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 FTC, Fair Credit Reporting Act, http://www.ftc.gov/os/statutes/fcrajump.shtm.

[5] 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 COPPA, see FTC, The Children's Online Privacy Protection Act, http://www.ftc.gov/privacy/privacyinitiatives/childrens.html.

[6] 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 & Acts, http://www.ftc.gov/bcp/edu/microsites/spam/rules.htm.

[7] 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.

[8] *See generally* Prepared Statement of the FTC on Consumer Privacy Before the Senate Committee on Commerce, Science, and Transportation (July 27, 2010), *available at* http://www.ftc.gov/os/testimony/100727consumerprivacy.pdf.

acts or practices in or affecting commerce."[9] The FTC uses this authority, for example, in cases where a business makes false or misleading claims about its data security procedures or where its failure to employ reasonable and appropriate security measures causes or is likely to cause substantial consumer injury. The FTC's Safeguards Rule issued under the GLB Act also contains data security requirements for financial institutions within the FTC's jurisdiction.[10] In addition, the FCRA requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information and imposes safe disposal obligations on entities that maintain consumer report information.[11]

The FTC has brought dozens of actions charging that companies failed to take reasonable and appropriate measures to secure sensitive consumer information, such as financial and health information.[12] The FTC approaches data security by analyzing what is reasonable and appropriate based on the totality of the circumstances, including the sensitivity of the information, the nature and scope of the company holding the information, and the security risks and vulnerabilities a company faces.[13] The FTC's actions have focused on preventing and stopping the variety of methods through which unauthorized access occurs. These cases also emphasize the importance of protecting consumers against common security threats and the need for businesses to evaluate their security procedures on an ongoing basis.

The FTC actively seeks to educate consumers and businesses about privacy and security issues.[14] For example, our main information security website provides businesses with guidance on how to protect personal information.[15] The FTC 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 their computers and personal information. We also released a guide for businesses on how to address the security risks associated with peer-to-peer ("P2P") file sharing software.[16]

---

[9] 15 U.S.C. § 45(a).

[10] FTC, Standards for Safeguarding Customer Information; Final Rule, 16 C.F.R. Part 314 (May 23, 2002) ("Safeguards Rule"), *available at* http://www.ftc.gov/os/2002/05/67fr36585.pdf.

[11] 15 U.S.C. §§ 1681e and 1681w. The FTC's implementing rule is at 16 C.F.R. Part 682.

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

[13] *See infra* Section II A (discussing this point in more detail).

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

[15] FTC, Protecting Personal Information, A Guide for Business, http://www.ftc.gov/infosecurity/.

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

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/.

[18] More information on the U.S. privacy framework going forward can be found at FTC, Comments Before the National Telecommunications and Information Administration, U.S. Department of Commerce In re Information Privacy and Innovation in the Internet Economy 5-6 (June 2010), *available at* http://ftc.gov/os/2010/06/100623ntiacomments.pdf.

[19] 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 agency has used in a number of consumer protection cases.

[20] *See generally* FTC, *supra* note 7.

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. Because companies may grow over time, security measures should be scalable to accommodate potential changes in the security threats they might face as a consequence of expansion.

The FTC has taken this flexible approach in developing the Safeguards Rule under the GLB Act.[22] The rule requires covered institutions to protect customer information according to a set of general objectives and specified actions. Importantly, the Safeguards Rule allows companies to select specific safeguards that are appropriate to their size and complexity, the nature and scope of their activities, and the sensitivity of

---

[21] 75 Fed. Reg. 26171, 26174.

[22] Safeguards Rule, *supra* note 10.

