



United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, DC 20580

Federal Trade Commission

July 17, 2017

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

**RE: Restoring Internet Freedom, Notice of Proposed Rulemaking, WC Docket
No. 17-108, FCC 17-60, Comment of the Staff of the Federal Trade
Commission**

Dear Secretary Dortch:

As the Acting Directors of the Federal Trade Commission's Bureau of Consumer Protection, Bureau of Competition, and Bureau of Economics, we submit this comment to assist the Federal Communications Commission in evaluating the consumer privacy implications of its Notice of Proposed Rulemaking on Restoring Internet Freedom.

Sincerely,

Thomas B. Pahl
Acting Director
Bureau of Consumer Protection

Markus H. Meier
Acting Director
Bureau of Competition

Ginger Z. Jin
Director
Bureau of Economics

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of

Restoring Internet Freedom

)
)
)
)
)
)
)

WC Docket No. 17-108

To: The Federal Communications Commission

Date: July 17, 2017

Comment of the Staff of the Federal Trade Commission

I. INTRODUCTION

The staff of the Federal Trade Commission (“FTC”) submits this comment to the Federal Communications Commission (“FCC”) in support of the proposal to return jurisdiction over Broadband Internet Access Service (“BIAS”) to the FTC, as set forth in the FCC’s Notice of Proposed Rulemaking on Restoring Internet Freedom (“Restoring Internet Freedom NPRM” or “NPRM”).¹ In 2015, the FCC had reclassified broadband as a common carrier service through its “Title II Order.”² Prior to the Title II Order, the FTC consistently protected broadband consumers from unfair and deceptive practices, including in the privacy and data security area.³ When the FCC issued the Title II Order reclassifying broadband as a common carrier service, it

¹ Restoring Internet Freedom, WC Docket No. 17-108, FCC 17-60 (proposed May 23, 2017), *published in* 82 Fed. Reg. 25568 (June 2, 2017) (to be codified in 47 C.F.R. pts. 8 & 20).

² Protecting and Promoting the Open Internet, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd. 5601 (2015).

³ *See* 15 U.S.C. § 45(a)(1) (2012) (prohibiting unfair or deceptive acts or practices in or affecting commerce).

effectively stripped the FTC of its authority over BIAS services, because the FTC is prohibited from regulating common carrier activities.⁴

The NPRM proposes to reverse the classification of BIAS from a common carrier service to an information service, which would have the effect of returning BIAS providers to FTC jurisdiction. The NPRM specifically seeks comment on its proposal to have “the FTC oversee[] Internet service providers’ privacy practices. . . .”⁵ FTC staff supports this proposal. Furthermore, by returning BIAS providers to FTC jurisdiction, the proposal would also restore the FTC’s ability to protect broadband consumers under its general consumer protection and competition authority. Thus, the proposal would allow the FTC to take action against BIAS providers engaged in “unfair competition,” which would include, for example, entering into agreements that substantially reduce competition. It would also allow the FTC to take action against “unfair or deceptive acts or practices,” such as fraud, deceptive advertising, or unauthorized billing.

This comment first provides an overview of the FTC’s activities on privacy and data security. Second, it explains why FTC staff supports the return of jurisdiction over BIAS providers’ privacy and data security practices to the FTC. Third, it highlights the importance of

⁴ See 15 U.S.C. §§ 45(a)(2) (exempting “common carriers subject to the Acts to regulate commerce”), 44 (defining “Acts to regulate commerce” as including “the Communications Act of 1934 and all Acts amendatory thereof and supplementary thereto”). Currently, the issue of whether the common carrier exception is “activity based” or “status based” is before the Ninth Circuit. A panel of the Ninth Circuit has held that the common carrier exemption precludes FTC oversight of common carriers’ non-common carrier services. See *FTC v. AT&T Mobility LLC*, 835 F.3d 993 (9th Cir. 2016). The Ninth Circuit recently granted rehearing of that case *en banc* and vacated the panel opinion. See *FTC v. AT&T Mobility LLC*, No. 15-16585, 2017 WL 1856836 (9th Cir. May 9, 2017). The FCC supported the petition for rehearing. *Amicus Curiae* Br. of the Fed. Commc’ns Comm’n In Supp. of the Fed. Trade Comm’n’s Pet. For Reh’g *En Banc*, *FTC v. AT&T Mobility LLC*, No. 15-16585 (9th Cir. Oct. 24, 2016), 2017 WL 2398744; Letter Pursuant to Fed R. App. P 28(j) of *amicus* FCC, *FTC v. AT&T Mobility LLC*, No. 15-16585 (9th Cir. Apr. 21, 2017). Regardless of the full Court’s decision, the FCC’s current classification of broadband Internet access service as a common carrier service would remain a constraint on the FTC’s enforcement of Section 5 of the FTC Act against BIAS providers.

⁵ Restoring Internet Freedom, *supra* note 1, at ¶ 67.

restoring the FTC's broad consumer protection jurisdiction over BIAS providers' practices, including practices outside the privacy and data security area. Finally, it discusses the effect of restoring the FTC's competition jurisdiction over BIAS providers' practices.

II. THE FTC HAS EXTENSIVE PRIVACY AND DATA SECURITY EXPERTISE

The FTC has long been the leading privacy and data security agency in the United States. Although its strategies have evolved with changing technology and business models, the goal in this area has remained constant: to protect consumers' information, promote innovation, and ensure that consumers have the confidence to take advantage of the benefits offered in the marketplace. The FTC's approach to protecting the privacy and security of consumers' data relies on three basic tools: enforcement, policy initiatives, and education.

A. Enforcement

As part of its consumer protection mandate, the FTC enforces a wide range of laws to protect the privacy and security of consumer data. The primary law enforced by the FTC, the FTC Act, prohibits unfair and deceptive acts or practices in or affecting commerce.⁶ A misrepresentation or omission is deceptive if it is material and is likely to mislead consumers acting reasonably under the circumstances.⁷ An act or practice is unfair if it causes, or is likely to cause, substantial injury that is not reasonably avoidable by consumers, and not outweighed by countervailing benefits to consumers or competition.⁸

In addition to the FTC Act, Congress has repeatedly and explicitly, by statute, charged the FTC with protecting consumer privacy and data security in various sectors. Thus, the FTC

⁶ 15 U.S.C. § 45(a) (2012).

⁷ See Fed. Trade Comm'n, FTC Policy Statement on Deception (Oct. 14, 1983), *appended to Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984), <https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception>.

⁸ See Fed. Trade Comm'n, FTC Policy Statement on Unfairness (Dec. 17, 1980), *appended to Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984), <https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness>; 15 U.S.C. § 45(n) (2012).

enforces statutes that protect certain health,⁹ credit,¹⁰ financial,¹¹ and children's information.¹² Congress has also given the FTC authority to issue and enforce rules to protect privacy and data security, such as the Health Breach Notification Rule,¹³ the Gramm-Leach-Bliley Safeguards Rule,¹⁴ and the Disposal Rule.¹⁵

To date, the FTC has brought over 500 cases protecting the privacy and security of consumer information.¹⁶ These cases address a wide range of practices, including spam, unwanted telemarketing, behavioral advertising, pretexting, and spyware. Through these cases, the FTC has gained expertise into a variety of industries, including social media, ad-tech, search, mobile, and Internet of Things ("IoT").¹⁷

This body of FTC cases covers both offline and online information and includes enforcement actions against companies large and small. In a wide range of cases, the FTC has alleged that companies made deceptive claims about how they collect, use, and share consumer data;¹⁸ failed to provide reasonable security for consumer data;¹⁹ deceptively tracked consumers

⁹ Health Information Technology for Clinical and Economic Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009) (codified as amended at 42 U.S.C. §§ 300jj *et seq.*; §§17901 *et seq.* (2012)).

¹⁰ Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681x (2012).

¹¹ Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C. (2012)).

¹² Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (2012).

¹³ 16 C.F.R. Part 318 (2017).

¹⁴ 16 C.F.R. Part 314 (2017).

¹⁵ 16 C.F.R. Part 682 (2017).

¹⁶ Letter from Edith Ramirez, Chairwoman, Fed. Trade Comm'n, to Věra Jourová, Commissioner for Justice, Consumers, and Gender Equality, European Commission, at 3 (Feb. 23, 2016), <https://www.ftc.gov/public-statements/2016/02/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice>.

