[130] One commenter cited Netflix's video recommendation feature as an example of how secondary uses of data can create consumer benefits. The commenter noted that Netflix originally collected information about subscribers' movie preferences in order to send the specific videos requested, but later used this information as the foundation for generating personalized recommendations to its subscribers.[131]

In addition, commenters raised concerns about who decides what a "specific business purpose" is.[132] For example, one purpose for collecting data is to sell it to third parties in order to monetize a service and provide it to consumers for free. Would collecting data for this purpose be a specific business purpose? If not, is the only alternative to charge consumers for the service, and would this result be better for consumers?

As an alternative to limiting collection to accomplish a "specific business purpose," many commenters advocated limiting collection to business purposes *that are clearly articulated*. This is akin to the Fair Information Practice Principle of "purpose specification," which holds that companies should specify to consumers all of the purposes for which information is collected at the time of collection. One commenter supported purpose specification statements in general categories to allow innovation and avoid making privacy policies overly complex.[133]

---

127 *Comment of Mozilla*, cmt. #00480, at 7.

128 *See* Chloe Albanesius, *Twitter Adds Always-On Encryption*, PC Magazine, Feb. 12, 2012, http://www.pcmag.com/article2/0,2817,2400252,00.asp.

129 *See, e.g.*, *Comment of Intel Corp.*, cmt. #00246, at 4-5, 7, 40-41; *Comment of Electronic Frontier Foundation*, cmt. #00400, at 4-6; *Comment of Center for Democracy & Technology*, cmt. #00469, at 4-5; *Comment of Electronic Privacy Information Center*, cmt. #00386, at 18.

130 *See, e.g.*, *Comment of Facebook, Inc.*, cmt. #00413, at 2, 7-8, 18; *Comment of Google Inc.*, cmt. #00417, at 4; *Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 14-15; *Comment of Intuit, Inc.*, cmt. #00348, at 5, 9; *Comment of TRUSTe*, cmt. #00450, at 9.

131 *Comment of Facebook, Inc.*, cmt. #00413, at 7-8.

132 *See Comment of SAS*, cmt. #00415, at 51; *Comment of Yahoo! Inc.*, cmt. #00444, at 5.

133 *Comment of Yahoo! Inc.*, cmt. #00444, at 5.

The Commission recognizes the need for flexibility to permit innovative new uses of data that benefit consumers. At the same time, in order to protect consumer privacy, there must be some reasonable limit on the collection of consumer data. General statements in privacy policies, however, are not an appropriate tool to ensure such a limit because companies have an incentive to make vague promises that would permit them to do virtually anything with consumer data.

Accordingly, the Commission clarifies the collection limitation principle of the framework as follows: Companies should limit data collection to that which is consistent with the context of a particular transaction or the consumer's relationship with the business, or as required or specifically authorized by law.[134] For any data collection that is inconsistent with these contexts, companies should make appropriate disclosures to consumers at a relevant time and in a prominent manner – outside of a privacy policy or other legal document. This clarification of the collection limitation principle is intended to help companies assess whether their data collection is consistent with what a consumer might expect; if it is not, they should provide prominent notice and choice. (For a further discussion of this point, see *infra* Section IV.C.2.) This approach is consistent with the Administration's Consumer Privacy Bill of Rights, which includes a Respect for Context principle that limits the use of consumer data to those purposes consistent with the context in which consumers originally disclosed the data.[135]

One example of a company innovating around the concept of privacy by design through collection limitation is the Graduate Management Admission Council ("GMAC"). This entity previously collected fingerprints from individuals taking the Graduate Management Admission Test. After concerns were raised about individuals' fingerprints being cross-referenced against criminal databases, GMAC developed a system that allowed for collection of palm prints that could be used solely for test-taking purposes.[136] The palm print technology is as accurate as fingerprinting but less susceptible to "function creep" over time than the taking of fingerprints, because palm prints are not widely used as a common identifier. GMAC received a privacy innovation award for small businesses for its work in this area.

d. Sound Data Retention: Companies Should Implement Reasonable Data Retention and Disposal Policies.

Similar to the concerns raised about collection limits, many commenters expressed concern about limiting retention of consumer data, asserting that such limits would harm innovation. Trade associations and businesses requested a flexible standard for data retention to allow companies to develop new products

134 This approach mirrors the revised standard for determining whether a particular data practice warrants consumer choice (see *infra* at section IV.C.1.a.) and is consistent with a number of commenters' calls for considering the context in which a particular practice takes place. *See, e.g.*, *Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 2-4; *Comment of Consumer Data Industry Ass'n*, cmt. #00363, at 5; *Comment of TRUSTe*, cmt. #00450, at 3.

