Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
U.S. DEPARTMENT OF COMMERCE
Washington, D.C. 20230

In the Matter of	)	Docket No.
	)	
Information Privacy and Innovation in the Internet Economy	)	100402174-0175-01
	)	

COMMENTS OF THE
FEDERAL TRADE COMMISSION

Introduction

The Federal Trade Commission ("FTC" or "Commission") appreciates this opportunity to comment on the Department of Commerce's ("Department") Notice of Inquiry on Information Privacy and Innovation in the Internet Economy ("Notice"). Currently, the FTC is exploring many of the same issues raised in the Notice as part of a recently concluded series of public roundtables on privacy and 21st century technology and business practices. These roundtables are part of an ongoing effort by the Commission to re-examine approaches to privacy, particularly in light of recent technological developments. The FTC plans to publish its initial privacy proposals later this year for public comment. The information gathered at these roundtables bears directly on the Department's inquiry.

The FTC is an independent administrative agency charged with promoting consumer protection, competition, and the efficient functioning of the marketplace. The keystone of the FTC's law enforcement mission is Section 5 of the FTC Act, which encompasses a wide range of business practices, including practices relating to both consumer privacy and business competition. Section 5 authorizes the FTC to challenge "unfair methods of competition," including violations of the antitrust laws, and "unfair or deceptive acts or practices in or affecting commerce."[1]

The Commission uses its Section 5 authority to address companies' privacy practices relating to the collection, use, and security of consumers' personal information. In addition, under the Gramm-Leach-Bliley Act,[2] the Commission has implemented rules requiring financial privacy notices and the administrative, technical, and physical

---

1 15 U.S.C. § 45(a).

2 15 U.S.C. §§ 6801-09, 6821-27, Pub. L. No. 106-102, 113 Stat. 1338 (1999). For more information on the FTC's role in enforcing the Gramm-Leach-Bliley Act, see FTC, The Gramm-Leach-Bliley Act, http://www.ftc.gov/privacy/privacyinitiatives/glbact.html.

safeguarding of personal information. The Commission also protects consumer privacy under a variety of other statutes, including the Fair Credit Reporting Act,[3] the Children's Online Privacy Protection Act,[4] and the CAN-SPAM Act.[5] The Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2006 ("U.S. SAFE WEB Act") further enhances the Commission's ability to cooperate with foreign enforcement authorities in addressing cross-border privacy violations.[6]

I. Promoting Innovation and Information Privacy through Competition and Consumer Protection Policies

As the Department's Notice observes, there is an important and mutually reinforcing relationship between competition policies and consumer protection policies in the context of privacy protection. Together, they benefit consumers by fostering new products and services, lower prices, and increased consumer confidence while conducting activities online.

Competition pressures producers to innovate by offering consumers the most attractive array of choices with respect to price, quality, and other options. Competitive firms constantly search for superior profit opportunities as they seek to win the favor of customers, who effectively vote with their dollars for preferred products and services. The U.S. Supreme Court has recognized that the benefits of competition go beyond lower prices and also extend to other dimensions, including the development of new products and services that will benefit consumers. "The assumption that competition is the best method of allocating resources in a free market recognizes that *all elements of a bargain - quality, service, safety, and durability* - and not just the immediate cost, are favorably affected by the free opportunity to select among alternative offers."[7]

At the same time, consumer protections promote informed consumer decision-making and require sellers to honor promises made about their offerings. In other words,

---

[3] 15 U.S.C. § 1681 et seq. For more information on the FTC's role in enforcing the Fair Credit Reporting Act, see FTC, Fair Credit Reporting Act, http://www.ftc.gov/os/statutes/fcrajump.shtm.

[4] 15 U.S.C. §§ 6501-6506, Pub. L. No. 105-277, 112 Stat. 2681-728 (1998). For more information on the FTC's role in enforcing the Children's Online Privacy Protection Act, see FTC, The Children's Online Privacy Protection Act, http://www.ftc.gov/privacy/privacyinitiatives/childrens.html.

[5] 15 U.S.C. §§ 7701-7713, Pub. L. No. 108-187, 117 Stat. 2699 (2003). For more information on the FTC's role in enforcing the CAN-SPAM Act, see FTC, Spam, Rules & Act, http://www.ftc.gov/bcp/edu/microsites/spam/rules.htm.