¹⁷ *See, e.g.*, FED. TRADE COMM'N, PRIVACY & SECURITY UPDATE: 2016 (2017), <https://www.ftc.gov/reports/privacy-data-security-update-2016>.

¹⁸ *See, e.g.*, *FTC v. VIZIO, Inc.*, No. 2:17-CV-00758 (D.N.J. Feb. 6, 2017), <https://www.ftc.gov/enforcement/cases-proceedings/162-3024/vizio-inc-vizio-inscape-services-llc>; *United States v. InMobi Pte. Ltd.*, No. 3:16-CV-03474 (N.D. Cal. June 22, 2016), <https://www.ftc.gov/enforcement/cases-proceedings/152-3203/inmobi-pte-ltd>; *Practice Fusion, Inc.*, No. C-4591 (F.T.C. Aug. 15, 2016), <https://www.ftc.gov/enforcement/cases-proceedings/142-3039/practice-fusion-inc-matter>; *Snapchat, Inc.*, No. C-4501 (F.T.C. Dec. 23, 2014), <https://www.ftc.gov/enforcement/cases-proceedings/132-3078/snapchat-inc-matter>.

online;²⁰ spammed and defrauded consumers;²¹ installed spyware or other malware on consumers' computers;²² violated Do Not Call and other telemarketing rules;²³ shared highly sensitive, private consumer data with unauthorized third parties;²⁴ and publicly posted such data online without consumers' knowledge or consent.²⁵ The FTC's frequent and ongoing enforcement actions send an important message to companies about the need to protect consumers' privacy and data security in both the physical and digital worlds.

Finally, the FTC has actively enforced the US-EU Safe Harbor Framework, which is the predecessor to the EU-US Privacy Shield Framework. These frameworks have provided a mechanism that allows U.S. companies to lawfully transfer the data of European consumers to the United States, without having to specifically comply with EU regulations.²⁶ Companies that

¹⁹ See, e.g., *FTC v. ruby Corp.*, No. 1:16-CV-02438 (D.D.C. Dec. 14, 2016), <https://www.ftc.gov/enforcement/cases-proceedings/152-3284/ashley-madison>; *ASUSTeK Computer, Inc.*, No. C-4587 (F.T.C. July 18, 2016), <https://www.ftc.gov/enforcement/cases-proceedings/142-3156/asustek-computer-inc-matter>. See generally *Data Security*, FED. TRADE COMM'N, <https://www.ftc.gov/datasecurity>.

²⁰ See, e.g., *Turn Inc.*, No. C-4612 (F.T.C. Apr. 6, 2017), <https://www.ftc.gov/enforcement/cases-proceedings/152-3099/turn-inc-matter>; *Compete, Inc.*, No. C-4384 (F.T.C. Feb. 20, 2013), <https://www.ftc.gov/enforcement/cases-proceedings/102-3155/compete-inc>; *Upromise, Inc.*, No. C-4351 (F.T.C. Mar. 27, 2012), <https://www.ftc.gov/enforcement/cases-proceedings/102-3116/upromise-inc>; *Sears Holdings Mgmt. Corp.*, No. C-4264 (F.T.C. Aug. 31, 2009), <https://www.ftc.gov/enforcement/cases-proceedings/082-3099/sears-holdings-management-corporation-corporation-matter>.

²¹ See, e.g., *FTC v. Tachht, Inc.*, No. 8:16-CV-01397 (M.D. Fla. Mar. 3, 2017), <https://www.ftc.gov/enforcement/cases-proceedings/152-3080/john-fowler>; *FTC v. INC21.com Corp.*, 688 F. Supp. 2d 927 (N.D. Cal. 2010).

²² See, e.g., *FTC v. CyberSpy Software, LLC*, No. 6:08-cv-1872-ORL-31GJK (M.D. Fla. Apr. 22, 2010), <http://www.ftc.gov/enforcement/cases-proceedings/082-3160/cyberspy-software-llc-trace-r-spence>; *FTC v. Enternet Media, Inc.*, No. CV 05-777 CAS (C.D. Cal. Aug. 22, 2006), <http://www.ftc.gov/enforcement/cases-proceedings/052-3135-x06-0003/enternet-media-inc-conspy-co-inc-et-al>.

²³ See, e.g., *FTC v. Life Mgmt. Servs., Inc.*, No. 6:16-cv-982-Orl-41TBS (M.D. Fla. June 8, 2016), <https://www.ftc.gov/enforcement/cases-proceedings/152-3216/life-management>; *United States v. Lilly Mgmt. & Mktg., LLC*, No. 6:16-CV-435-0-137DAB (M.D. Fla. Mar. 16, 2016), <https://www.ftc.gov/enforcement/cases-proceedings/152-3115/usa-vacation-station>; *United States v. KFJ Mktg., LLC*, No. 2:16-cv-01643 (C.D. Cal. Mar. 10, 2016), <https://www.ftc.gov/enforcement/cases-proceedings/152-3166/kfj-marketing-llc>.

²⁴ See, e.g., *FTC v. Sitesearch Corp.*, No. CV-14-02750-PHX-NVW (D. Az. Feb. 5, 2016), <https://www.ftc.gov/enforcement/cases-proceedings/142-3192-x150060/sitesearch-corporation-doing-business-leaplab>; *FTC v. Accusearch Inc.*, 570 F.3d 1187 (10th Cir. 2009) (*en banc*).

²⁵ See, e.g., *Jerk, LLC*, No. 9361 (F.T.C. Mar. 13, 2015), <https://www.ftc.gov/enforcement/cases-proceedings/122-3141/jerk-llc-dba-jerkcom-matter>; *Craig Brittain*, No. C-4564 (F.T.C. Dec. 28, 2015), <https://www.ftc.gov/enforcement/cases-proceedings/132-3120/craig-brittain-matter>.

²⁶ See generally *PRIVACY SHIELD FRAMEWORK*, <https://www.privacyshield.gov> (last visited July 13, 2017).

self-certify their adherence to seven privacy principles will be deemed to have “adequate” privacy protection under EU law. The FTC enforces these self-certifications: If a company does not comply with the privacy principles, it could be engaged in a deceptive practice under the FTC Act. To date, the FTC has brought approximately forty enforcement actions against companies that violated the US-EU Safe Harbor Framework and has committed to enforce the EU-US Privacy Shield Framework with the same vigor.

Through enforcement actions, the FTC stops law violations, prevents future violations, and requires companies to take affirmative steps to remediate the unlawful behavior. This includes, when appropriate, orders requiring the implementation of comprehensive privacy and security programs, biennial assessments by independent experts, equitable monetary relief for consumers, deletion of illegally obtained consumer information, and robust transparency and choice mechanisms for consumers. FTC orders also commonly include “fencing in” remedies designed to prevent future unlawful conduct by including “provisions . . . that are broader in scope than the conduct that is declared unlawful.”²⁷ If a company violates an FTC order, the FTC can seek civil monetary penalties for the violations. The FTC can also obtain civil monetary penalties for violations of certain privacy and data security statutes and rules, including the Children’s Online Privacy Protection Act (“COPPA”)²⁸ and the Fair Credit Reporting Act (“FCRA”).²⁹

²⁷ *Telebrands Corp. v. FTC*, 457 F.3d 354, 357 n.5 (4th Cir. 2006); *see also FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 394-95 (1965); *FTC v. Ruberoid Co.*, 343 U.S. 470, 473 (1952); *Kraft, Inc. v. FTC*, 970 F.2d 311, 326-27 (7th Cir. 1992).

²⁸ 15 U.S.C. §§ 6501-6506 (2012).

²⁹ 15 U.S.C. §§ 1681–1681x (2012).

B. Policy Initiatives

The FTC has engaged in a variety of policy initiatives to promote privacy and data security in all sectors of the economy. Since 1996, the FTC has hosted over thirty-five workshops, town halls, and roundtables bringing together stakeholders to discuss emerging issues in consumer privacy and security. Most recently, the FTC hosted workshops on identity theft³⁰ and connected cars.³¹ The FTC also hosts an annual PrivacyCon event aimed at examining cutting-edge research and trends in protecting consumer privacy and security. The FTC recently announced that its next PrivacyCon event will take place on February 28, 2018.³²

The FTC and its staff have also issued numerous reports on privacy and data security issues. These include a report setting forth a general privacy framework for business,³³ a report on facial recognition technology,³⁴ a report on mobile privacy disclosures,³⁵ an Internet of Things report,³⁶ a report on the data broker industry,³⁷ and a report on the practice of cross-

³⁰ *Identity Theft: Planning for the Future*, FED. TRADE COMM’N (May 24, 2017), <https://www.ftc.gov/news-events/events-calendar/2017/05/planning-future-conference-about-identity-theft>.