135 *See* White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, 15-19, (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf. For a further discussion of this point, see *infra* at Section IV.C.1.a.

136 *See* Jay Cline, *GMAC: Navigating EU Approval for Advanced Biomterics*, Inside Privacy Blog (Oct. 15, 2010), https://www.privacyassociation.org/publications/2010_10_20_gmac_navigating_eu_approval_for_advanced_biometrics (explaining GMAC's adoption of palm print technology); *cf.* Kashmir Hill, *Why 'Privacy by Design' is the New Corporate Hotness*, Forbes, July 28, 2011, *available at* http://www.forbes.com/sites/kashmirhill/2011/07/28/why-privacy-by-design-is-the-new-corporate-hotness/.

and other uses of data that provide benefits to consumers.[137] One company raised concerns about prescriptive retention periods, arguing that retention standards instead should be based on business need, the type and location of data at issue, operational issues, and legal requirements.[138] Other commenters noted that retention limits should be sufficiently flexible to accommodate requests from law enforcement or other legitimate business purposes, such as the need of a mortgage banker to retain information about a consumer's payment history.[139] Some commenters suggested that the Commission's focus should be on data security and proper handling of consumer data, rather than on retention limits.[140]

In contrast, some consumer groups advocated specific retention periods. For example, one such commenter cited a proposal made by a consortium of consumer groups in 2009 that companies that collect data for online behavioral advertising should limit their retention of the data to three months and that companies that retained their online behavioral advertising data for only 24 hours may not need to obtain consumer consent for their data collection and use.[141] Others stated that it might be appropriate for the FTC to recommend industry-specific retention periods after a public consultation.[142]

The Commission confirms its conclusion that companies should implement reasonable restrictions on the retention of data and should dispose of it once the data has outlived the legitimate purpose for which it was collected.[143] Retention periods, however, can be flexible and scaled according to the type of relationship and use of the data; for example, there may be legitimate reasons for certain companies that have a direct relationship with customers to retain some data for an extended period of time. A mortgage company will maintain data for the life of the mortgage to ensure accurate payment tracking; an auto dealer will retain data from its customers for years to manage service records and inform its customers of new offers. These long retention periods help maintain productive customer relationships. This analysis does not, however, apply to all data collection scenarios. A number of commenters noted that online behavioral advertising data often becomes stale quickly and need not be retained long.[144] For example, a consumer researching hotels in a particular city for an upcoming vacation is unlikely to be interested in continuing to see hotel advertisements after the trip is completed. Indefinite retention of data about the consumer's interest in finding a hotel for a particular weekend serves little purpose and could result in marketers sending the consumer irrelevant advertising.

137 *See Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 2-4, 14; *Comment of American Catalog Mailers Ass'n,* cmt. #000424, at 5; *Comment of IBM*, cmt. #00433, at 4; *Comment of Intuit, Inc.*, cmt. #00348, at 9.

138 *Comment of Verizon*, cmt. #00428, at 10-11.

139 *See, e.g.*, C*omment of CTIA - The Wireless Ass'n*, cmt. #00375, at 14.

140 *Comment of Yahoo! Inc.*, cmt. #00444, at 6; *see also Comment of American Catalog Mailers Ass'n*, cmt. #00424, at 3-4.

141 *Comment of Consumer Federation of America*, cmt. #00358, at 4 (citing *Legislative Primer: Online Behavioral Tracking and Targeting Concerns and Solutions from the Perspective of the Center for Digital Democracy and U.S. PIRG, Consumer Federation of America, Consumers Union, Consumer Watchdog, Electronic Frontier Foundation, Privacy Lives, Privacy Rights Clearinghouse, Privacy Times, U.S. Public Interest Research group, The World Privacy Forum* (Sept. 2009), *available at* http://www.consumerfed.org/elements/www.consumerfed.org/file/OnlinePrivacyLegPrimerSEPT09.pdf).

142 *Comment of Center for Democracy & Technology*, cmt. #00469, at 6 ("Flexible approaches to data retention should not, however, give *carte blanche* to companies to maintain consumer data after it has outlived its reasonable usefulness.").

143 In the alternative, companies may consider taking steps to de-identify the data they maintain, as discussed above.

144 *See Comment of Consumers Union*, cmt. #00362, at 8.