[6] Pub. L. No. 109-455, 120 Stat. 3372 (2006) (codified in scattered sections of 15 U.S.C. and 12 U.S.C. § 3412(e)). For more information on the FTC's role in enforcing the U.S. SAFE WEB Act, see FTC, THE U.S. SAFE WEB ACT: THE FIRST THREE YEARS, A REPORT TO CONGRESS (2009), *available at* http://www.ftc.gov/os/2009/12/P035303safewebact2009.pdf.

[7] *Nat'l Soc'y of Prof'l Eng'rs v. United States*, 435 U.S. 679, 695 (1978) (emphasis added); *accord, FTC v. Superior Court Trial Lawyers Ass'n*, 493 U.S. 411, 423 (1990).

strong consumer protection policies enable and clarify consumer choices by prohibiting firms from engaging in unfair or deceptive acts or practices and, thus, reinforce competition on the merits.

As the Department's Notice explains, the mutually beneficial relationship between innovation, which is driven by competition, and consumer protection policies applies forcefully to the dynamic Internet context. This relationship between competition and consumer protection policies is critical to facilitating the development and consumer use of the content and applications enabled by the Internet's infrastructure. Indeed, privacy practices may be an important factor that influences consumers' choices among competing products and services. In turn, competitive pressures can push companies to tailor their privacy practices more closely to what consumers desire in order to attract and retain them as customers. The Commission recognizes that inadequate protection of personal information and data security in the Internet context could hamper consumer confidence and undermine the Internet's benefits. For these reasons, the Commission often reviews acts and practices in the Internet area from both a competition and consumer protection perspective including, for example, how consumer protection considerations may affect the competitive analysis of various practices.

II. FTC Activities Relating to Online Privacy and Security

The FTC has made online privacy one of its highest consumer protection priorities for more than a decade. As technology has evolved, the FTC's goals have remained constant: to protect consumers' personal information and to ensure that consumers have the confidence to take advantage of the many benefits offered by the ever-changing online environment.[8] The Commission has sought to achieve these goals through law enforcement, consumer and business education, and policy initiatives.

First, enforcement remains the bedrock of the Commission's privacy program. For example, since 2001 the FTC has brought almost 30 cases challenging business practices that allegedly failed to adequately protect consumers' personal information.[9] These cases emphasize the importance of protecting consumers' data against common security threats and the need for businesses to evaluate their security procedures on an ongoing basis. Most recently, for instance, the entertainment company Dave & Buster's agreed to settle FTC charges that it left consumers' payment card information vulnerable to hackers. The Commission alleged that the company, among other things, failed to use appropriate firewalls or to limit access to its computer networks through wireless access points, resulting in breaches that led to several hundred thousand dollars in fraudulent charges.[10] In another recent enforcement action, the FTC settled charges against Sears

---

[8] *See generally* FTC, Privacy Initiatives, http://www.ftc.gov/privacy/index.html.

[9] *See id.*

[10] *See generally* Press Release, FTC, Dave & Buster's Settles FTC Charges it Failed to Protect Consumers' Information (Mar. 25, 2010), *available at* http://www.ftc.gov/opa/2010/03/davebusters.shtm.

alleging that company failed to disclose adequately the scope of personal information it collected from consumers via a downloadable software application. The settlement calls for Sears to stop collecting data from the consumers who downloaded the software, to destroy all data it had previously collected, and not to engage in similar conduct in the future.[11]

Second, the Commission actively seeks to educate consumers and businesses about privacy and security issues.[12] For example, it sponsors the site OnGuardOnline.gov, which provides practical tips from the federal government and the technology industry to help consumers guard against Internet fraud and protect the security of their computers and personal information. As an example of business education, the Commission recently released a guide for businesses on how to address the security risks associated with peer-to-peer ("P2P") file-sharing software.[13]

Third, the Commission is actively engaged in policy initiatives to improve consumer privacy. For example, the FTC staff has promoted self-regulation in the context of behavioral advertising, the practice of tracking consumers' online activities for the purpose of serving them with targeted advertisements. Behavioral advertising offers potential benefits for consumers in the form of free or subsidized online content and more relevant advertising. However, it also raises important privacy concerns, including the invisibility of the practice to consumers, the potential for companies to develop and store detailed profiles about consumers, and the risk that the data collected for behavioral advertising – including sensitive data regarding health, finance, or children – could fall into the wrong hands or be used for unanticipated purposes.