³¹ *Connected Cars: Privacy, Security Issues Related to Connected, Automated Vehicles*, FED. TRADE COMM’N (June 28, 2017), <https://www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected>.

³² *PrivacyCon 2018*, FED. TRADE COMM’N, <https://www.ftc.gov/news-events/events-calendar/2018/02/privacycon-2018>.

³³ FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), <https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers> [hereinafter “2012 PRIVACY REPORT”] (Commission Report).

³⁴ FED. TRADE COMM’N, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES (2012), <https://www.ftc.gov/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies> (Staff Report).

³⁵ FED. TRADE COMM’N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY (2013), <https://www.ftc.gov/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission> [hereinafter “MOBILE PRIVACY DISCLOSURES”] (Staff Report).

³⁶ FED. TRADE COMM’N, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD (2015), <https://www.ftc.gov/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things> (Staff Report).

³⁷ FED. TRADE COMM’N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014), <https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014> (Commission Report).

device tracking.³⁸ These reports have highlighted best practices for protecting privacy and security.

The FTC also frequently provides its privacy and data security expertise to other government agencies and to Congress. For example, earlier this year, the FTC testified before the House Committee on Small Business on the issue of coordinating federal government resources to help small businesses with cybersecurity issues.³⁹ In addition, the staff has provided comments to the National Telecommunications and Information Administration on a variety of topics, including security updates for connected devices⁴⁰ and communications between companies and researchers on security vulnerabilities.⁴¹ Last year, FTC staff filed a comment with the National Highway Traffic Safety Administration regarding its proposed industry guidance for highly automated vehicles.⁴²

The FTC fosters technical expertise in privacy and data security, both externally and internally. In addition to generating research about privacy, data security, and technology through events such as PrivacyCon, the FTC created its own Office of Technology, Research, and Investigations (“O-Tech”), which conducts independent studies, evaluates new practices, and assists FTC staff by providing technical expertise, investigative assistance, and training. Most

³⁸ FED. TRADE COMM’N, CROSS-DEVICE TRACKING (2017), <https://www.ftc.gov/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017> [hereinafter “CROSS-DEVICE TRACKING”] (Staff Report).

³⁹ *Small Business Cybersecurity: Federal Resources and Coordination, Before the Comm. on Small Business*, 115th Cong. (2017), (statement of Maureen Ohlhausen, Acting Chairman, Federal Trade Commission), <https://www.ftc.gov/public-statements/2017/03/prepared-statement-federal-trade-commission-small-business-cybersecurity>.

⁴⁰ Comment of FTC Staff on “Communicating IoT Device Security Update Capability to Improve Transparency for Consumers,” to the Nat’l Telecomms. & Info. Admin. (June 2017), <https://www.ftc.gov/policy/policy-actions/advocacy-filings/2017/06/ftc-comment-national-telecommunications-information>.

⁴¹ Comment of FTC Staff on “Coordinated Vulnerability Disclosure ‘Early Stage’ Template,” to the Nat’l Telecomms. & Info. Admin. Safety Working Grp. (Feb. 2017), <https://www.ftc.gov/policy/policy-actions/advocacy-filings/2017/02/ftc-staff-comment-national-telecommunications>.

⁴² See Comment of Jessica L. Rich, Dir. of Bureau of Consumer Prot., Fed. Trade Comm’n, to Nathaniel Beuse, Assoc. Adm’r for Vehicle Safety Research, Nat’l Highway Traffic Safety Admin. (Nov. 21, 2016), <https://www.ftc.gov/policy/policy-actions/advocacy-filings/2016/11/comment-jessica-l-rich-director-bureau-consumer>.

recently, O-Tech conducted a study about how quickly data thieves access leaked credentials⁴³ and provided guidance to businesses on how to implement email authentication.⁴⁴ O-Tech also hosts a Technology Blog to discuss some of the more technical aspects of the agency's privacy and data security work.⁴⁵ The agency's work on new technologies is often ahead of the curve. For example, the FTC hosted a workshop on ransomware issues last year⁴⁶ and distributed education materials for businesses on these issues,⁴⁷ well before the recent WannaCry ransomware attacks that affected businesses across the globe.

The FTC also fosters innovative approaches to protect privacy and data security in other ways. For example, this year the FTC announced an IoT Home Inspector Challenge. Under the America Competes Act, it will give prize money to those who win the challenge by creating the most innovative tools for consumers to easily update the IoT products in their homes.⁴⁸ The FTC will announce the winners later this summer.

By engaging in these types of activities, the FTC and its staff have been able to build strong technical expertise. With this expertise, the FTC is able to analyze highly-technical cases in both competition and consumer protection contexts. Similarly, by hosting workshops,

⁴³ Tina Yeung & Dan Salsburg, *Tracking the Use of Leaked Consumer Data*, FED. TRADE COMM'N (May 24, 2017), https://www.ftc.gov/system/files/documents/public_events/987523/ftc-leakeddataresearch-slides.pdf.

⁴⁴ FED. TRADE COMM'N, BUSINESSES CAN HELP STOP PHISHING AND PROTECT THEIR BRANDS USING EMAIL AUTHENTICATION (Mar. 2017), <https://www.ftc.gov/reports/businesses-can-help-stop-phishing-protect-their-brands-using-email-authentication-ftc-staff> (Staff Perspective).

⁴⁵ See generally *Tech@FTC*, FED. TRADE COMM'N, <https://www.ftc.gov/news-events/blogs/techftc>.

⁴⁶ *Fall Technology Series: Ransomware*, FED. TRADE COMM'N (Sept. 7, 2016), <https://www.ftc.gov/news-events/events-calendar/2016/09/fall-technology-series-ransomware>.

⁴⁷ Ben Rossen, *Ransomware – A Closer Look*, FED. TRADE COMM'N: BUSINESS BLOG (Nov. 10, 2016, 11:05 AM), <https://www.ftc.gov/news-events/blogs/business-blog/2016/11/ransomware-closer-look>.

⁴⁸ See *IoT Home Inspector Challenge*, FED. TRADE COMM'N, <https://www.ftc.gov/iot-home-inspector-challenge>. This is the latest in a series of America Competes competitions that the FTC has held over the last several years. See, e.g., *Robocalls: Humanity Strikes Back*, FED. TRADE COMM'N, <https://www.ftc.gov/news-events/contests/robocalls-humanity-strikes-back>; *DetectaRobo*, FED. TRADE COMM'N, <https://www.ftc.gov/news-events/contests/detectarobo>; *Zapping Rachel*, FED. TRADE COMM'N, <https://www.ftc.gov/news-events/contests/zapping-rachel>; Press Release, Fed. Trade Comm'n, FTC Announces Robocall Challenge Winners (Apr. 2, 2013), <https://www.ftc.gov/news-events/press-releases/2013/04/ftc-announces-robocall-challenge-winners>.

engaging with industry, and conducting studies, the FTC has developed a unique understanding of evolving technology-related business models.

C. Business Guidance and Consumer Education

Finally, the FTC engages in business guidance and consumer education about privacy and data security issues in order to increase the impact of its enforcement and policy development initiatives. The Commission uses a variety of tools—publications, online resources, workshops, and social media—to educate consumers on a wide range of topics, including mobile apps, children’s privacy, and data security. Furthermore, the FTC helps consumers better understand the privacy and security implications of new and existing technologies. For example, the FTC’s *Net Cetera* publication helps parents, teachers, and other adults talk to children about how to be safe, secure, and responsible online.⁴⁹

Additionally, the FTC has issued numerous education materials to help consumers protect themselves from identity theft and to deal with its consequences when it does occur. Last year, the FTC launched an improved version of IdentityTheft.gov⁵⁰ (robodeidentidad.gov in Spanish⁵¹), allowing identity theft victims to create a personal recovery plan based on the type of identity theft they face, and get pre-filled letters and forms to send to credit bureaus, businesses, and debt collectors. The team that created the website is a finalist for a 2017 Service to America Medal, or “Sammie.”⁵²

Business guidance is also an important priority for the FTC. The FTC offers user-friendly guidance to help companies of all sizes improve their data security practices and comply

⁴⁹ FED. TRADE COMM’N, NET CETERA: CHATTING WITH KIDS ABOUT BEING ONLINE (2014), <https://www.consumer.ftc.gov/articles/pdf-0001-netcetera.pdf>.