In determining when to dispose of data, as well as limitations on collection described above, companies should also take into account the nature of the data they collect. For example, consider a company that develops an online interactive game as part of a marketing campaign directed to teens. The company should first assess whether it needs to collect the teens' data as part of the game, and if so, how it could limit the data collected, such as by allowing teens to create their own username instead of using a real name and email address. If the company decides to collect the data, it should consider disposing of it even more quickly than it would if it collected adults' data. Similarly, recognizing the sensitivity of data such as a particular consumer's real time location, companies should take special care to delete this data as soon as possible, consistent with the services they provide to consumers.

Although restrictions may be tailored to the nature of the company's business and the data at issue, companies should develop clear standards and train its employees to follow them. Trade associations and self-regulatory groups also should be more proactive in providing guidance to their members about retention and data destruction policies. Accordingly, the Commission calls on industry groups from all sectors – the online advertising industry, online publishers, mobile participants, social networks, data brokers and others – to do more to provide guidance in this area. Similarly, the Commission generally supports the exploration of efforts to develop additional mechanisms, such as the "eraser button" for social media discussed below,[145] to allow consumers to manage and, where appropriate, require companies to delete the information consumers have submitted.

e. Accuracy: Companies should maintain reasonable accuracy of consumers' data.

The preliminary staff report called on companies to take reasonable steps to ensure the accuracy of the data they collect and maintain, particularly if such data could cause significant harm or be used to deny consumers services. Similar to concerns raised about collection limits and retention periods, commenters opposed rigid accuracy standards,[146] and noted that the FCRA already imposes accuracy standards in certain contexts.[147] One commenter highlighted the challenges of providing the same levels of accuracy for non-identifiable data versus data that is identifiable.[148]

To address these challenges, some commenters stated that a sliding scale approach should be followed, particularly for marketing data. These commenters stated that marketing data is not used for eligibility purposes and that, if inaccurate, the only harm a consumer may experience is an irrelevant advertisement.[149] Providing enhanced accuracy standards for marketing data would raise additional privacy and data security concerns,[150] as additional information may need to be added to marketing databases to increase accuracy.[151]

145 See *infra* at Section IV.D.2.b.

146 *See Comment of Experian*, cmt. #00398, at 2.

147 *See Comment of SIFMA*, cmt. #00265, at 4.

148 *Comment of Phorm Inc.*, cmt. #00353, at 4.

149 *Comment of Experian*, cmt. #00398, at 11 (arguing against enhanced standards for accuracy, access, and correction for marketing data); *see also Comment of Yahoo! Inc.*, cmt. #00444, at 6-7.

150 *Id.*

151 *Cf. Comment of Yahoo! Inc.*, cmt. #00444, at 7 (arguing that it would be costly, time consuming, and contrary to privacy objectives to verify the accuracy of user registration information such as gender, age or hometown).

The Commission agrees that the best approach to improving the accuracy of the consumer data companies collect and maintain is a flexible one, scaled to the intended use and sensitivity of the information. Thus, for example, companies using data for marketing purposes need not take special measures to ensure the accuracy of the information they maintain. Companies using data to make decisions about consumers' eligibility for benefits should take much more robust measures to ensure accuracy, including allowing consumers access to the data and the opportunity to correct erroneous information.[152]

Final Principle: Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy.

2. COMPANIES SHOULD ADOPT PROCEDURAL PROTECTIONS TO IMPLEMENT THE SUBSTANTIVE PRINCIPLES.

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

In addition to the substantive principles articulated above, the preliminary staff report called for organizations to maintain comprehensive data management procedures, such as designating personnel responsible for employee privacy training and regularly assessing the privacy impact of specific practices, products, and services. Many commenters supported this call for accountability within an organization.[153] Commenters noted that privacy risk assessments promote accountability, and help identify and address privacy issues.[154] One commenter stated that privacy risk assessments should be an ongoing process, and findings should be used to update internal procedures.[155] The Commission agrees that companies should implement accountability mechanisms and conduct regular privacy risk assessments to ensure that privacy issues are addressed throughout an organization.

The preliminary staff report also called on companies to "consider privacy issues systemically, at all stages of the design and development of their products and services." A range of commenters supported the principle of "baking" privacy into the product development process.[156] One commenter stated that this approach of including privacy considerations in the product development process was preferable to requiring

152 See *infra* at Section IV.D.2. The Commission notes that some privacy-enhancing technologies operate by introducing deliberate "noise" into data. The data accuracy principle is not intended to rule out the appropriate use of these methods, provided that the entity using them notifies any recipients of the data that it is inaccurate.

