United States Government Accountability Office

Statement for the Record to the Committee on Commerce, Science, and Transportation, U.S. Senate

For Release on Delivery
Expected at 2:30 p.m. EST
Wednesday, December 18, 2013

INFORMATION RESELLERS

Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace

Statement for the Record of Alicia Puente Cackley, Director Financial Markets and Community Investment

December 18, 2013

INFORMATION RESELLERS

Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace

Highlights of GAO-14-251T, a statement for the record to the Committee on Commerce, Science, and Transportation, U.S. Senate

Why GAO Did This Study

Members of Congress and others have raised privacy concerns about information resellers (data brokers) and consumer information. In part, their concerns stem from consumers not always knowing the nature and extent of the information collected and how it is used. Growing use of the Internet, social media, and mobile applications has intensified privacy concerns because these media greatly facilitate gathering of personal information, tracking of online behavior, and monitoring of individuals' locations and activities. This statement for the record discusses (1) existing federal laws and regulations on the privacy of consumer information held by information resellers, (2) any gaps that may exist in this legal framework, and (3) views on approaches for improving consumer data privacy.

This statement draws from a September 2013 report (GAO-13-663), which focuses on information used for marketing. GAO analyzed relevant laws and regulations; interviewed representatives of federal agencies, trade associations, consumer and privacy groups, and resellers; and identified and reviewed approaches for improving consumer data privacy.

What GAO Recommends

In September 2013, GAO suggested that Congress should consider strengthening the consumer privacy framework and review issues such as the adequacy of consumers' ability to access, correct, and control their personal information; and privacy controls related to new technologies such as web tracking and mobile devices.

View GAO-14-251T. For more information, contact Alicia Puente Cackley at (202) 512-8678 or cackleya@gao.gov.

What GAO Found

No overarching federal privacy law governs the collection and sale of personal information among private-sector companies, including information resellers. Instead, laws tailored to specific purposes, situations, or entities govern the use, sharing, and protection of personal information. For example, the Fair Credit Reporting Act limits the use and distribution of personal information collected or used to help determine eligibility for such things as credit or employment, but does not apply to information used for marketing. Other laws apply specifically to health care providers, financial institutions, or to the online collection of information about children.

The current statutory framework for consumer privacy does not fully address new technologies—such as tracking of online behavior or mobile devices—and the vastly increased marketplace for personal information, including the proliferation of information sharing among third parties. No federal statute provides consumers the right to learn what information is held about them for marketing and who holds it. In many circumstances, consumers also do not have the legal right to control the collection or sharing with third parties of sensitive personal information (such as health information) for marketing purposes. As a result, although some industry participants have stated that current privacy laws are adequate, GAO found that gaps exist in the current statutory framework for information privacy. The framework also does not fully reflect the Fair Information Practice Principles, widely accepted principles for protecting the privacy and security of personal information that have served as a basis for many privacy recommendations federal agencies have made.

Views differ on the approach that any new privacy legislation or regulation should take. Some privacy advocates have argued that a comprehensive privacy law would provide greater consistency and address gaps in law left by the current sector-specific approach. Others have stated that a comprehensive, one-size-fits-all approach would be burdensome and inflexible. Some privacy advocates also cited the need to provide consumers with greater ability to access, control the use of, and correct information about themselves, particularly for data being used for purposes different than those for which they originally were provided. Industry representatives have asserted that restrictions on the collection and use of personal data would impose compliance costs, inhibit innovation, and reduce consumer benefits. Nonetheless, the rapid increase in the amount and type of personal information that is collected and resold warrants reconsideration of how well the current privacy framework protects personal information. The challenge will be providing appropriate privacy protections without unduly inhibiting the benefits to consumers, commerce, and innovation that data sharing can accord.

Chairman Rockefeller, Ranking Member Thune, and Members of the Committee:

I am pleased to submit this statement on our recent work on privacy, personal information, and information resellers.[1] As you know, information resellers (also known as data brokers) offer several types of products to customers that include retailers, advertisers, individuals, nonprofit organizations, law enforcement, and government agencies. This statement is based on a report we issued this September in response to a request from this committee to review privacy issues related to the consumer data that information resellers collect, use, and sell. Others also have raised privacy concerns about resellers and consumer information. In part, their concerns stem from consumers not always knowing the nature and extent of the information collected and how it is used. Moreover, growing use of the Internet, social media, and mobile applications has intensified privacy concerns because these media greatly facilitate the gathering of personal information, tracking of online behavior, and monitoring of individuals' locations and activities.