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 information that they collect from or about consumers, similar to programs required under the Safeguards Rule.[24] Companies are required to have independent, third-party audits of their security procedures to ensure compliance.[25]

The FTC's case against TJX illustrates how a company failed to provide reasonable and appropriate security measures to counteract basic security threats that should have been well-known to such a retailer.[26] As a result of the failure to guard against threats to its computer networks, an intruder obtained information relating to tens of millions of credit and debit payment cards that consumers used at TJX stores. Banks claimed that tens of millions of dollars in fraudulent charges were made as a result and millions of payment cards had to be cancelled and reissued. The FTC's complaint alleged that TJX unreasonably transmitted in clear text sensitive consumer payment information; did not use readily available security measures to limit wireless access to its networks; did not require network administrators and others to use strong passwords or to use different passwords to access different programs, computers, and networks; and

---

[23] The Safeguards Rule's objectives are to ensure the security and confidentiality of customer information; protect against any anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer. Covered financial institutions must take specified steps to develop, implement, and maintain a program. They must designate one or more employees to coordinate the safeguards program; identify and assess the risks to customer information in each relevant area of a company's operation (including employee management and training, information systems, and management of system failures); design and implement information safeguards and regularly test them; oversee related service providers; and evaluate and adjust the program in light of relevant circumstances, including changed circumstances. *Id*.

[24] *See id*.

[25] Auditors must document the specific administrative, technical, and physical safeguards that the company has implemented and maintained; explain how these safeguards are appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of personal information collected from or about consumers; explain how the safeguards address the specific security deficiencies; and certify that the program is operating effectively. For an example of this type of settlement order, see, e.g., *In re The TJX Cos.*, FTC Docket No. C-4227 (July 29, 2008) (consent order), *available at* http://www.ftc.gov/os/caselist/0723055/080801tjxdo.pdf.

[26] *See* Press Release, FTC, Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data (Mar. 27, 2008), *available at* http://www.ftc.gov/opa/2008/03/datasec.shtm; *see also* 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.

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 unauthorized administrative control of its system, including access to non-public user information, access to messages that consumers had designated private, and the ability to send out phony messages from any user account.[27] The FTC alleged that Twitter failed to make administrative passwords hard to guess; enforce their periodic change; prohibit plain text storage of them in personal email accounts; suspend or disable such passwords after a reasonable number of unsuccessful login attempts; provide a separate administrative login webpage made known only to authorized persons; restrict administrative access based on an employee's job; and implement other reasonable restrictions.

Further, appropriate security practices could encompass the training and oversight of employees, as highlighted by the FTC's action against pharmaceutical manufacturer Eli Lilly.[28] This case involved a situation where an employee of Eli Lilly addressed an e-mail (using the "To" line) to all users of its Prozac depression medication who subscribed to a service on Lilly's website, essentially disclosing the identities of all Prozac user-subscribers. The FTC alleged that the company unreasonably failed to provide appropriate training for its employees regarding consumer privacy and information security; provide appropriate training and oversight for the employee who sent the e-mail; and implement appropriate checks on employees who use sensitive customer data.

Data security is not limited solely to the collection, storage, and transfer of data online. It also extends to cases where data is translated into hard copy form. This point is illustrated by the FTC's recent settlements with pharmacies Rite Aid and CVS over charges they failed to protect the sensitive financial and medical information of their customers and employees when they used dumpsters to discard trash containing such information.[29] The FTC's complaints in these cases alleged that each company failed to use reasonable procedures in regard to disposing of personal information; assessing

---

[27] *See* Press Release, FTC, Twitter Settles Charges that it Failed to Protect Consumers' Personal Information; Company Will Establish Independently Audited Information Security Program (June 24, 2010), *available at* http://www.ftc.gov/opa/2010/06/twitter.shtm.

[28] *See* Press Release, FTC, Eli Lilly Settles FTC Charges Concerning Security Breach (Jan. 18, 2002), *available* at http://www.ftc.gov/opa/2002/01/elililly.shtm.

[29] *See* Press Release, FTC, Rite Aid Settles FTC Charges That It Failed to Protect Medical and Financial Privacy of Customers and Employees (July 27, 2010), *available at* http://www.ftc.gov/opa/2010/07/riteaid.shtm; Press Release, FTC, CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays $2.25 Million to Settle Allegations of HIPAA Violations (Feb. 18, 2009), *available at* http://www.ftc.gov/opa/2009/02/cvs.shtm.

compliance with its disposal policies and procedures; and employing a reasonable process for discovering and remedying risks to personal information.

B. A Cyber Security Certification Program Should Be Able to Adjust to Evolving Security Threats

A cyber security certification program should be able to adjust to evolving security threats.[30] Technologies and business realities change over time. New technologies likely will have new vulnerabilities waiting to be discovered. Hackers and thieves will attempt to adapt to whatever measures are in place. New ways of doing business can potentially raise novel security issues as well. Therefore, a certification program should not allow itself to become outdated. Rather, a program should regularly assess its effectiveness and make necessary adjustments in response to evolving security threats. A program's specific objectives and practices also should be forward-looking and capable of being applied dynamically to confront ever-changing risks and vulnerabilities.[31] Further, we recommend that the FCC should be able to modify, supplement, or remove particular objectives or practices as warranted by changes in technology and associated risks and vulnerabilities

As part of addressing security risks and vulnerabilities on an ongoing basis, a program should similarly require that the companies it certifies proactively assess and respond to the risks and vulnerabilities they face. A program should not allow participating companies to simply wait for a data security breach to occur before taking action. Rather, a program should require them to take appropriate steps to guard against risks and vulnerabilities that can be reasonably anticipated.

The FTC's actions against data broker ChoicePoint, for example, highlight this point. There, the FTC alleged that the company lacked reasonable security procedures to verify the legitimacy of its customers, with the result that it sold 160,000 consumer files to identity thieves posing as clients.[32] The FTC's settlement with ChoicePoint required it to implement new procedures to ensure that it provides consumer reports only to legitimate businesses for lawful purposes, to establish and maintain a comprehensive information security program, and to obtain audits by an independent third-party security

---

[30] *Compare supra* notes 17-18 and related text (discussing the FTC's ongoing review of our consumer privacy framework).

[31] Accordingly, we recommend that any program be technology-neutral. Selecting one particular technological approach, including technologies that might be developed in the future, may inadvertently cause program participants to become "locked in" to a particular security approach that could become outdated. Rather, a program should seek to achieve its goals while allowing for continued experimentation and technological advancement.

[32] *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198 (N.D. Ga. Feb. 15, 2006).

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] If consumers are to rely on a certification in choosing among communications service providers, it is important that a program is backed up with meaningful consequences for companies that falsely claim to

---

[33] *See* Press Release, FTC, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan. 26, 2006), *available at* http://www.ftc.gov/opa/2006/01/choicepoint.shtm.

[34] *See* Press Release, FTC, Consumer Data Broker ChoicePoint Failed to Protect Consumers' Personal Data, Left Key Electronic Monitoring Tool Turned Off for Four Months (Oct. 19, 2009), *available at* http://www.ftc.gov/opa/2009/10/choicepoint.shtm.

[35] *See* Press Release, FTC, BJ's Wholesale Club Settles FTC Charges (June 16, 2005), *available at* http://www.ftc.gov/opa/2005/06/bjswholesale.shtm.

[36] *See* Press Release, FTC, DSW Inc. Settles FTC Charges (Dec. 1, 2005), *available at* http://www.ftc.gov/opa/2005/12/dsw.shtm.

[37] *See* Press Release, FTC, FTC/DOJ Issue Annual HSR Premerger Notification Report to Congress; Commission Approves Final Consent Order in Matter of CardSystems Solutions (Sept. 2006), *available at* http://www.ftc.gov/opa/2006/09/fyi0658.shtm.

[38] The FTC's law enforcement actions in this area require companies that settle unfairness and deception charges against them to establish, implement, and maintain a comprehensive security program that is regularly audited for a specified period of time by an independent third-party. *See supra* notes 24-25 and related text.

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