⁵⁰ See IdentityTheft.gov, FED. TRADE COMM’N, <https://identitytheft.gov/>.

⁵¹ See RobodeIdentidad.gov, FED. TRADE COMM’N, <https://robodeidentidad.gov/>.

⁵² Nat Wood and the IdentityTheft.gov Development Team, SAMUEL J. HEYMAN SERVICE TO AMERICA MEDALS, https://servicetoamericamedals.org/honorees/view_profile.php?profile=483 (last visited July 14, 2017).

with the FTC Act. In November, the FTC released an update to *Protecting Personal Information: A Guide for Business*.⁵³ The FTC first published this guide in 2007 and has updated it periodically ever since. The FTC also released *Data Breach Response: A Guide for Business*, which outlines steps businesses should follow when they experience a data breach.⁵⁴

In 2015, the FTC launched its *Start with Security* initiative, which includes a guide for businesses that summarizes the lessons learned from the FTC's data security cases,⁵⁵ as well as 11 short videos.⁵⁶ These materials discuss ten important security topics and give advice about specific security practices for each. As part of this initiative, the FTC hosted events in San Francisco, Austin, Seattle, and Chicago, bringing business owners and app developers together with industry experts to discuss practical tips and strategies for implementing effective data security.⁵⁷

Last year, FTC staff also published a blog post directed toward businesses to educate them on how the FTC approach and the NIST Cybersecurity Framework are consistent.⁵⁸ Most recently, the FTC launched ftc.gov/SmallBusiness, a site to help small businesses stay ahead of the latest scams, reduce the risk of cyber threats, and respond in case of a data breach.⁵⁹ In the

⁵³ FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (2016), <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business>.

⁵⁴ FED. TRADE COMM'N, DATA BREACH RESPONSE: A GUIDE FOR BUSINESS (2016), <https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business>.

⁵⁵ FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (2015), <https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business>.

⁵⁶ *Start with Security: Free Resources for Any Business*, FED. TRADE COMM'N (Feb. 19, 2016), <https://www.ftc.gov/news-events/audio-video/video/start-security-free-resources-any-business>.

⁵⁷ *See Start with Security – Chicago*, FED. TRADE COMM'N (June 15, 2016), <https://www.ftc.gov/news-events/events-calendar/2016/06/start-security-chicago>; *Start with Security – Seattle*, FED. TRADE COMM'N (Feb. 9, 2016), <https://www.ftc.gov/news-events/events-calendar/2016/02/start-security-seattle>; *Start with Security – Austin*, FED. TRADE COMM'N (Nov. 5, 2015), <https://www.ftc.gov/news-events/events-calendar/2015/11/start-security-austin>; *Start with Security – San Francisco*, FED. TRADE COMM'N (Sept. 9, 2015), <https://www.ftc.gov/news-events/events-calendar/2015/09/start-security-san-francisco>.

⁵⁸ Andrea Arias, *The NIST Cybersecurity Framework and the FTC*, FED. TRADE COMM'N: BUSINESS BLOG (Aug. 31, 2016, 2:34 PM), <https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc>.

⁵⁹ *Protecting Small Businesses*, FED. TRADE COMM'N, <https://www.ftc.gov/smallbusiness>.

coming months, the FTC plans to expand its outreach to small businesses around data security issues, with a focus on helping very small businesses identify risks and develop data security plans.

In addition, the FTC develops privacy and data security guidance for specific industries. For example, the FTC has developed specific guidance for mobile app developers as they create, release, and monitor their apps.⁶⁰ The FTC also creates business guidance materials on specific topics – such as a tool for health-related mobile app developers to understand what federal laws and regulations might apply to their apps⁶¹ as well as business guidance aimed at helping health app developers comply with the FTC Act.⁶² Further, the FTC released guidance about ways to provide data security for Internet of Things devices, which includes tips such as designing products with authentication in mind and protecting the interfaces between devices connected to the Internet.⁶³

III. PRIVACY AND DATA SECURITY JURISDICTION OVER BIAS PROVIDERS SHOULD BE RETURNED TO THE FTC

FTC staff strongly supports returning jurisdiction to the FTC to oversee BIAS provider privacy and data security practices. This section highlights the reasons why such a return of jurisdiction would benefit consumers and industry.

⁶⁰ *App Developers: Start with Security*, FED. TRADE COMM’N (May 2017), <https://www.ftc.gov/tips-advice/business-center/guidance/app-developers-start-security>. See also *Mobile Apps*, FED. TRADE COMM’N (Mar. 13, 2013), <https://www.ftc.gov/news-events/audio-video/video/mobile-apps>.

⁶¹ *Mobile Health Apps Interactive Tool*, FED. TRADE COMM’N (Apr. 2016), <https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool>.

⁶² *Mobile Health App Developers: FTC Best Practices*, FED. TRADE COMM’N (Apr. 2016), <https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices>.

⁶³ FED. TRADE COMM’N, CAREFUL CONNECTIONS: BUILDING SECURITY IN THE INTERNET OF THINGS (2015), <https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things> [hereinafter “CAREFUL CONNECTIONS”].

A. The FTC Has Comprehensive Privacy and Data Security Expertise

First, as described above, the FTC has extensive experience addressing privacy and data security issues. Through its enforcement efforts, it sends a strong message to companies about the need to protect the privacy and security of consumers' data. Through workshops, research, and other policymaking efforts, the FTC stays abreast of technology issues and develops unique experience on the intersection of privacy, data security, and technology. And because of the FTC's far-reaching education efforts, businesses often have a one-stop shop when seeking guidance on privacy and security issues.

If the FCC adopts the proposal in the NPRM, the common carrier exception would no longer bar the FTC's oversight of a BIAS provider's privacy and data security practices. Accordingly, a BIAS provider that makes commitments—either expressly or implicitly—regarding its privacy or data security practices, and fails to live up to such commitments, would risk violating the FTC Act. Moreover, even absent such statements, a BIAS provider that fails to take reasonable precautions to protect the privacy or security of consumer data may violate the unfairness prohibition of the FTC Act.

B. The FTC Has a Deep Understanding of Privacy and Data Security in the Context of BIAS Services

Second, the FTC has developed specific expertise over privacy and data security issues affecting BIAS providers. As early as 2007, the FTC issued a staff report—*Broadband Connectivity Competition Policy*—which identified guiding principles that policymakers should consider when evaluating proposed regulations or legislation relating to BIAS providers and

network neutrality.⁶⁴ Among other things, the report highlighted the importance of protecting consumers of residential broadband service. Specifically, the report found that “effective consumer protection in the broadband marketplace 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.”⁶⁵ The report also recommended that policymakers proceed with caution in the evolving and dynamic industry of broadband Internet access.⁶⁶ The report stated that the FTC would continue to devote substantial resources to maintaining competition and protecting consumers in the broadband area.⁶⁷ Finally, the report concluded that the FTC and the FCC “each play[] an important role” in protecting consumers.⁶⁸ As for the FTC’s role, the report also concluded that enforcement of the FTC Act, a flexible and effective tool, is critical to protecting consumers of BIAS.⁶⁹ The views expressed in the report remain true today.

The FTC has consistently used its privacy and data security enforcement authority against unfair and deceptive practices by BIAS providers. For example, prior to the effective date of the Title II order, in an action against an ISP, the FTC alleged that the company caused substantial consumer injury when it distributed spam, child pornography, malware, and other harmful

⁶⁴ FED. TRADE COMM’N, BROADBAND CONNECTIVITY COMPETITION POLICY (2007), <https://www.ftc.gov/reports/broadband-connectivity-competition-policy-staff-report> [hereinafter “BROADBAND CONNECTIVITY COMPETITION POLICY”] (Staff Report).