Our September report examined (1) existing federal laws and regulations related to the privacy of consumer information held by information resellers, (2) any gaps that may exist in this legal framework, and (3) views on approaches for improving consumer data privacy. We focused on privacy issues related to information used for marketing and individual reference services (look-up or people-search); we did not focus on information used for other purposes such as determining credit or employment eligibility.[2]

For our September 2013 report, we reviewed and analyzed relevant laws, regulations, and enforcement actions. We interviewed representatives of federal agencies, trade associations, consumer and privacy groups, and resellers to obtain their views on data privacy laws related to resellers. We identified and reviewed approaches (legislative, regulatory, or self-

[1]GAO, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, GAO-13-663 (Washington, D.C.: Sept. 25, 2013).

[2]In a 2006 report, we examined financial institutions' use of information resellers, focusing on consumer information used for eligibility determinations, compliance with legal requirements, and fraud prevention. GAO, *Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data*, GAO-06-674 (Washington, D.C.: June 26, 2006).

regulatory) for improving consumer data privacy that federal entities—such as the White House, Federal Trade Commission (FTC), and Department of Commerce (Commerce)—or representatives of industry, consumer, and privacy groups advocated. We interviewed representatives of these entities and reviewed relevant studies, hearings, position papers, public comments, and other sources. More details about our scope and methodology can be found in our published report.

We conducted the performance audit on which this statement is based from August 2012 through September 2013, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Resellers maintain large, sophisticated databases with consumer information that can include credit histories, insurance claims, criminal records, employment histories, incomes, ethnicities, purchase histories, and interests. Resellers largely obtain their information from public records, publicly available information (such as directories and newspapers), and nonpublic information (such as from retail loyalty cards, warranty registrations, contests, and web browsing). Characterizing the precise size and nature of the reseller industry can be difficult because of limited publicly known information about the industry.

In 1972, a U.S. government advisory committee first proposed the Fair Information Practice Principles (FIPP) for protecting the privacy and security of personal information. While FIPPs are not legal requirements, they provide a framework for balancing privacy with other interests. The Organisation for Economic Co-operation and Development (OECD) developed a revised version of the FIPPs that has been widely adopted (see table 1).[3]

[3]Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data* (Paris, France: Sept. 23, 1980). OECD's 30 member countries include the United States. OECD has been considering whether to revise or update its privacy guidelines to account for changes in the role of personal data in the economy and society.

Table 1: Fair Information Practice Principles

Principle	Description
Collection limitation	The collection of personal information should be limited, obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.
Data quality	Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.
Purpose specification	The purposes for the collection of personal information should be disclosed before collection and upon any change to those purposes, and the use of the information should be limited to those purposes and compatible purposes.
Use limitation	Personal information should not be disclosed or otherwise used for purposes other than a specified purpose without consent of the individual or legal authority.
Security safeguards	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
Openness	The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.
Individual participation	Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.
Accountability	Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.

Source: OECD.

FIPPs served as the basis for the Privacy Act of 1974—which governs the collection, maintenance, use, and dissemination of personal information by federal agencies.[4] The principles also were the basis for many FTC and Commerce privacy recommendations and for a framework for consumer data privacy the White House issued in 2012.[5]

[4]Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a). The act generally prohibits (with a number of exceptions) the disclosure by federal entities of records about an individual without the individual's written consent and provides U.S. persons with a means to seek access to and amend their records.

[5]The framework includes a consumer privacy bill of rights and encourages Congress to provide FTC with enforcement authorities for the bill of rights. The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Washington, D.C.: Feb. 23, 2012).

Several Laws Apply in Specific Circumstances to Consumer Data That Resellers Hold

No comprehensive federal privacy law governs the collection, use, and sale of personal information by private-sector companies. More narrowly tailored laws govern the use, sharing, and protection of personal information—they apply for specific purposes, in certain situations, to certain sectors, or to certain types of entities. The primary laws include the following:

Fair Credit Reporting Act (FCRA).[6] FCRA protects the security and confidentiality of personal information collected or used to help make decisions about individuals' eligibility for credit, insurance, or employment.[7] It applies to "consumer reporting agencies" (such as credit bureaus) that provide "consumer reports."[8]

Gramm-Leach-Bliley Act (GLBA).[9] GLBA protects nonpublic personal information that individuals provide to "financial institutions" or that such institutions maintain.[10] GLBA sharing and disclosure restrictions apply to financial institutions or entities that receive nonpublic personal information from such institutions.[11] For example, a third party that receives nonpublic personal information from a financial institution to process consumers' account transactions may not use the information or resell it for marketing purposes.

Health Insurance Portability and Accountability Act (HIPAA).[12] HIPAA establishes a set of national standards to protect certain health

[6]Pub. L. No. 91-508, Tit. VI, 84 Stat. 1114, 1128 (1970) (codified as amended at 15 U.S.C. §§ 1681-1681x).

[7]See 15 U.S.C. § 1681.

[8]For the definition of "consumer reporting agency," see 15 U.S.C. § 1681a(f). For the definition of "consumer report," see 15 U.S.C. § 1681a(d).