153 *See, e.g.*, *Comment of The Centre for Information Policy Leadership at Hunton & Williams LLP*, cmt. #00360, at 2-3; *Comment of Intel Corp.*, cmt. #00246, at 6; *Comment of Office of the Information & Privacy Commissioner of Ontario*, cmt. #00239, at 3.

154 *Comment of GS1*, cmt. #00439, at 3; *Comment of Office of the Information & Privacy Commissioner of Ontario*, cmt. #00239, at 6.

155 *Comment of Office of the Information & Privacy Commissioner of Ontario*, cmt. #00239, at 7.

156 *Comment of Intel Corp.*, cmt. #00246, at 6; *Comment of United States Council for International Business*, cmt. #00366, at 2; *Comment of Consumer Federation of America*, cmt. #00358, at 3.

after-the-fact reviews.[157] Another argued that privacy concerns should be considered from the outset, but observed that such concerns should continue to be evaluated as the product, service, or feature evolves.[158]

The Commission's recent settlements with Google and Facebook illustrate how the procedural protections discussed above might work in practice.[159] In both cases, the Commission alleged that the companies deceived consumers about the level of privacy afforded to their data.

The FTC's orders will require the companies to implement a comprehensive privacy program reasonably designed to address privacy risks related to the development and management of new and existing products and services and to protect the privacy and confidentiality of "covered information," defined broadly to mean *any* information the companies collect from or about a consumer.

The privacy programs that the orders mandate must, at a minimum, contain certain controls and procedures, including: (1) the designation of personnel responsible for the privacy program; (2) a risk assessment that, at a minimum, addresses employee training and management and product design and development; (3) the implementation of controls designed to address the risks identified; (4) appropriate oversight of service providers; and (5) evaluation and adjustment of the privacy program in light of regular testing and monitoring.[160] Companies should view the comprehensive privacy programs mandated by these consent orders as a roadmap as they implement privacy by design in their own organizations.

As an additional means of implementing the substantive privacy by design protections, the preliminary staff report advocated the use of privacy-enhancing technologies ("PETs") – such as encryption and anonymization tools – and requested comment on implementation of such technologies. One commenter stressed the need for "privacy-aware design," calling for techniques such as obfuscation and cryptography to reduce the amount of identifiable consumer data collected and used for various products and services.[161] Another stressed that PETs are a better approach in this area than rigid technical mandates.[162]

The Commission agrees that a flexible, technology-neutral approach towards developing PETs is appropriate to accommodate the rapid changes in the marketplace and will also allow companies to innovate on PETs. Accordingly, the Commission calls on companies to continue to look for new ways to protect consumer privacy throughout the life cycle of their products and services, including through the development and deployment of PETs.

Finally, Commission staff requested comment on how to apply the substantive protections articulated above to companies with legacy data systems. Many commenters supported a phase-out period for legacy data systems, giving priority to systems that contain sensitive data.[163] Another commenter suggested that

157 *Comment of Intel Corp.*, cmt. #00246, at 6.

158 *Comment of Zynga Inc.*, cmt. #00459, at 2.

159 Of course, the privacy programs required by these orders may not be appropriate for all types and sizes of companies that collect and use consumer data.

160 *In the Matter of Google Inc.*, FTC Docket No. C-4336 (Oct. 13, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/index.shtm.

161 *Comment of Electronic Frontier Foundation*, cmt. #00400, at 5.

162 *Comment of Business Software Alliance*, cmt. #00389, at 7-9.

163 *Comment of The Centre for Information Policy Leadership at Hunton & Williams LLP*, cmt. #00360, at 3; *Comment of the Information Commissioner's Office of the UK*, cmt. #00249, at 2; *Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 14.

imposing strict access controls on legacy data systems until they can be updated would enhance privacy.[164] Although companies need to apply the various substantive privacy by design elements to their legacy data systems, the Commission recognizes that companies need a reasonable transition period to update their systems. In applying the substantive elements to their legacy systems, companies should prioritize those systems that contain sensitive data and they should appropriately limit access to all such systems until they can update them.

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

164 *Comment of Yahoo! Inc.*, cmt. #00444, at 7.