⁶⁵ *Id.* at 130.

⁶⁶ *Id.* at 159-61.

⁶⁷ *Id.* at 155, 161.

⁶⁸ *Id.* at 161.

⁶⁹ *Id.*

electronic content.⁷⁰ The FTC also investigated Verizon for issues related to the security of its routers and issued a closing letter in 2014.⁷¹

One privacy law—not affected by the Title II Order—that the FTC continues to enforce against BIAS providers is the FCRA.⁷² Sometimes described as the first Big Data law, the FCRA is best known for regulating the activities of consumer reporting agencies. But the FCRA also applies to companies that provide information to those entities (“furnishers”) and companies that use consumer reports (“users”). BIAS providers often are both furnishers and users under the FCRA. The FTC has enforced FCRA requirements against BIAS providers. For example, the FTC brought separate cases against Time Warner Cable and Sprint for allegedly imposing less favorable terms on consumers who had negative information on their credit reports, without providing notices required by the FCRA. In both cases, the FTC obtained strong injunctions and civil penalties—\$1.9 million against Time Warner Cable⁷³ and \$2.95 million against Sprint.⁷⁴ Through these types of investigations and enforcement actions, the FTC has gained additional insight into BIAS providers’ privacy and data security related practices.

⁷⁰ *FTC v. Pricewert LLC*, No. 09-CV-2407 RMW (N.D. Cal. Apr. 8, 2010), <https://www.ftc.gov/enforcement/cases-proceedings/092-3148/pricewert-llc-dba-3fnnet-ftc>.

⁷¹ See Letter from Maneesha Mithal, Assoc. Dir. of the Div. of Privacy & Identity Prot., Fed. Trade Comm’n, to Dana Rosenfeld, Kelley Drye (Nov. 12, 2014), https://www.ftc.gov/system/files/documents/closing_letters/verizon-communications-inc./141112verizonclosingletter.pdf (finding that while Verizon took steps to mitigate the risk to consumer information, the use of WEP as an encryption standard could amount to an unreasonable practice). In addition to privacy and security enforcement actions, the FTC has also brought other kinds of cases against BIAS providers. See *infra* Part IV.

⁷² Unlike the FTC Act, the FCRA does not contain an exemption for common carrier services. See 15 U.S.C. § 1681s(a)(1) (2012) (“For the purpose of the exercise by the Federal Trade Commission of its functions and powers under the Federal Trade Commission Act, a violation of any requirement or prohibition imposed under this subchapter shall constitute an unfair or deceptive act or practice in commerce, in violation of section 5(a) of the Federal Trade Commission Act (15 U.S.C. [§] 45(a)), and shall be subject to enforcement by the Federal Trade Commission under section 5(b) of that Act [15 U.S.C. § 45(b)] with respect to any consumer reporting agency or person that is subject to enforcement by the Federal Trade Commission pursuant to this subsection, irrespective of whether that person is engaged in commerce or meets any other jurisdictional tests under the Federal Trade Commission Act.”)

⁷³ *United States v. Time Warner Cable, Inc.*, No. 13-Civ.-8998 (S.D.N.Y. Dec. 19, 2013), <https://www.ftc.gov/enforcement/cases-proceedings/122-3149/time-warner-cable-inc>.

⁷⁴ *United States v. Sprint Corp.*, No. 2:15-CV-9340 (D. Kan. Oct. 21, 2015), <https://www.ftc.gov/enforcement/cases-proceedings/142-3094/sprint-corporation-sprint-asl-program-0>.

In addition to enforcement, the FTC has long engaged in policy initiatives and business guidance efforts particularly germane to BIAS providers' privacy and data security practices. For example, in addition to the FTC staff's 2007 report on broadband competition, the FTC discussed how principles of transparency, choice, and privacy-by-design would apply to BIAS providers in its *2012 Privacy Report*. For example, the report noted that while the FTC had strong concerns about the use of deep packet inspection for unexpected purposes without affirmative express consent, it supported a technology neutral framework that did not single out one particular type of entity or practice.⁷⁵ Following the issuance of the report, the FTC hosted a workshop on the privacy practices of large platform providers, such as BIAS providers, operating systems, browsers, and social media companies.⁷⁶ The event examined the benefits and risks of comprehensive data collection practices by these entities, whether consumers are aware of these practices, and the extent to which consumers could exercise choices over these practices. These initiatives illustrate the expertise and the interest of the FTC in vigorously protecting consumers of BIAS.

Similarly, much of the business guidance discussed above is instructive for BIAS providers, as they can collect and use the exact same types of data as other companies that are in the Internet ecosystem and are currently under the FTC's jurisdiction. FTC guidance—ranging from securing personal information, to what to do in the event of a breach or ransomware attack, to how to implement email authentication—is equally applicable to BIAS providers.

⁷⁵ 2012 PRIVACY REPORT, *supra* note 33, at 55-57.

⁷⁶ *The Big Picture: Comprehensive Online Data Collection*, FED. TRADE COMM'N (Dec. 6, 2012), <https://www.ftc.gov/news-events/events-calendar/2012/12/big-picture-comprehensive-online-data-collection>.

C. The FTC Can Enforce Heightened Standards for Protecting Children's Information

A third reason to return the FTC's jurisdiction over BIAS providers is so that children's online information receives the higher level of privacy protection Congress intended it to have. If the FCC adopts the NPRM's proposed reclassification, the FTC's COPPA Rule will once again apply to BIAS providers. The COPPA Rule requires certain entities to provide notice to parents and obtain verifiable consent before they collect personal information from children under 13 years of age. These entities include operators of child-directed websites and online services, and third parties that knowingly collect information from such websites and online services. Thus, an entity that conducts behavioral advertising on a website it knows to be child-directed may be subject to the COPPA Rule. Currently, third-party advertising networks are subject to these requirements but BIAS providers are not.

Since 2000, the FTC has brought twenty-six COPPA cases and obtained more than \$10,000,000 in civil penalties. The FTC has enforced COPPA's requirements against businesses ranging from advertising networks⁷⁷ to mobile app developers⁷⁸ to social media companies.⁷⁹ If the FCC adopts the proposed reclassification, certain BIAS providers may be subject to COPPA and its implementing rules, thereby reestablishing a uniform, robust, and comprehensive application of rules to protect the privacy and security of children's data online.

⁷⁷ See, e.g., *United States v. InMobi Pte. Ltd.*, No. 3:16-CV-03474 (N.D. Cal. June 22, 2016), <https://www.ftc.gov/enforcement/cases-proceedings/152-3203/inmobi-pte-ltd>.

⁷⁸ See, e.g., *United States v. W3 Innovations, LLC*, No. CV-11-03958 (N.D. Cal. Sept. 8, 2011), <https://www.ftc.gov/enforcement/cases-proceedings/102-3251/w3-innovations-llc-dba-broken-thumb-apps-justin-maples-us>.

⁷⁹ See, e.g., *United States v. Path, Inc.*, No. 3:13-cv-00448-RS (N.D. Cal. Jan. 31, 2013), <https://www.ftc.gov/enforcement/cases-proceedings/122-3158/path-inc>.

D. The FTC Should Be Able to Address Privacy and Security Issues Throughout the Entire Internet Ecosystem

A fourth reason to return jurisdiction to the FTC is to close an important gap in online consumer protection. As a matter of consistency, it makes little sense to exclude only BIAS providers from the FTC's privacy and data security jurisdiction, which covers virtually all other entities in the Internet ecosystem, including some of the largest and most powerful companies using consumer data. Indeed, the FTC has actively applied its authority across the Internet, including bringing actions against social media companies,⁸⁰ Original Equipment Manufacturers,⁸¹ operating systems,⁸² software providers,⁸³ content providers,⁸⁴ app developers,⁸⁵ IoT companies,⁸⁶ and ad networks.⁸⁷ It has issued specific guidance to app stores,⁸⁸ app developers,⁸⁹ ad networks,⁹⁰ and others.⁹¹ And, as noted earlier, prior to 2015, the FTC had

⁸⁰ See, e.g., *Facebook, Inc.*, No. C-4365 (F.T.C. July 27, 2012), <https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc>; *Google, Inc.*, No. C-4336 (F.T.C. Oct. 13, 2011), <https://www.ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter>.

