Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of

Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans)))))))) Docket No. 14 -126

To: The Federal Communications Commission

Comment of the Federal Trade Commission

In its inquiry into the status of broadband availability and deployment to all Americans, the Federal Communications Commission has asked for comment regarding the relevance of privacy and/or data security concerns to consumer adoption of broadband.[1] Among other issues, the FCC asked whether broadband providers must comply with their own voluntary statements about privacy and security and whether any other potential obligations exist for providers.[2] As reflected in our enforcement, research, and policy work on consumer privacy issues, the FTC believes that promoting consumer trust in digital technology is of critical importance to

---

[1] Federal Communications Commission, *Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act*, GN Docket No. 14-126, Tenth Broadband Progress Notice of Inquiry, 29 FCC Rcd 9747 (rel. Aug. 5, 2014)("NOI").

regarding privacy and/or security which broadband providers may be subject? If so, what are these, and what relevance, if any, would they have to our [section 706(b)] determination [as to whether advanced telecommunications capability is being deployed to all Americans in a reasonable and timely fashion]?").

consumers and businesses alike. The FTC therefore appreciates the oppor

broadband provider that fails to reasonably protect the privacy or security of consumer data in a way that causes a likelihood of substantial harm that is not reasonably avoidable by consumers and is without countervailing benefits to consumers or competition may violate the unfairness prohibition of Section 5.

Indeed, the FTC has used Section 5 to challenge dozens of companies' express and implied claims about what data they collect, whether they share it with third parties, what choices they offer to consumers, and the level of security they provide for consumers' personal data. To date, the FTC has brought over 50 cases alleging lax security practices, 20 of which charged that the business had engaged in unfair acts or practices. The FTC's privacy and security matters

malware installed on consumers' computers,[17] or by sending unwanted or deceptive "spam" emails[18] or text messages.[19]

B. Fair Credit Reporting Act

Another law that imposes privacy and security-related obligations on broadband providers is the FCRA. Although best known for regulating the activities of credit bureaus, the FCRA also applies to companies that provide information to credit bureaus ("furnishers") and companies that use credit reports ("users"). Broadband providers often are both furnishers and users under the FCRA.[20] As such, certain FCRA requirements apply. For example, if a broadband provider furnishes information to credit bureaus, the FCRA imposes obligations to make sure the information is accurate. If the provider uses credit reports, it must certify to the credit bureaus that it has a "permissible purpose" for obtaining the report, such as the fact that it will use the report to set credit or employment terms. A broadband provider that uses credit reports must also provide notices to its customers when it offers less favorable terms based on information in a credit report. These notices must explain how the consumer can dispute any inaccurate information in their credit report.

---

[17] *See, e.g., Aaron's, Inc.*, Docket No. C-4442 (Mar. 10, 2014) (final decision and order), *available at* http://www.ftc.gov/system/files/documents/cases/140311aaronsdo.pdf.

[18] *See, e.g., FTC v. Linda Jean Lightfoot d/b/a Universal Direct*, No. C-3-02-145 (S.D. Ohio Apr. 11, 2002) (stipulated preliminary injunction), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2002/04/lightfootstip.pdf.

[19] *See, e.g., FTC v. Advert Mktg., Inc.*, No. 4:13-cv-00590 (S.D. Tex. June 9, 2014) (Stipulated Final J.), *available at* http://www.ftc.gov/system/files/documents/cases/140612advertorder.pdf.

[20] The FCRA does not contain an exemption for common carrier services.

The FTC's recent enforcement action against Time Warner Cable illustrates this last requirement.[21] There, the FTC charged Time Warner Cable with obtaining prospective customers' credit reports before providing them with video, high-speed data, telephony, and

The FTC has brought a number of cases to enforce these requirements against mobile app developers,[22] social media companies,[23] and others. To date, the FTC has brought 23 COPPA cases and obtained more than $9,000,000 in civil penalties. To the extent that a broadband service provider were to knowingly collect personal information from children under 13, it would be subject to COPPA's privacy and security requirements.

II. <u>FTC Policy and Educational Efforts</u>

In addition to the laws discussed above, the FTC has engaged in a variety of policy and education initiatives to promote privacy and data security in all sectors of the economy. This work provides important guidance that broadband providers can look to as they incorporate privacy and security best practices into their products and services.

A. Policy Initiatives

On the policy front, the FTC has hosted public workshops, issued reports, and frequently testified before Congress on business practices and tech Tc -0.00tivII.fecting the privacy and security of consumer data. For example, the FTC testified before Congress on privacy and data security reTc (tat)-16(ed)-4(i)-6(s)-5(s)-5(u)-4(es)-3(5)8T(N.D. Cal. Sept. 8, 2011)-6(S)-22(gle)-10(ta)]TJ), 0 Tc 0 T
available at http://www.ftc.gov/sites/default/files/documents/cases/2011/09/110908w3order.pdf

____.

[23] *See Path, Inc., supra* note 16.