[9]Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.).

[10]See 15 U.S.C. §§ 6801-6802. Subtitle A of Title V of the act contains the privacy provisions relating to the disclosure of nonpublic personal information. 15 U.S.C. §§ 6801-6809.

[11]15 U.S.C. § 6802. A "financial institution" is any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act (12 U.S.C. § 1843(k)). 15 U.S.C. § 6809(3)(a).

[12]Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

information. The HIPAA privacy rule governs the use and disclosure of an individual's health information for purposes including marketing.[13] With some exceptions, the rule requires an individual's written authorization before a covered entity—a health care provider that transmits health information electronically in connection with covered transactions, health care clearinghouse, or health plan—may use or disclose the information for marketing.[14] The act does not directly restrict the use, disclosure, or resale of protected health information by resellers or others not considered covered entities under the act.

Children's Online Privacy Protection Act (COPPA).[15] COPPA and its implementing regulations apply to the collection of information—such as name, e-mail, or location—that would allow someone to identify or contact a child under 13.[16] Covered website and online service operators must obtain verifiable parental consent before collecting such information. COPPA may not directly affect information resellers, but the covered entities are potential sources of information for resellers.

Electronic Communications Privacy Act (ECPA).[17] ECPA prohibits the interception and disclosure of electronic communications by third parties unless an exception applies (such as one party to the communication consenting to disclosure). For example, the act would prevent an Internet service provider from selling the content of its customers' e-mails to a reseller for marketing purposes, unless the customers had consented to disclosure. However, ECPA provides more limited protection for information considered to be "non-content," such as a customer's name and address.

[13]45 C.F.R. Parts 160, 164.

[14]For the definition of "marketing," including exceptions, see 45 C.F.R. § 164.501.

[15]Pub. L. No. 105-277, Div. C, Tit. XIII, 112 Stat. 2681-728 (1998) (codified at 15 U.S.C. §§ 6501-6506).

[16]FTC issued regulations implementing COPPA, 16 C.F.R. Part 312.

[17]Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

Federal Trade Commission Act (FTC Act), **Section 5**.[18] The FTC Act prohibits unfair or deceptive acts or practices in or affecting commerce. Although the act does not explicitly grant FTC the specific authority to protect privacy, it has been interpreted to apply to deceptions or violations of written privacy policies. For example, if a retailer's written privacy policy stated customers' personal information would not be shared with resellers and the retailer later sold information to such parties, FTC could bring an enforcement action against the retailer for unfair and deceptive practices.

As they relate to specific types of consumer services or records, other federal privacy laws also may apply to information resellers' practices and products. For instance, while not specifically a privacy law, the **Computer Fraud and Abuse Act (CFAA)** can restrict a third party from collecting personal information from a website when the collection would violate the site's terms of service.[19] The **Telecommunications Act** requires telecommunications carriers to protect the confidentiality of proprietary information of customers.[20]

Laws Have Limited Scope over Personal Data Used for Marketing

Privacy protections under federal law have been limited for consumer data used for marketing. The scope of protections is narrow in relation to individuals' ability to access, control, and correct their personal data; collection methods and sources and types of information collected; and new technologies.

[18]15 U.S.C. § 45. Section 5 of the FTC Act, as originally enacted, only related to "unfair methods of competition." The Wheeler-Lea Act, passed in 1938, expanded the Commission's jurisdiction to include "unfair or deceptive acts or practices." Wheeler-Lea Amendments of 1938, Pub. L. No. 75-447, 52 Stat. 111.

[19]Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified as amended at 18 U.S.C. § 1030). Courts have held that CFAA prohibits access to websites when that access exceeds the sites' terms of use or end-user license agreements. For example, see *Snap-On Bus. Solutions Inc. v. O'Neil & Assoc., Inc.*, 708 F.Supp. 2d 669 (N.D. Ohio 2010); *Southwest Airlines Co. v. Farechase, Inc.*, 318 F.Supp. 2d 435 (N.D. Tex. 2004); and *America Online, Inc. v. LCGM, Inc.*, 46 F.Supp. 2d 444 (E.D. Va. 1998).

[20]Pub. L. No. 104-104, 110 Stat. 56 (1996) (codified as amended in scattered sections of 15 and 47 U.S.C.).

Laws Provide Individuals Limited Ability to Access, Control, and Correct Their Personal Data

No federal statute that we examined generally requires resellers to allow individuals to review personal information (intended for marketing purposes), control its use, or correct it. The FIPPs (for collection limitation and openness) state that individuals should be able to know about and consent to the collection of their information, while the individual participation principle states they should have the right to access the information, request correction, and challenge the denial of those rights.