⁸¹ See, e.g., *HTC Am. Inc.*, No. C-4406 (F.T.C. June 25, 2013), <https://www.ftc.gov/enforcement/cases-proceedings/122-3049/htc-america-inc-matter>.

⁸² See, e.g., *Microsoft Corp.*, No. C-4069 (F.T.C. Dec. 20, 2002), <https://www.ftc.gov/enforcement/cases-proceedings/012-3240/microsoft-corporation-matter>.

⁸³ See, e.g., *Oracle Corp.*, No. C-4571 (F.T.C. Mar. 28, 2016), <https://www.ftc.gov/enforcement/cases-proceedings/132-3115/oracle-corporation-matter>.

⁸⁴ See, e.g., *FTC v. ruby Corp.*, No. 1:16-CV-02438 (D.D.C. Dec. 14, 2016), <https://www.ftc.gov/enforcement/cases-proceedings/152-3284/ashley-madison>.

⁸⁵ See, e.g., *Credit Karma, Inc.*, No. C-4480 (F.T.C. Aug. 13, 2014), <https://www.ftc.gov/enforcement/cases-proceedings/132-3091/credit-karma-inc>; *Fandango, LLC*, No. C-4481 (F.T.C. Aug. 13, 2014), <https://www.ftc.gov/enforcement/cases-proceedings/132-3089/fandango-llc>.

⁸⁶ See, e.g., *ASUSTeK Computer, Inc.*, No. C-4587 (F.T.C. July 18, 2016), <https://www.ftc.gov/enforcement/cases-proceedings/142-3156/asustek-computer-inc-matter>; *TRENDnet, Inc.*, No. C-4426 (F.T.C. Jan. 16, 2014), <https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter>.

⁸⁷ See, e.g., *Turn Inc.*, No. C-4612 (F.T.C. Apr. 6, 2017), <https://www.ftc.gov/enforcement/cases-proceedings/152-3099/turn-inc-matter>; *United States v. InMobi Pte. Ltd.*, No. 3:16-CV-03474 (N.D. Cal. June 22, 2016), <https://www.ftc.gov/enforcement/cases-proceedings/152-3203/inmobi-pte-ltd>.

⁸⁸ See, e.g., *MOBILE PRIVACY DISCLOSURES*, *supra* note 35.

⁸⁹ See, e.g., *App Developers: Start with Security*, *supra* note 60; *Mobile Apps*, *supra* note 60.

⁹⁰ See, e.g., *CROSS-DEVICE TRACKING*, *supra* note 38.

⁹¹ See, e.g., *CAREFUL CONNECTIONS*, *supra* note 63.

brought cases against BIAS providers as well.⁹² The Title II Order pulled the BIAS provider puzzle piece out of an otherwise unified picture of internet consumer protection.

The resulting gap is especially problematic with the advent of IoT. For example, consider last year's Mirai botnet attack, where attackers used IoT devices on home networks as botnets to launch Distributed Denial of Service Attacks. Both IoT companies and BIAS providers have a role in stopping such attacks. IoT companies can enhance the security of their devices so that they do not become part of botnet armies, and BIAS providers can address denial of service attacks that originate on or attack their networks. Closing the consumer protection gap by restoring jurisdiction to an agency with expertise over both sets of entities will help address future IoT botnet attacks.

Indeed, having one agency with jurisdiction over these entities would ensure consistent standards and consistent application of such standards. FTC staff believes that the same federally-enforced, consumer-focused privacy and data security approach should apply regardless of whether companies provide broadband services, data analytics, social media, or other so-called edge services. Accordingly, FTC staff encourages the FCC to adopt the proposed reclassification, thereby creating a level playing field for all companies operating in the Internet ecosystem.

⁹² See, e.g., *FTC v. Pricewert LLC*, No. 09-CV-2407 RMW (N.D. Cal. Apr. 8, 2010), <https://www.ftc.gov/enforcement/cases-proceedings/092-3148/pricewert-llc-dba-3fnnnet-ftc>; *Am. Online, Inc.*, No. C-4105 (F.T.C. Jan. 28, 2004), <https://www.ftc.gov/enforcement/cases-proceedings/002-3000/america-online-inc-compuserve-interactive-services-incin>; *Juno Online Servs., Inc.*, No. C-4016 (F.T.C. June 25, 2001), <https://www.ftc.gov/enforcement/cases-proceedings/002-3061/juno-online-services-inc>; *Am. Online, Inc.*, No. C-3787 (F.T.C. Mar. 16, 1998), <https://www.ftc.gov/enforcement/cases-proceedings/952-3331/america-online-inc-matter>; *CompuServe, Inc.*, No. C-3789 (F.T.C. Mar. 16, 1998), <https://www.ftc.gov/enforcement/cases-proceedings/962-3096/compuserve-inc-matter>; *Prodigy Servs. Corp.*, No. C-3788 (F.T.C. Mar. 16, 1998), <https://www.ftc.gov/enforcement/cases-proceedings/952-3332/prodigy-services-corporation-matter>.

E. If the FTC’s Jurisdiction Is Returned, Companies Will Be Eligible to Sign Up for the EU-U.S. Privacy Shield Framework for Their BIAS Services

Fifth, returning the FTC’s jurisdiction to BIAS companies will expand the number of companies eligible to sign up for the EU-U.S. Privacy Shield Framework.⁹³ Only companies that are subject to the jurisdiction of the FTC or the Department of Transportation are eligible to sign up for the Privacy Shield at this time.⁹⁴ If jurisdiction is returned to the FTC, companies will be eligible to participate in Privacy Shield for their BIAS services, allowing BIAS providers to continue to protect the privacy and security of consumers’ data, avoid undue regulatory burdens, and ensure that their cross-border data flows are not interrupted in an increasingly global economy.

F. The FTC’s Approach to Privacy and Data Security Protects Consumers and Promotes Innovation

Finally, the FTC’s flexible, enforcement-focused approach has enabled the agency to apply strong consumer privacy and security protections across a wide range of changing technologies and business models, without imposing unnecessary or undue burdens on industry. As discussed earlier, the FTC’s enforcement, policy, and education work have successfully shaped business practices and have highlighted to industry the importance of protecting consumer privacy and data security.

The FTC enforces laws set forth by Congress, or rules established by the FTC pursuant to Congressional grants of authority. Each such case and accompanying order corrects past actions by the defendant company, prevents future violations by that company, and deters other companies from the problematic behavior. By focusing on practices that have already harmed or

⁹³ See generally PRIVACY SHIELD FRAMEWORK, *supra* note 26.

⁹⁴ *Enforcement of Privacy Shield*, PRIVACY SHIELD FRAMEWORK, <https://www.privacyshield.gov/article?id=Enforcement-of-Privacy-Shield> (last visited July 14, 2017).

are likely to harm consumers, and on claims that are material to consumers, the FTC can address the most problematic privacy and security practices, while avoiding overly-prescriptive rules that may quickly become obsolete in a rapidly-changing industry.

Some have criticized the FTC’s Section 5 enforcement-focused approach as inadequate compared to a rules-based approach. This is a false dichotomy. Effective rule of law requires both appropriate standards—whether established by common law court, Congress in statute, or by an agency in rules—and active enforcement of those standards. Congress has charged the FTC with preventing unfair and deceptive practices. This standard has proven to be enforceable in the courts, as demonstrated by the FTC’s success in thousands of consumer protection cases. This standard has also proven adaptable to protecting consumers in a wide range of industries and situations, including online privacy and data security.

In short, the FTC has delivered the message to entities in a range of fields—retailers, app developers, data brokers, health companies, financial institutions, third-party service providers, and others—that they need to provide consumers with strong privacy and data security protections. The same approach and oversight should apply to BIAS providers.

IV. IT IS ALSO IMPORTANT TO RESTORE THE FTC’S GENERAL CONSUMER PROTECTION AUTHORITY OVER BIAS PROVIDERS

Adopting the proposed rule would not only restore the FTC’s jurisdiction over BIAS providers’ privacy and data security practices but would also restore the FTC’s unique jurisdiction over BIAS providers’ consumer protection practices as a whole. The FTC staff supports this outcome.