[24] *See* Prepared Statement of the Fed. Trade Comm'n, "*The Location Privacy Protection Act of 2014*," Before the Senate Committee on the Judiciary, 113th Cong., June 4, 2014, *available at* http://www.ftc.gov/system/files/documents/public_statements/313671/604locationprivacyact.pdf; Prepared Statement of the Fed. Trade Comm'n, "*Emerging Threats in the Online Advertising Industry*," Before the Senate Committee on Homeland Security and Governmental Affairs, 113th Cong., May 15, 2014, *available at* http://www.ftc.gov/system/files/documents/public_statements/309891/515emergingthreatsonline.pdf; Prepared Statement of the Fed. Trade Comm'n, "*Data Breach on the Rise: Protecting Personal Information from Harm*," Before the Senate Committee on Homeland Security and Governmental Affairs, 113th Cong., Apr. 2, 2014, *available at* http://www.ftc.gov/system/files/documents/public_statements/296011/140402datasecurity.pdf; Prepared Statement of the Fed. Trade Comm'n, "*Protecting Personal Consumer Information from Cyber Attacks and Data Breaches*," Before the Senate Committee on Commerce, Science, and Transportation, 113th

over the past decade to promote data security and privacy in the private sector through civil law enforcement, policy initiatives, and consumer and business education. In addition, the FTC testified about the privacy issues related to the

will be essential to robust competition in that market," in part because "inadequate protection of privacy of personal information and data security in the provision of broadband Internet access could hamper consumer confidence in the industry."[27] The report concluded that the FTC and the FCC "each play[ ] an important role" in protecting consumers.[28]

Two points are worth noting in this regard. First, through its recent policy initiatives, the FTC has emphasized the importance of privacy by design.[34] While disclosure, as noted in the FCC's NOI, is an important element of a comprehensive approach to privacy and security, it does not guarantee adequate protections. For example, consumers should not have to sift through and compare disclosures to determine which companies implement which practices for the data they collect. Companies should simply implement practices that are reasonable given the context of the data collection. This is part of a privacy by design process that the FTC has encouraged all companies to implement.

Second, the FTC has set forth some best practices related to deep packet inspection ("DPI") and similar technologies.[35] In its 2012 Privacy Report, the FTC discussed the position of ISPs as major gateways to the Internet and their ability to access vast amounts of unencrypted data and to develop comprehensive profiles of their customers.[36]

B. FTC Consumer Education and Business Guidance

The FTC is also committed to promoting better privacy and data security practices through consumer education and business guidance. On the consumer education front, the FTC has distributed millions of copies of educational materials for consumers and businesses to address ongoing threats to security and privacy. It also makes its guidance materials available online. For example, the FTC recently released an updated version of "Net Cetera: Chatting with Kids About Being Online," a guide to help parents and other adults talk to kids about being safe,

---

[34] *See, e.g., Protecting Consumer Privacy in an Era of Rapid Change*, *supra* note 30, at 22. (Commissioner Ohlhausen and Commissioner Wright were not members of the FTC at the time and thus did not participate in the vote on the report.)

[35] DPI refers to an internet service provider's ("ISP") ability to analyze the information, comprised of data packets, that traverses its network when consumers use its service.

[36] *Protecting Consumer Privacy in an Era of Rapid Change*, *supra* note 30, at 55-56.

secure, and responsible online.[37] This new version deals with such topics as mobile apps and privacy, public Wi-Fi security, text message spam, and the amendments to the FTC's COPPA Rule. As another example, the FTC sponsors OnGuard Online, a website designed to educate consumers about basic computer security.[38] OnGuard Online and its Spanish-language counterpart, Alerta en Línea,[39] average more than 2.2 million unique visits per year. The FTC's website also includes timely advice to consumers on how to handle security breaches, such as the recent Target breach.[40]

Further, the FTC has released guidance directed to businesses. For instance, the FTC widely disseminates its business guide on data security,[41] along with an online tutorial based on the guide.[42] These resources provide a variety of businesses with practical, concrete advice as they develop data security programs and plans for their companies. This guidance provides an important resource for broadband providers, which often collect and maintain sensitive information about their customers.

---

[37] *See* http://www.consumer.ftc.gov/articles/pdf-0001-netcetera.pdf.

[38] *See* http://www.onguardonline.gov.

[39] *See* http://www.alertaenlinea.gov.

[40] *See* FTC Consumer Blog,

III. Conclusion

In sum, companies that provide broadband services must adhere to the privacy and security obligations imposed by the FTC Act, the FCRA, and COPPA. The FTC has actively enforced these laws and will continue to do so, where appropriate, in the broadband service market. As the FCC explores the laws and standards applicable to broadband providers, including those that may apply pursuant to the Communications Act, the FTC encourages the FCC to consider the well-established legal standards and best practices.[43] The FTC welcomes the opportunity to share its experience promoting consumer privacy and data security with the FCC and looks forward to working with the FCC to