No federal statute provides consumers the right to learn what information is held about them and who holds it for marketing or look-up purposes. FCRA provides individuals with certain access rights, but only when information is used for credit eligibility purposes. And GLBA's provisions allowing consumers to opt out of having their personal information shared with third parties apply only in specific circumstances. Otherwise, individuals cannot require that their personal information not be collected, used, and shared. Also, no federal law provides correction rights (the ability to have resellers and others correct or delete inaccurate, incomplete, or unverifiable information).

Laws Largely Do Not Address Data Collection Methods, Sources, and Types

Federal privacy laws are limited in addressing the methods by which, or the sources from which, resellers collect and aggregate personal information, or the types of information collected for marketing or look-up purposes. FIPPs (for data quality, purpose specification, and collection limitation) state that personal information should be relevant, limited to the purpose for which it was collected, and collected with the individual's knowledge or consent.

Federal laws generally do not govern the methods resellers may use to collect personal information. An example of such a method is "web scraping," in which resellers, advertisers, and others use software to search the web for information about individuals and extract and download bulk information from websites with consumer information. Resellers or retailers also may collect information indirectly (by combining information from transactions).

Current law generally allows resellers to collect personal information from sources including warranty registration cards, surveys, and online sources such as discussion boards, social media sites, blogs, and web browsing histories and searches. Current law does not require disclosure to consumers when their information is collected from these sources.

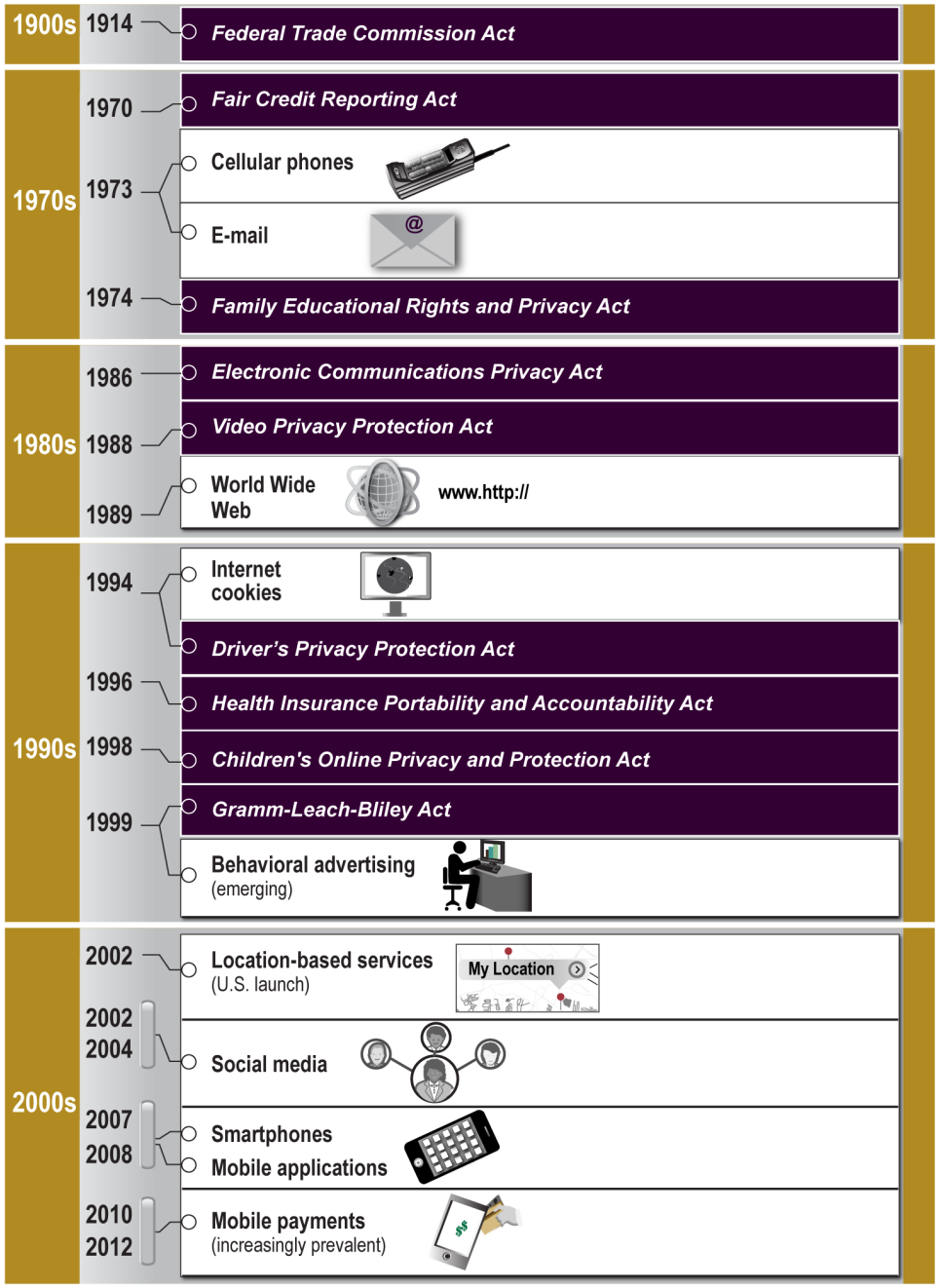
The federal laws that address the types of consumer information that can be collected and shared are not comprehensive. Under most circumstances, information that many people may consider very personal or sensitive can be collected, shared, and used for marketing. This can include information about physical and mental health, income and assets, political affiliations, and sexual habits and orientation. For health information, HIPAA provisions apply only to covered entities.