DATA COLLECTION AND DISPOSAL CASE STUDY: MOBILE

The rapid growth of the mobile marketplace illustrates the need for companies to implement reasonable limits on the collection, transfer, and use of consumer data and to set policies for disposing of collected data. The unique features of a mobile phone – which is highly personal, almost always on, and travels with the consumer – have facilitated unprecedented levels of data collection. Recent news reports have confirmed the extent of this ubiquitous data collection. Researchers announced, for example, that Apple had been collecting geolocation data through its mobile devices over time, and storing unencrypted data files containing this information on consumers' computers and mobile devices.[1] The Wall Street Journal has documented numerous companies gaining access to detailed information – such as age, gender, precise location, and the unique ID associated with a particular mobile device – that can then be used to track and predict consumer behavior.[2] Not surprisingly, consumers are concerned: for example, a recent Nielsen study found that a majority of smartphone app users worry about their privacy when it comes to sharing their location through a mobile device.[3] The Commission calls on companies to limit collection to data they need for a requested service or transaction. For example, a wallpaper app or an app that tracks stock quotes does not need to collect location information.[4]

The extensive collection of consumer information – particularly location information – through mobile devices also heightens the need for companies to implement reasonable policies for purging data.[5] Without data retention and disposal policies specifically tied to the stated business purpose for the data collection, location information could be used to build detailed profiles of consumer movements over time that could be used in ways not anticipated by consumers.[6] Location information is particularly useful for uniquely identifying (or re-identifying) individuals using disparate bits of data.[7] For example, a consumer can use a mobile application on her cell phone to "check in" at a restaurant for the purpose of finding and connecting with friends who are nearby. The same consumer might not expect the application provider to retain a history of restaurants she visited over time. If the application provider were to share that information with third parties, it could reveal a predictive pattern of the consumer's movements thereby exposing the consumer to a risk of harm such as stalking.[8] Taken together, the principles of reasonable collection limitation and disposal periods help to minimize the risks that information collected from or about consumers could be used in harmful or unexpected ways.

With respect to the particular concerns of location data in the mobile context, the Commission calls on entities involved in the mobile ecosystem to work together to establish standards that address data collection, transfer, use, and disposal, particularly for location data. To the extent that location data in particular is collected and shared with third parties, entities should work to provide consumers with more prominent notice and choices about such practices. Although some in the mobile ecosystem provide notice about the collection of geolocation data, not all companies have adequately disclosed the frequency or extent of the collection, transfer, and use of such data.

NOTES

1 *See* Jennifer Valentino-Devries, *Study: iPhone Keeps Tracking Data*, Wall St. J., Apr. 21, 2011, *available at* http://online.wsj.com/article/SB10001424052748704570704576275323811369758.html.

2 *See, e.g.*, Robert Lee Hotz, *The Really Smart Phone*, Wall St. J., Apr. 22, 2011, *available at* http://online.wsj.com/article/SB10001424052748704547604576263261679848814.html (describing how researchers are using mobile data to predict consumers' actions); Scott Thurm & Yukari Iwatane Kane, *Your Apps are Watching You*, Wall St. J., Dec. 18, 2010, *available at* http://online.wsj.com/article/SB10001424052748704368004576027751867039730.html (documenting the data collection that occurs through many popular smartphone apps).

3 *Privacy Please! U.S. Smartphone App Users Concerned with Privacy When It Comes to Location*, NielsenWire Blog (Apr. 21, 2011), http://blog.nielsen.com/nielsenwire/online_mobile/privacy-please-u-s-smartphone-app-users-concerned-with-privacy-when-it-comes-to-location/; *see also* Ponemon Institute, *Smartphone Security: Survey of U.S. Consumers* 7 (Mar. 2011), *available at* http://aa-download.avg.com/filedir/other/Smartphone.pdf (reporting that 64% of consumers worry about their location being tracked when using their smartphones).

4 Similarly, the photo-sharing app Path faced widespread criticism for uploading its users' iPhone address books without their consent. *See, e.g.*, Mark Hachman, *Path Uploads Your Entire iPhone Contact List By Default*, PC Magazine, Feb. 7, 2012, *available at* http://www.pcmag.com/article2/0,2817,2399970,00.asp.

5 The Commission is currently reviewing its COPPA Rule, including the application of COPPA to geolocation information. *See* FTC, Proposed Rule and Request for Public Comment, Children's Online Privacy Protection Rule, 76 Fed. Reg. 59,804 (Sept. 15, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-09-27/pdf/2011-24314.pdf.

6 *See* ACLU of Northern California, *Location-Based Services: Time for a Privacy Check-In*, 14-15 (Nov. 2010), *available at* http://dotrights.org/sites/default/files/lbs-white-paper.pdf.

7 *Comment of Electronic Frontier Foundation*, cmt. #00400, at 3.

8 *Cf. U.S. v. Jones*, 565 U.S. 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) (noting that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations").