Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Cyber Security Certification Program	)	PS Docket No. 10-93

COMMENTS OF THE
FEDERAL TRADE COMMISSION

Introduction

The Federal Trade Commission ("FTC") appreciates this opportunity to comment on the Federal Communications Commission's ("FCC") Notice of Inquiry on a voluntary cyber security certification program for communications service providers.[1] The FCC's Notice of Inquiry seeks comment on whether it should establish a voluntary program under which communications service providers would be certified for their adherence to a set of cyber security objectives and/or practices. The FTC provides the following comments to highlight lessons learned from our law enforcement, consumer and business education, and policy activities relating to data security.

The FTC uses a flexible approach to data security to analyze whether companies' practices are reasonable and appropriate in light of the risks and vulnerabilities they face. For over a decade, the FTC has brought law enforcement actions against a variety of commercial entities, such as retailers, data brokers, and social networking web sites, which have failed to implement reasonable and appropriate security measures to protect consumer data. In these cases we have required companies to establish, implement, and maintain a data security program that is subject to independent audit.

Because communications service providers hold and handle similar sensitive consumer information and face similar security risks as those entities we have examined and investigated for their data security practices, we recommend that the FCC use a flexible approach if it decides to move forward with a certification program. A program's objectives and practices should allow for flexibility so that security practices are reasonable and appropriate in light of the risks and vulnerabilities facing communications service providers. In addition, a certification program should be able to adjust to evolving security threats. Finally, a program should include a strong enforcement mechanism so that consumers can rely on the certification in choosing among communications service providers.

The FTC is an independent agency charged with promoting consumer protection and competition in the marketplace. Section 5 of the FTC Act authorizes the FTC to

---

[1] 75 Fed. Reg. 26171 (May 11, 2010).

challenge unfair or deceptive business practices, including those that relate to data security.[2] A variety of other statutes also empower the FTC to protect consumer data. The FTC enforces the Gramm-Leach-Bliley Act ("GLB Act"),[3] the Fair Credit Reporting Act ("FCRA"),[4] the Children's Online Privacy Protection Act ("COPPA"),[5] and the Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM Act").[6] The Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act ("U.S. SAFE WEB Act")[7] further enhances the FTC's ability to cooperate with foreign enforcement authorities, including those addressing cross-border privacy violations.

Section I of these comments summarizes the FTC's strong commitment to protecting data security and privacy. Section II provides the FTC's observations as they relate to the FCC's proposed voluntary cyber security certification program.

I. The FTC's Strong Commitment to Protecting Consumer Data

To promote data security through law enforcement, the FTC brings enforcement actions against businesses that fail to implement reasonable and appropriate security measures to protect consumer data.[8] The keystone of our law enforcement mission is Section 5 of the FTC Act, which authorizes the FTC to challenge "unfair or deceptive

---

[2] 15 U.S.C. § 45(a). Regarding the scope of the FTC's consumer unfairness jurisdiction, see 15 U.S.C. § 45(n); Letter from FTC to Hon. Wendell H. Ford and Hon. John C. Danforth (Dec. 17, 1980), appended to *Int'l Harvester Co.*, 104 FTC 949, 1070 (1984), available at http://www.ftc.gov/bcp/policystmt/ad-unfair.htm. Regarding the scope of the FTC's consumer deception jurisdiction, see Letter from FTC to Hon. John D. Dingell (Oct. 14, 1983), appended to *Cliffdale Assocs., Inc.*, 103 FTC 110, 174 (1984), available at http://www.ftc.gov/bcp/policystmt/ad-decept.htm.

[3] 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 GLB Act, see FTC, The Gramm-Leach-Bliley Act, http://www.ftc.gov/privacy/privacyinitiatives/glbact.html.

[4] 15 U.S.C. §§ 1681 et seq. For more information on the FTC's role in enforcing the FCRA, see

acts or p

On the policy front, the FTC recently hosted a series of day-long roundtable workshops 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 the information and technological innovation.[17] FTC staff expect to publish their initial privacy proposals later this year for public comment.[18]

The FTC is actively involved in several cross-border privacy enforcement initiatives. For example, the FTC, along with foreign counterparts, led the effort to develop the Asia Pacific Economic Cooperation's "Cross-border Privacy Enforcement Arrangement." This arrangement establishes a framework for regional cooperation in the enforcement of privacy laws. The FTC also worked alongside its foreign privacy enforcement counterparts to launch a network designed to facilitate privacy enforcement cooperation. This network, the Global Privacy Enforcement Network ("GPEN"), was formed in March of 2010.

The FTC has significant tools that enable it to cooperate with its international counterparts. In enacting the U.S. SAFE WEB Act in December 2006, Congress recognized the increasing threats to U.S. consumers from the proliferation of spam, spyware, telemarketing, and other cross-border threats. This statute gives the agency new or expanded powers in several key areas, including enhanced cooperation with foreign law enforcement agencies.[19] The FTC has used its enhanced authority to quickly and effectively protect consumers in the global economy.[20]

II. Observations Relating to the FCC's Proposed Voluntary Cyber Security Certification Program

The FCC's Notice of Inquiry seeks comment on whether it should establish a voluntary program under which communications service providers would be certified for their adherence to a set of cyber security objectives and/or practices. The Notice of Inquiry seeks comment on four possible security objectives that it proposes as the starting

---

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

point of the security regime: (1) secure equipment management; (2) updating software; (3) intrusion prevention and detection; and (4) intrusion analysis and response.[21]

If the FCC decides to move forward, we recommend that: (1) the program's objectives and practices should allow for flexibility; (2) the program should be able to adjust to evolving security threats; and (3) the program should include a strong enforcement mechanism. The next three sections describe these recommendations.

A. A Cyber Security Certification Program's Objectives and Practices Should Allow for Flexibility So That Security Practices Are Reasonable and Appropriate in Light of the Risks and Vulnerabilities

The FTC recommends that a certification program's objectives and practices should allow for flexibility. A flexible approach would allow communications service providers to implement security practices that are reasonable and appropriate in light of the risks and vulnerabilities they face and also would take into account the costs associated with implementation of these practices. Such an approach would allow a program's objectives and practices address a broad range of security threats that might arise in a variety of different contexts.

What is reasonable and appropriate is a question that encompasses the totality of the circumstances in which a company operates. Based on our law enforcement experience regarding data security, the FTC has recognized there is no "one size fits all" security plan. Increased levels of information sensitivity require increased protection. Different technologies may present different risks and vulnerabilities. Different types of businesses, business methods, and customers may require companies to address security in regard to different aspects of their operations. The costs associated with implementation of security practices are also relevant to a reasonableness and appropriateness inquiry. Particular security measures that may be reasonable for the data of one company in light of all the costs and benefits may or may not be reasonable for another company. Becad leve

the customer information they maintain in order to reasonably achieve the rule's objectives.[23]

The FTC's data security law enforcement cases further illustrate this flexible approach to defining the contours of reasonable and appropriate security objectives and practices. Under resulting settlement orders, the FTC has required companies to establish, implement, and maintain a comprehensive security program reasonably and appropriately designed to protect the security, confidentiality, and integrity of personal

failed to employ sufficient measures to detect and prevent unauthorized access to its networks or to conduct security investigations.

Similarly, appropriate security practices could extend to protecting against well-known tools frequently used by hackers. For instance, in our case against social networking site Twitter, Inc. the FTC alleged that hackers were able to obtain unauthorized administrative control of the site by using an automated tool to determine an employee's administrative password. The FTC charged that Twitter put consumers' privacy at risk by failing to take reasonable steps to prevent unauthori

professional every other year for 20 years.[33] Last year, however, the FTC obtained a stipulated modified order against ChoicePoint after charging that the company failed to implement the comprehensive information security program that was required by the earlier court order.[34] This failure left the door open to a data breach in 2008 that compromised the personal information of 13,750 people and put them at risk of identify theft. The modified order expands the company's data security assessment and reporting duties.