Current Law Does Not Directly Address Some Privacy Issues New Technology Raises

The current privacy framework does not fully address new technologies such as social media, web tracking, and mobile devices. In a 2013 report, FTC noted that mobile technologies present unique privacy challenges (for instance, mobile devices identify a user's geographical location).[21] As shown in figure 1, the original enactment of several federal privacy laws predates these trends and technologies.

[21]Federal Trade Commission, *Mobile Privacy Disclosures: Building Trust through Transparency* (Washington, D.C.: February 2013).

Figure 1: Dates of Enactment of Key Federal Privacy Laws and the Introduction of New Technologies



Source: GAO.

Note: The most recent amendments to the federal laws referenced in figure 1 are as follows:

- Federal Trade Commission Act of 1914: last amended July 21, 2010 (Pub. L. 111-203).
- Fair Credit Reporting Act of 1970: last amended Dec. 18, 2010 (Pub. L. No. 111-319).
- Family Educational Rights and Privacy Act of 1974: last amended Jan. 14, 2013 (Pub. L. No. 112-278).
- Electronic Communications Privacy Act of 1986: last amended Oct. 19, 2009 (Pub. L. No. 111-79).
- Video Privacy Protection Act of 1988: last amended Jan. 10, 2013 (Pub. L. No. 112-258).
- Driver's Privacy Protection Act of 1994: last amended Oct. 23, 2000 (Pub. L. No. 106-346).
- Health Insurance Portability and Accountability Act of 1996: last amended Mar. 23, 2010 (Pub. L. No. 111-148).
- Children's Online Privacy Protection Act of 1998: has not been amended.
- Gramm-Leach-Bliley Act of 1999: last amended July 21, 2010 (Pub. L. No. 111-203).

Because these laws were enacted to protect the privacy of information involving specific sectors rather than to address specific technologies, some have been interpreted to apply to new technologies. For example, FTC has taken enforcement actions under COPPA and revised the statute's implementing regulations to account for smartphones and mobile applications.

Online Tracking

No federal privacy law explicitly addresses the full range of practices to track or collect data from consumers' online activity. Cookies—text files placed on a computer by the website that the computer user visits—allow website operators to recall information such as user name and address, credit card number, and purchases in a shopping cart. Resellers can match information in cookies and their databases to augment consumer profiles. Third parties also can synchronize their cookie files with resellers' files. Advertisers can use third-party cookies—placed on a computer by a domain other than the site being visited—to track visits to the websites on which they advertise. Consumers' ability to prevent such tracking can be restricted. For example, so-called flash cookies do not expire at the end of a browsing session and cannot be erased.[22]

While current law does not explicitly address web tracking, FTC has taken enforcement actions related to web tracking under its authority to enforce the prohibition on unfair or deceptive acts. For example, in 2011, FTC settled charges with Google for $22.5 million after alleging that Google

[22]Shannon Canty, Chris Jay Hoofnagle, et al., "Flash Cookies and Privacy" (Aug. 10, 2009), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862.

violated an earlier privacy settlement with FTC when it misrepresented to users of Apple's Safari web browser that it would not track and serve targeted advertisements to Safari users.[23] Google agreed to disable its advertising tracking cookies.

Federal law also does not expressly prohibit "history sniffing," which uses code on a webpage to record visitors' browsing history. However, in 2012, FTC took an enforcement action against Epic Marketplace, a large online advertising network, for deceptively failing to disclose its use of history-sniffing technology.[24] Epic Marketplace used the data it collected to target advertising.

Mobile Technologies

In relation to collection and use of consumer data for marketing, no federal privacy laws that we identified specifically govern mobile applications and technologies.

Mobile applications. No federal law specifically governs mobile applications—software downloaded onto mobile devices for uses such as providing information and online banking and shopping.[25] Application developers, mobile carriers, advertisers, and others may collect an individual's information through services provided on a mobile device. However, FTC has taken enforcement action against companies for use of mobile applications that violate COPPA and FCRA.[26] The agency also

[23]*United States v. Google Inc.*, No. CV 12-04177-SI, 2012 WL 5833994 (N.D. Cal. Nov. 16, 2012).