The FTC has extensive expertise with advertising, marketing, and billing of BIAS services, which it exercised routinely prior to the issuance of the Title II order.⁹⁵ Indeed, the FTC has brought numerous cases involving these practices dating back to 1998. In that year, it brought a trio of cases against America Online, Prodigy, and CompuServe for deceptive advertising of trial periods for online services.⁹⁶ In the 2000s, it brought a series of cases involving deceptive advertising for Internet access services. For example, in a case against Juno Online Services, the FTC challenged the company's deceptive representations about the actual cost to consumers of the company's free and fee-based dial-up Internet access services.⁹⁷ It also challenged the company's failure to honor cancellations during a purported free trial period.⁹⁸ In addition, the FTC brought a case alleging that AOL and CompuServe continued to bill Internet service subscribers who asked that their service be cancelled, and failed to timely deliver \$400 rebates.⁹⁹ In 2014, the FTC alleged that AT&T deceptively advertised "unlimited" data while throttling mobile customers who used certain amounts of data.¹⁰⁰ Finally, in 2015, TracFone, the

⁹⁵ While this comment is limited to returning jurisdiction over BIAS providers to the FTC through FCC reclassification, the FTC separately continues to advocate to Congress that it repeal the common carrier exception, which would give the FTC jurisdiction over both BIAS and traditional common carrier services, such as telephony. The exception no longer makes sense in today's deregulated environment where the lines between telecommunications and other services are increasingly blurred. *See, e.g., Oversight of the Federal Trade Commission Before the S. Comm. on Commerce, Sci., & Transp.*, 114th Cong. 22-25 (2016), <https://www.ftc.gov/public-statements/2016/09/prepared-statement-federal-trade-commission-oversight-federal-trade> (statement of the Fed. Trade Comm'n).

⁹⁶ *Am. Online, Inc.*, No. C-3787 (F.T.C. Mar. 16, 1998), <https://www.ftc.gov/enforcement/cases-proceedings/952-3331/america-online-inc-matter>; *CompuServe, Inc.*, No. C-3789 (F.T.C. Mar. 16, 1998), <https://www.ftc.gov/enforcement/cases-proceedings/962-3096/compuserve-inc-matter>; *Prodigy Servs. Corp.*, No. C-3788 (F.T.C. Mar. 16, 1998), <https://www.ftc.gov/enforcement/cases-proceedings/952-3332/prodigy-services-corporation-matter>.

⁹⁷ *Juno Online Servs., Inc.*, No. C-4016 (F.T.C. June 25, 2001), <https://www.ftc.gov/enforcement/cases-proceedings/002-3061/juno-online-services-inc>.

⁹⁸ *Id.*

⁹⁹ *Am. Online, Inc.*, No. C-4105 (F.T.C. Jan. 28, 2004), <https://www.ftc.gov/enforcement/cases-proceedings/002-3000/america-online-inc-compuserve-interactive-services-incin>.

¹⁰⁰ *FTC v. AT&T Mobility, LLC*, No. 3:14-CV-04785-EMC (N.D. Cal. Oct. 28, 2014), <https://www.ftc.gov/enforcement/cases-proceedings/122-3253/att-mobility-llc-mobile-data-service>. That case, which presents the issue of whether the common carrier exception is activity-based or status-based, is currently

largest prepaid mobile provider in the United States, agreed to pay \$40 million to the FTC for consumer refunds to settle charges that it deceived millions of consumers with regard to its “unlimited” data service.¹⁰¹

Indeed, in consumer protection areas outside of privacy and data security, the FTC often obtains monetary relief in the form of redress to consumers. In 2016, for example, the FTC returned \$160 million to over 5 million consumers. Where BIAS providers engage in deceptive advertising, unauthorized billing, or pure fraud, the FTC must be able to take action, not only to stop such practices prospectively, but also to return money to consumers who have already been harmed.

V. THE FTC HAS EXPERTISE IN ENFORCING THE ANTITRUST LAWS ACROSS ALL INDUSTRIES

Reclassifying BIAS from a common carrier service to an information service would restore not only the Commission’s authority over unfair and deceptive acts or practices, but also over unfair methods of competition, returning the Commission’s antitrust enforcement authority to that which existed prior to 2015. In that regulatory environment, after years of substantial and systematic deregulation of broadband services and facilities by the FCC, the FTC enforced the antitrust laws for the benefit of consumers in BIAS markets, just as it does throughout the economy.¹⁰²

before the Ninth Circuit *en banc*. See *FTC v. AT&T Mobility LLC*, No. 15-16585, 2017 WL 1856836 (9th Cir. May 9, 2017). See also *supra* note 4 and accompanying text.

¹⁰¹ *FTC v. TracFone Wireless, Inc.*, No. 15-cv-00392-EMC (N.D. Cal. Feb. 20, 2015), <https://www.ftc.gov/enforcement/cases-proceedings/132-3176/straight-talk-wireless-tracfone-wireless-inc>.

¹⁰² For example, prior to 2015, the FTC examined mergers among firms that provided multichannel video programming distribution, some of which were jurisdictional to the FCC and some of which were not. See Statement of Chairman Majoras, Commissioner Kovacic, and Commissioner Rosch Concerning the Closing of the Investigation Into Transactions Involving Comcast, Time Warner Cable, and Adelphia Communications (Jan. 31, 2006), <https://www.ftc.gov/public-statements/2006/01/statement-chairman-majoras-commissioner-kovacic-commissioner-rosch>; Statement of Commissioners Jon Leibowitz and Pamela Jones Harbour (Concurring in Part, Dissenting in Part), Time Warner/Comcast/Adelphia (Jan. 31, 2006),

The FTC has worked to prevent unfair methods of competition since its inception over a century ago, and has developed deep expertise in applying competition principles across many industries. The antitrust laws protect the competitive process, which fosters a “state of affairs in which output is maximized, price is minimized, and consumers are entitled to make their own choices.”¹⁰³ These laws apply across all industries, and are flexible enough to encompass emerging technologies and companies that may transform the existing competitive landscape. They are sufficiently adaptable to change along with the economic and industrial landscape, and have been successfully applied to a diverse array of industries across the entire economic spectrum: coal; railroads; electricity; air and surface transportation; computers and computer software; and a variety of markets that transitioned away from utility-style regulation.

The FTC’s antitrust mission complements its consumer protection mission. It is a fact-based, flexible, and enforcement-focused approach built on the FTC’s significant experience in weighing potential anticompetitive effects against the procompetitive effects and efficiencies that drive business practices in fast-growing industries. Using this approach, the FTC is able to protect consumers and the competitive process without placing undue burdens on industry. Prior to 2015, the FTC used this approach in a number of important investigations in Internet and Internet-related markets.¹⁰⁴

<https://www.ftc.gov/public-statements/2006/01/statement-chairman-majoras-commissioner-kovacic-commissioner-rosch>. The FTC shares antitrust jurisdiction with the Department of Justice (“DOJ”) in most areas of the economy, and relies on long-standing arrangements and understandings with the DOJ in order to avoid inconsistent or duplicative efforts. DOJ has also examined competition in BIAS markets during its review of telephone company mergers. *See, e.g., United States v. SBC Commc’ns., Inc.*, 489 F. Supp. 2d 1 (D.D.C. 2007).

¹⁰³ HERBERT HOVENKAMP, *FEDERAL ANTITRUST POLICY: THE LAW OF COMPETITION AND ITS PRACTICE* 339 (5th ed. 2015). *See also* *FTC v. Indiana Fed’n of Dentists*, 476 U.S. 447 (1986).

¹⁰⁴ *See, e.g., Nielsen Holdings N.V.*, No. C-4439 (F.T.C. Feb. 24, 2014), <https://www.ftc.gov/enforcement/cases-proceedings/131-0058/nielsen-holdings-nv-arbitron-inc-matter>; *Am. Online, Inc.*, 131 F.T.C. 829 (2000); *Cablevision Sys. Corp.*, 125 F.T.C. 813 (1998); *Time Warner Inc.*, 123 F.T.C. 171 (1997); *Summit Commc’ns. Grp., Inc.*, 120 F.T.C. 846 (1995).

The competitive issues raised by the growth of the Internet and all of its subsidiary technologies are not new to antitrust law, which is well equipped to analyze potential conduct and business arrangements involving ISP access, contracting, merger issues, or other arrangements that may impact competitive dynamics.¹⁰⁵ Indeed, the FTC has significant expertise in understanding competition in broadband markets.¹⁰⁶ In conducting an antitrust analysis, the ultimate issue would be whether broadband Internet access providers engage in unilateral or joint conduct that is likely to harm competition in a relevant market, depriving customers and consumers of the benefits of a free market. There is no reason to assume that Internet-related firms are any more or less willing or able to engage in anticompetitive behavior than firms in other economic sectors.

Internet-related markets may be susceptible to a number of practices that traditionally raise antitrust issues. Unilateral conduct on the part of broadband providers—for example, foreclosing rival content in an exclusionary or predatory manner—may be challenged under Section 2 of the Sherman Act. Section 1 of the Sherman Act could be used to analyze contractual relationships that may block access to the Internet by content or applications providers or discriminate in favor of a supplier with whom the broadband provider has an affiliated or contractual relationship under exclusive dealing theories. Vertical integration into content or applications markets by broadband providers would be analyzed under the merger laws.

¹⁰⁵ See generally Maureen K. Ohlhausen, *Antitrust over Net Neutrality: Why We Should Take Competition in Broadband Seriously*, 15 COLO. TECH. L.J. 119 (2016) (explaining how antitrust can protect against anticompetitive violations of net neutrality).

¹⁰⁶ See generally BROADBAND CONNECTIVITY COMPETITION POLICY, *supra* note 64.

A. Unilateral Conduct

Section 2 of the Sherman Act makes it illegal for a firm to monopolize or attempt to monopolize trade. As an example, Section 2 bars exclusionary conduct by a firm with market power—for example, blocking emerging rivals from using available channels of distribution—where such conduct prevents such rivals from competing on the merits and enables the firm to maintain or attain a monopoly position (absent a sufficient procompetitive justification). Section 2 claims are judged under a rule of reason, weighing the potential for anticompetitive harm against any legitimate business justifications for the conduct.

Although the FTC is not a sector regulator, its antitrust authority can address concerns that often motivate utility-style regulation. Specifically, Section 2 can address, without comprehensive regulation, problematic conduct related to access, discrimination, pricing, bundling and regulatory evasion.

For instance, Section 2 may prohibit a firm with a dominant position from using exclusive contracts to deny potential rivals access to efficient distribution or supply. Exclusive dealing programs can be harmful when they allow a monopolist to maintain its monopoly power by preventing rivals from achieving the scale of operations required to become efficient competitors.¹⁰⁷ Absent a demonstrable procompetitive rationale, the use of exclusive contracts, especially when coupled with threats to withhold supply, may hinder entry and deprive customers of the benefits of price, innovation, and quality competition.¹⁰⁸ Similarly, a monopolist may not rely on *de facto* exclusive arrangements—offering payments or other

¹⁰⁷ See *McWane v. FTC*, 783 F.3d 814, 832 (11th Cir. 2015).

¹⁰⁸ See *Victrex plc*, No. C-4586 (F.T.C. July 30, 2016).

incentives to customers to avoid using rivals' products—where this would unreasonably impede such rivals' ability to compete (absent some sufficient procompetitive justification).¹⁰⁹

B. Section 1 Issues

The antitrust laws also prohibit agreements among competitors that substantially reduce competition. For instance, agreements among competitors to fix prices, reduce output, or allocate customers are so inherently likely to harm competition that they are deemed *per se* illegal. Other collaborations among competitors are judged under a rule of reason analysis. That analysis examines the purpose and effect of the joint conduct, the product characteristics, market dynamics and other competitive characteristics of the affected sector, along with any procompetitive business justifications. Examples of such conduct include exchange of competitively sensitive information among competitors and standard setting activities. For example, the Department of Justice recently settled allegations that DIRECTV acted as a ringleader to exchange competitively sensitive information among three competitors (Cox Communications, Charter Communications, and AT&T) while the firms were separately negotiating for the rights to telecast live Dodgers games in the Los Angeles area.¹¹⁰ DOJ alleged that these communications, which revealed each firm's negotiating position, strategy, or tactics concerning potential agreements, violated Section 1 of the Sherman Act and were a material factor in the companies' decisions not to carry the Dodger Channel. The defendants settled the charges by agreeing not to share competitively sensitive information about future actions.

¹⁰⁹ See *United States v. Dentsply Int'l, Inc.*, 399 F.3d 181, 187 (3d Cir. 2005).

¹¹⁰ *United States v. DIRECTV Grp. Holdings, LLC*, 2:16-cv-08150 (C.D. Cal. Mar. 23, 2017), <https://www.justice.gov/atr/case/us-v-directv-group-holdings-llc-and-att-inc>.

C. Vertical Integration

Most forms of vertical integration can generate procompetitive efficiencies, thus antitrust analysis generally regards them as harmless or even beneficial to consumer welfare.¹¹¹

However, such integration may be anticompetitive under specific circumstances. A vertical merger between a firm with significant market power and one of its suppliers (or one of its distributors), for example, could substantially impede rivals' competitive opportunities and thereby harm competition where entry at each level is costly and/or requires an extended period of time. Such competitive harm might occur by either denying competitors access to essential inputs (for example, in the market for broadband Internet access) or denying access to downstream distribution outlets (for example, in the market for online content and applications).

The Commission has investigated vertical mergers in Internet-related markets and imposed conditions when necessary to prevent conduct that would disadvantage rivals. For instance, in 2000, the Commission reviewed the merger of America Online, Inc. ("AOL") and Time Warner and issued an order designed to prevent the newly integrated company from denying competitors access to then-emerging broadband technology. According to the Commission, combining AOL, the nation's largest ISP, with Time Warner, owner of many cable systems and valuable programming, would substantially lessen competition in the markets for residential broadband Internet access and interactive television, as well as undermine AOL's incentive to promote DSL broadband internet service as an emerging alternative to cable broadband. The Commission's order resolved these antitrust concerns by imposing a number of

¹¹¹ James C. Cooper et al., *Vertical Antitrust Policy as a Problem of Inference*, 23 INT'L J. INDUS. ORG. 639, 662 (2005); see also February 2007 Submission of the U.S. Department of Justice and the U.S. Federal Trade Commission on Vertical Mergers DAF/COMP/WD2(2007)38, at 7-9 (Feb. 15, 2007), <https://www.ftc.gov/sites/default/files/attachments/us-submissions-oecd-and-other-international-competition-fora/07RoundtableonVerticalMergers.pdf>.

conditions to prevent the integrated firm from denying access to or discriminating against unaffiliated ISPs.¹¹²

The FTC's investigations and enforcement actions in Internet-related markets has been consistent with its actions in other industries. Where harm to competition outweighs the potential benefits to consumers, the FTC has initiated antitrust enforcement. Equally important, the Commission has stayed its hand when business practices are procompetitive. To grow output and foster innovation across the economy as a whole, firms must be subject to consistent antitrust enforcement—enforcement that holds firms accountable to protect consumers without placing undue restrictions on business practices that enable new technologies to flourish. The FTC's activities in Internet-related markets demonstrate its ability to protect the competitive process, promote the innovation that such competition fosters, and preserve the resulting benefits to consumers.

VI. CONCLUSION

FTC staff appreciates this opportunity to describe the agency's expertise in protecting consumers and the competitive process online, and to express its support for the proposal to return jurisdiction over BIAS to the FTC. FTC staff looks forward to working with the FCC to ensure a consistent, efficient, and effective approach to enforcement and oversight in the broadband area.

¹¹² *Am. Online, Inc.*, No. C-3989 (F.T.C. Apr. 17, 2001), <https://www.ftc.gov/enforcement/cases-proceedings/0010105/america-online-inc-time-warner-inc>. Specifically, under the Commission's order, AOL Time Warner was: required to open its cable system to competitor ISPs; prohibited from interfering with content passed along the bandwidth contracted for by non-affiliated ISPs and from interfering with the ability of non-affiliated providers of interactive TV services to interact with interactive signals, triggers or content that AOL Time Warner has agreed to carry; prevented from discriminating on the basis of affiliation in the transmission of content, or from entering into exclusive arrangements with other cable companies with respect to ISP services or interactive TV services; and required to market and offer AOL's digital subscriber line services to subscribers in Time Warner cable areas where affiliated cable broadband service is available in the same manner and at the same retail pricing as they do in those areas where affiliated cable broadband ISP service is not available.