In the fall of 2007, the Commission held a town hall meeting to explore the privacy implications of online behavioral advertising. Following this meeting, staff issued a set of proposed self-regulatory principles for public comment and, after receiving over 60 comments, issued a final report on the subject in February 2009. The FTC's behavioral advertising principles emphasize the importance of transparency and consumer choice. In response to the FTC's efforts, some industry organizations have developed new self-regulatory principles for online behavioral advertising. A number of companies also have instituted new policies and procedures to inform consumers about online tracking and provide consumers with additional protections and controls over these practices. Such developments include new tools to allow consumers to opt out of receiving targeted online advertisements. The Commission will continue to encourage self-regulation and monitor progress in this area.

---

[11] *Sears Holdings Mgmt. Corp.*, FTC File No. 082-3099 (final order Aug. 31, 2009).

[12] *See generally* FTC, ID Theft, Privacy, & Security, http://www.ftc.gov/bcp/menus/consumer/data.shtm.

[13] FTC, Peer-to-Peer File Sharing: A Guide for Business, http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus46.shtm.

Most recently, the FTC has hosted a series of day-long roundtables to review consumer privacy issues more broadly. The purpose of the roundtables was to explore how best to protect consumer privacy while supporting beneficial uses of consumer data and technological innovation.[14] The roundtable record is discussed in more detail below.

III. The U.S. Privacy Framework Going Forward

The Department's Notice raises a series of questions regarding the current status of the U.S. privacy framework and whether there are modifications that would better support innovation, fundamental privacy principles, and evolving consumer expectations. The issues raised in the Department's Notice are very similar to the ones that Commission staff has been examining as part of its roundtables, in which the Department participated. In its Notice, the Department specifically cites these roundtables as an example of the reassessment of approaches to privacy that are currently taking place both domestically and globally, given the ongoing changes in the information economy.

The Commission began the roundtable discussions because of concerns that existing approaches to consumer privacy have practical limitations. For example, the current privacy framework in the United States is based on companies' issuance of long, complicated privacy notices that purport to explain the companies' privacy practices and consumers' choices regarding how their information is used. In reality, we have learned that many consumers do not read, let alone understand, such notices, limiting their ability to make informed choices. In addition, the emergence of new business models, such as social networking, raise new challenges in ensuring that privacy practices are transparent to consumers and consistent with their reasonable expectations. One of the key goals of the roundtables has been to explore how best to ensure consumer privacy in this changing environment.

The Commission gathered a wealth of information from academics, industry representatives, government officials, and consumer groups who attended the roundtables. Discussions focused in detail on the collection and use of data in several specific contexts, including behavioral advertising, information brokering, social networking, cloud computing, and the use of mobile devices.

Participants debated the parameters of what constitutes "sensitive" consumer information and whether such a concept, in fact, can be defined objectively or whether it is purely a subjective construct. They also explored possible ways to reconcile the privacy interests of individuals with other societal goals, such as improving public health through the aggregation of health-related information. Further, discussions at the roundtables focused on various models for managing the privacy and security of consumer information, including: fair information principles, sector-specific regulation,

---

[14] More information about the Privacy Roundtables can be found at FTC, Exploring Privacy, A Roundtable Series, http://www.ftc.gov/bcp/workshops/privacyroundtables/.

self-regulation, and approaches that would enable individuals to apply their privacy preferences themselves.

Several important themes emerged from these roundtable discussions. First, experts confirmed that consumers generally do not understand data collection practices and are largely unaware that there may be companies collecting and analyzing their data for use by other companies. Second, participants noted that consumers should have greater control over their privacy without undue burdens, such as having to spend considerable time reviewing dense privacy disclosures. Third, it may be reasonable and useful to distinguish between data practices that raise genuine privacy concerns and those that do not. Fourth, protecting consumers' privacy should not stifle marketplace innovations that consumers genuinely desire. Fifth, an improved privacy framework should be both flexible enough to accommodate diverse business models and also simple enough to provide clear norms and expectations. The Commission will take into account all of the comments it received through the roundtable process as it develops initial recommendations on privacy later this year.