[24]FTC alleged that Epic Marketplace's use of history sniffing was deceptive because it collected data about sites outside of its network that consumers had visited, contrary to Epic's privacy policy, which represented that it would collect information only about consumers' visits to websites in its network. *In the Matter of Epic Marketplace, Inc., and Epic Media Group, LLC*, FTC File No. 112 3182, decision and order (Mar. 13, 2013).

[25]On July 25, 2013, Commerce released a draft of a voluntary code of conduct for mobile applications, including guidelines for notices to consumers about collection and sharing of information with third parties. See Department of Commerce, National Telecommunications and Information Administration, *Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices*, redline draft (July 25, 2013), available at http://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf.

[26]FTC settled charges that a social networking service deceived consumers when it collected information from children under 13 through its mobile application in violation of COPPA. *See United States v. Path, Inc.*, No. C13-0448 (N.D. Cal. Jan. 31, 2013). FTC also settled charges that a company compiled and sold criminal record reports through its mobile application and operated as a consumer reporting agency in violation of FCRA. See *In the Matter of Filiquarian Publishing, LLC*, FTC File No. 112 3195 (Apr. 30, 2013).

has taken action under the FTC Act.[27] And CFAA, which bans unauthorized access to computers, has been found to apply to mobile phones.[28]

Location tracking. No federal privacy laws, except COPPA, expressly address location data, location-based technology, and consumer privacy. We and others have reported that the capability of mobile devices to provide consumer's location engenders privacy risks, particularly if companies use or share location data without consumers' knowledge.[29] ECPA might not apply if location data were not deemed content and would not govern entities such as developers of location-based applications that are not covered by ECPA. But FTC could pursue enforcement action if a company's collection or use of the information violated COPPA.

Mobile payments. No federal privacy laws expressly address mobile payments (for example, by smartphone). An FTC report noted that although mobile payment can be an easy way for individuals to pay for goods and services, privacy concerns have arisen because of the number of companies in the mobile payment marketplace and the large amount of detailed personal and purchase information collected and consolidated.[30]

[27]For example, in addition to the alleged COPPA violation, Path allegedly deceived users by collecting personal information from their mobile address books without their knowledge and consent. See *United States v. Path, Inc.*, No. C13-0448 (N.D. Cal. Jan. 31, 2013).

[28]In 2011, the U.S. Court of Appeals for the Eighth Circuit held that a basic cellular telephone—used only to place calls and send text messages—was a computer for CFAA purposes. The judicial decision did not address more advanced devices such as smartphones in the CFAA context. See *U.S. v. Kramer*, 631 F.3d 900 (8th Cir. 2011).

[29]Risks included disclosure to third parties for unspecified uses, tracking of consumer behavior, and identity theft. See GAO, *Mobile Device Location ID: Additional Federal Actions Could Help Protect Consumer Privacy*, GAO-12-903 (Washington, D.C.: Sept. 11, 2012). A Federal Communications Commission report also noted privacy risks. See Federal Communications Commission, *Location-Based Services: An Overview of Opportunities and Other Considerations* (Washington, D.C.: May 2012).

[30]Federal Trade Commission, *Paper, Plastic or Mobile? An FTC Workshop on Mobile Payments* (Washington, D.C.: March 2013).

Stakeholders Diverge on Adequacy of Legal Framework and Need for Legislation

Stakeholder views diverge on whether significant gaps exist in the legal framework for privacy, whether more legislation is needed, or whether self-regulation can suffice. The marketing and information reseller industries generally have argued that the current framework of sector-specific laws and regulations has not left significant gaps in consumer privacy protections. Privacy advocates and others stated that the current privacy scheme leaves significant gaps. Industry and privacy advocates also disagreed on the need for more legislation or regulation and the efficacy of self-regulatory approaches to protect privacy. Industry representatives acknowledged the importance of consumer privacy protections, but argued that voluntary industry measures and self-regulation mitigated the need for additional legislation. Some privacy advocates and others argued that voluntary compliance or self-regulation was not sufficient to uniformly protect consumer privacy rights.

Views Differ on Approaches to Privacy Law and Consumer Interests

Debate also has focused on appropriate approaches for new privacy legislation or regulation. This debate can be framed around three sets of issues: a comprehensive versus sector-specific approach to privacy legislation; how to address consumers' interests in accessing, controlling, and correcting their data; and the potential impact of new regulation on consumers and commerce.

Comprehensive versus Sector-Specific Approaches

Ongoing debate centers on what kind of legislative approach—sectoral or comprehensive—would best effect enhanced consumer privacy protections. Industry stakeholders have argued a comprehensive privacy law would amount to a one-size-fits-all approach and could be overly burdensome. Stakeholders also said that the current sector-specific system was flexible and well-suited to addressing any gaps. In contrast, some consumer and privacy groups and academic experts cited advantages to comprehensive privacy legislation such as filling gaps in existing privacy protections and providing comprehensive and consistent protections. Privacy advocates and some business representatives also argued that comprehensive legislation would benefit businesses internationally and help reduce compliance costs.