A number of other FTC cases further illustrate why companies should proactively guard against risks and vulnerabilities. For example, our cases against BJ's Warehouse,[35] DSW Shoe Warehouse,[36] and CardSystems Solutions[37] make clear that businesses should not retain sensitive consumer data they no longer need. Doing so is unreasonable because such information is unnecessarily put at risk. In each of these cases, the complaint alleged that the company unnecessarily stored unencrypted, full magnetic stripe information of payment cards long after the time of the transaction when there was no longer any business need for that data. As a result, when thieves gained access to the companies' systems, they were able to obtain hundreds of thousands or, in some cases, millions of credit card numbers and security codes.

C. A Cyber Security Certification Program Requires a Strong Enforcement Mechanism

A cyber security certification program also requires a strong enforcement mechanism to maintain its integrity and effectiveness.[38]

adhere to its objectives and practices. Thus, a program must have the resources necessary to conduct regular reviews of participating companies, evaluate complaints of non-compliance, and take remedial action where necessary.[39]

Recent FTC cases demonstrate that flawed privacy and security certification schemes can be deceptive. Such schemes can mislead consumers who reasonably conclude from a company's display of a program's seal that a third party has positively evaluated that company's privacy or security practices. Companies that falsely state they adhere to certain security standards can potentially expose consumers to significant harm if, in fact, consumers receive a lesser degree of protection.

The FTC has brought such enforcement actions against a variety of companies purporting to operate or adhere to online privacy and data security certification programs. For example, the FTC earlier this year settled charges against ControlScan, a third party company on which consumers relied to certify the privacy and security of online retailers and certain other web sites.[40] ControlScan offered a variety of privacy and security seals for display on web sites it certified. Consumers could click on the seals to discover exactly what assurances each seal conveyed. The FTC alleged that ControlScan deceived consumers about how often it actually monitored the sites it certified and the steps it took to verify the sites' privacy and security practices. The settlement bars such misrepresentations and requires the company to take down its seals.

Within the last year the FTC also settled charges that six companies misled consumers by falsely claiming they participated in the U.S./E.U. Safe Harbor program when, in fact, their self-certifications had lapsed.[41] The U.S./E.U. Safe Harbor program is administered by the U.S. Department of Commerce in consultation with the European Commission and enables the transfer of personal information about individuals from the European Union to participating U.S. companies. To participate, a company must self-certify annually to the Department of Commerce that it complies with a defined set of privacy requirements. Under the settlements, the companies are prohibited from misrepresenting the extent to which they participate in any privacy, security, or other compliance program sponsored by a government or third party.

Conclusion

If the FCC decides to move forward with a voluntary cyber security certification program, we recommend that the program's objectives and practices allow for flexibility so that security practices are reasonable and appropriate in light of the risks and vulnerabilities facing communications service providers. The FTC has used a flexible

---

[39] Compare supra note 25 (discussing the use of independent, third-party auditors to monitor compliance with settlement orders in FTC data security law enforcement actions).

[40] See Press Release, FTC, Online Privacy and Security Certification Service Settles FTC Charges (Feb. 25, 2010), available at http://www.ftc.gov/opa/2010/02/controlscan.shtm.

[41] See 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.

approach to data security for a over a decade to require a variety of different types of companies to establish, implement, and maintain reasonable and appropriate practices to safeguard consumer information based on the totality of the circumstances they face. In addition, a certification program should be able to adjust to evolving security threats. Finally, a program should include a strong enforcement mechanism so that consumers can rely on the certification in choosing among communications service providers. Because communications service providers hold and handle similar sensitive consumer information and face similar security risks as those entities we have examined and investigated for their data security practices, we recommend that any program should incorporate these fundamental principles.

By Direction of the Commission.

Donald S. Clark