In addition to these roundtable discussions, the Commission also is embarking on a review of the Children's Online Privacy Protection Rule. The current rule was enacted in 2000 and, among other things, requires web site operators to obtain parental consent before collecting, using, or disclosing personal information from children under the age of thirteen. In light of rapidly changing technologies, such as the increased use of smartphones and other mobile Internet access devices, the FTC hosted a public workshop on June 2, 2010 to explore whether to update the rule.[15]

IV. International Privacy

As the Notice observes, Internet commerce and related technologies, such as cloud computing, are increasingly global in nature. Thus, the FTC's policy work is not limited to domestic activities. The FTC actively participates in international policy initiatives relating to privacy and cross-border data flows through various international networks and organizations, including the Organization for Economic Cooperation and Development ("OECD") and the Asia-Pacific Economic Cooperation ("APEC") forum.

The FTC supports continued dialogue with its foreign counterparts and with international organizations on how to protect privacy and security across borders without restricting beneficial information flows. For example, in 2009, the Commission staff hosted a two-day international conference in conjunction with the OECD and APEC to

---

[15] More information about this review can be found at FTC, FTC Seeks Comment on Children's Online Privacy Protections; Questions Whether Changes to Technology Warrant Changes to Agency Rule, http://www.ftc.gov/opa/2010/03/coppa.shtm.

address how companies can manage data security in a global environment where data can be stored and accessed from multiple jurisdictions.[16]

The Commission also understands that, in a global economy, companies find it increasingly challenging to comply with varying privacy requirements around the world, particularly those relating to the cross-border transfer of personal consumer information. Likewise, the cross-border enforcement of privacy laws and regulations continues to raise novel questions for consumer protection authorities. The Commission recognizes that, as the need for cross-border data flow increases, facilitating companies' compliance with applicable laws as well as protecting consumers' data in the event of a failure to do so will require international cooperation.

In December 2006, Congress recognized the increasing threats facing U.S. consumers in the global marketplace from the proliferation of spam, spyware, telemarketing, and other cross-border consumer law violations, and passed the U.S. SAFE WEB Act. The Act enhances the FTC's ability to protect consumers by giving the agency new or expanded powers in several key areas.[17] The FTC has used the Act's authority to quickly and effectively protect consumers in the global economy. The Act has helped the FTC to overcome obstacles to cross-border enforcement it faced in the past and is critical to the FTC's ability to address problems that consumers may face in the future.[18] The FTC, therefore, has recommended that Congress preserve this much-needed authority and repeal the 7-year sunset provision contained in the Act.[19]

In addition, the FTC is actively involved in cross-border privacy enforcement initiatives. In November 2009, APEC approved a privacy enforcement cooperation arrangement for privacy enforcement authorities in the APEC region.[20] The FTC is actively participating in implementing this arrangement. Most recently, the FTC, along with ten other privacy enforcement authorities around the world, started a privacy enforcement cooperation network called the Global Privacy Enforcement Network

---

16 More information about this workshop can be found at FTC, Securing Personal Data in the Global Economy, http://www.ftc.gov/bcp/workshops/personaldataglobal/index.shtm.

17 The Act authorizes the FTC, in appropriate consumer protection matters, to share compelled and confidential information and provide investigative assistance to foreign law enforcement agencies addressing conduct substantially similar to conduct that would violate U.S. law. 15 U.S.C. §§ 46(f), (j), 57b-2(b)(6). It also gives the FTC a variety of other tools to improve international enforcement cooperation, which the FTC has used in a substantial number of consumer protection cases.

18 *See generally* FTC, *supra* note 6.

19 *Id.* at 19-21.

20 *See* APEC, APEC Cooperation Arrangement for Cross-Border Privacy Enforcement, *available at* http://aimp.apec.org/Documents/2010/ECSG/DPS1/10_ecsg_dps1_013.pdf.

("GPEN"). The FTC also has brought several cases enforcing the U.S.-European Union "Safe Harbor" arrangement for data transfers.[21]

Conclusion

The Federal Trade Commission is pleased to provide these comments on information privacy and innovation in the Internet economy in light of our years of experience protecting consumer privacy both online and offline. The FTC will continue to devote substantial resources to protecting consumers using the Commission's law enforcement, consumer education, and policy development tools. The Commission would be pleased to assist the Department of Commerce in any way that would be useful toward the completion of its inquiry and report on information privacy and innovation in the Internet economy.

By Direction of the Commission.

Donald S. Clark
Secretary

[21] *See generally* Press Release, FTC, FTC Settles with Six Companies Claiming to Comply with International Privacy Framework (Oct. 6, 2009), *available at* http://www.ftc.gov/opa/2009/10/safeharbor.shtm.