While not recommending a comprehensive federal privacy statute as such, in 2010 Commerce's Internet Policy Task Force recommended the adoption of a baseline commercial data privacy framework built on an expanded FIPPs. The 2012 White House privacy framework called for enacting baseline legislation while preserving existing sector-specific laws. The Administration supported exempting companies from consumer

data privacy legislation to the extent their activities were subject to existing data privacy laws.

Views on How to Address Consumers' Interests in Use and Control of Their Data

Other debate on privacy protections has focused on the third-party market for and usage of consumer data, whether or how consumers can access and control such usage or correct data, and how or if limits should apply to web tracking.

Use of Consumer Data

Consumer and privacy advocates have noted that consumers often were not aware of, and had not always consented to, personal information being repurposed for marketing and other uses. Changes in the marketplace for consumer data include a vast increase in recent years in the number and types of companies that collect and share such data with third parties. The Administration noted that consumers have a right to expect that companies will collect, use, and disclose their information in ways consistent with the context in which the information was provided.[31] FTC articulated a "context of the interaction" standard for determining when a practice required consumer choice.[32]

Representatives of information resellers, marketers, and other industries that use consumer data have argued that repurposing generally is not inappropriate or harmful. One reseller argued that personal information on unrestricted websites—such as blogs—becomes publicly available and can be used by a third party, without legal or ethical limitations on its use.

Access and Correction

Stakeholders' views differed on the extent to which consumers should be able to access data held about them. FTC said that companies should provide reasonable access to consumer data they maintain, a position many privacy groups echoed. FTC called on information resellers that compile data for marketing purposes to explore creating a centralized website on which resellers would identify themselves, describe how they collect and use the data, and consumers' access rights and choices.

Debate also developed on consumers' right to correct information held about them. Some privacy advocates and members of Congress have

[31]The White House, *A Framework for Protecting Privacy* (2012).

[32]Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change,* pp. 38-39.

argued that consumers should have the right to correct inaccurate information. One advocate noted that data not covered by FCRA also can be used for fraud prevention and identity verification, and that inaccuracies in this context could harm a consumer. Another advocate noted that companies may base some individual product pricing on a consumer's profile, so inaccurate data could affect the price offered. But FTC and the Direct Marketing Association said that special measures were not needed to ensure the accuracy of data maintained and used for marketing.[33] The Administration expressed a similar view in its privacy framework. Some resellers also said that because they acquire information from many sources, giving consumers the opportunity to correct information would not be effective unless consumers also could have information corrected at the sources from which it had been drawn.

Web Tracking

Some of the most publicized debate on privacy and new technologies has centered on consumers' ability to control tracking of their web activity. Areas of disagreement include the effectiveness of voluntary initiatives that allow consumers to exert some control over tracking and the use of information collected during tracking. For example, the Digital Advertising Alliance developed an icon to let web page users know that their visit was being tracked and their actions used to infer their interests and target future advertising. Users can click on the icon to learn more about targeted advertising and control whether they receive such advertising and from which companies.[34] Some privacy advocates have pointed to limitations to this mechanism (for example, the opt-out option only applies to companies in the Digital Advertising Alliance).

Debate also has developed about the implementation of "do not track." Under this approach, consumers would be able to choose whether to allow the collection and use of data about their online searching and browsing. FTC supported the concept of a universal do-not-track

[33]Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, pp. 38-39; and letter from Direct Marketing Association to members of Congress on August 13, 2012, available at http://the-dma.org/news/August-13-2012-DMALetter.pdf.

[34]According to the Digital Advertising Alliance, in 2012 more than 5.2 million unique users accessed the resources at www.aboutads.info, and nearly 1 million exercised a choice using the site's opt-out mechanism.

mechanism in its 2010 and 2012 privacy reports.[35] On the self-regulatory side, some Internet browsers, including Mozilla Firefox, have introduced do-not-track features. The World Wide Web Consortium has been developing a universal web protocol for do not track.[36] But disagreements on different issues (such as scope and technological specifications) have delayed widespread adoption or standardization of do not track.[37]

Proposals in Congress and elsewhere would require FTC to promulgate regulations for a do-not-track mechanism.[38] Proponents of such proposals noted that the use of third-party cookies greatly increased in recent years—for example, the Wall Street Journal identified more than 3,000 tracking files the top 50 websites placed on a test computer.[39] Advocacy organizations argued that Internet users may not be fully aware of the extent of third-party tracking and that users should affirmatively consent to tracking. Some members of Congress raised concerns about flash cookies and whether the FTC Act's prohibition of unfair or deceptive acts or practices would cover them. Representatives of the advertising and other industries have cautioned against many of the proposals.

Views on Potential Impacts of New Regulation on Consumers and Commerce

Representatives of the marketing and reseller industries argued that regulatory restrictions on using consumer data could reduce the benefits consumers get. Advertising representatives noted that targeted marketing and advertising helps underwrite applications and services available free to consumers. Some resellers said that targeted (behavioral) advertising

[35]Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* (2012) and *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers;* preliminary staff report (Washington, D.C.: December 2010).

[36]In the World Wide Web Consortium, member organizations and the public work together to develop web protocols and standards. The consortium's Tracking Protection Working Group proposes recommendations and technologies to improve user privacy and control. See http://w3.org/2011/tracking-protection/.

[37]Senate Committee on Commerce, Science, and Transportation, *A Status Update on the Development of Voluntary Do-Not-Track Standards*, 113th Cong., 1st sess., April 24, 2013; see testimony of Justin Brookman, Director, Consumer Privacy, Center for Democracy and Technology.

[38]For example, see *Do-Not-Track Online Act of 2013*, S. 418, 113th Cong.

[39]Julia Angwin, "The Web's New Gold Mine: Your Secrets," *Wall Street Journal*, July 30, 2010.

gives consumers information relevant to their specific interests, needs, or preferences. However, some privacy advocates believe that consumer benefits have been overstated. Some advocates also raised concerns that the profiling and scoring techniques used to deliver specific advertisements to specific consumers might have discriminatory effects because they present information, sales, or opportunities only to consumers with certain characteristics.

Stakeholder views also diverged on the potential economic effects of strengthened privacy regulations. Industry representatives said that new restrictions on the use of consumer information could inhibit innovation and increase compliance costs for businesses. Privacy and consumer groups said that the industry's claims that increased privacy protections would be too burdensome and stifle innovation have not been accompanied by convincing evidence. And in public comments solicited by Commerce in 2010 on information privacy and innovation in the Internet economy, online businesses and advertisers noted the importance of respecting customers' privacy if they wanted to retain their business or encourage individuals to adopt new devices and services.[40]

Views vary on the economic effects of greater harmonization of U.S. and foreign privacy rules. Commerce's Internet Policy Task Force noted that a significant number of comments they received concerned difficulties and costs in complying with foreign data protection rules and regulations. For example, the European Union's 1995 Data Protection Directive states that personal information of European Union citizens may not be transmitted to nations not deemed to have "adequate" data protection laws.[41] The United States does not have an adequacy finding from the European Commission.[42]

[40]Department of Commerce, Notice of Inquiry, Information Privacy and Innovation in the Internet Economy (Privacy and Innovation NOI), 75 Fed. Reg. 21226, Apr. 23, 2010, available at http://ntia.doc.gov/frnotices/2010/FR_PrivacyNOI_04232010.pdf.

[41]European Union, *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 the Free Movement of Such Data* (Oct. 24, 1995).

[42]However, companies participating in the U.S.-EU Safe Harbor Framework are deemed to provide adequate data protections and may transfer personal data from the European Union. FTC has the authority to enforce the substantive privacy requirements of the U.S.-EU Safe Harbor Framework.

The task force recommended the U.S. government work toward mutual recognition of other commercial data privacy frameworks.[43] Many commenters also advocated for greater harmonization of privacy rules. In contrast, some industry observers warned against enacting a stricter privacy regime like the European Union's. A reseller representative said moving to a stricter regime would hinder commerce and innovation.

New technologies have enormously changed the amount of personal information private companies collect and how they use it. But our current privacy framework does not fully address these changes. Laws protecting privacy interests are tailored to specific sectors and uses. And, consumers have little control over how their information is collected, used, and shared with third parties for marketing purposes. As a result, current privacy law is not always aligned with the Fair Information Practice Principles, which Commerce and others have said should serve as the foundation for commercial data privacy. Thus, the privacy framework warrants reconsideration in relation to consumer interests, new technologies, and other issues. In our September report, we suggested that Congress consider strengthening it and review issues such as the adequacy of consumers' ability to access, correct, and control their personal information; and privacy controls related to new technologies. The challenge will be providing appropriate protections without unduly inhibiting the benefits to consumers, commerce, and innovation that data sharing can accord.

This concludes my statement for the record.

For further information on this statement, please contact Alicia Puente Cackley at 202-512-8678 or cackleya@gao.gov. Contact points for our offices of Congressional Relations and Public Affairs may be found on the last page of this statement. In addition to the contact above, Michelle Bowsky, Jason Bromberg, William R. Chatlos, Rachel DeMarcus, Kun-Fang Lee, Barbara Roesmann, and Rachel Siegel contributed to this statement.

[43]Department of Commerce, Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (Washington, D.C.: 2010).

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper.