Before the
NATIONAL TELECOMMUNICATIONS & INFORMATION ADMINISTRATION
Washington, DC

In the Matter of Developing the Administration's Approach to Consumer Privacy	Docket No. 180821780–8780–01

To: National Telecommunications and Information Administration
Date: November 9, 2018

I. Introduction

Thank you for the opportunity for FTC staff to comment on the Department of Commerce, National Telecommunications and Information Administration ("NTIA") Request for Comment on Developing the Administration's Approach to Consumer Privacy ("RFC").

As the nation's consumer protection and competition agency, the Federal Trade Commission ("FTC" or "Commission") is committed to protecting consumers' privacy and security interests while promoting competition and innovation. We commend the NTIA for addressing this timely issue and support efforts by both the Administration and Congress to evaluate the effectiveness of current frameworks and to identify "ways to advance consumer privacy while protecting prosperity and innovation."[1] The Commission is exploring precisely these issues through a series of Hearings on Competition and Consumer Protection in the 21st Century.[2]

[1] NAT'L TELECOMM. & INFO. ADMIN., Request for Comment on Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48600 (Sept. 26, 2018).

[2] *See* Press Release, Fed. Trade Comm'n, FTC Announces Hearings On Competition and Consumer Protection in the 21st Century (June 20, 2018), https://www ftc.gov/news-events/press-releases/2018/06/ftc-announces-hearings-competition-consumer-protection-21st. Just this week, the Commission held hearings on the Intersection of Big Data, Privacy, and Competition. Agenda, The Intersection of Big Data, Privacy, and Competition, Hearings on

Consumer data privacy is an important and timely topic. Today, companies often provide digital services and content powered by (or in exchange for) consumer data. News headlines draw attention to remarkable innovation—in mobile apps,[3] mobile payment systems,[4] connected devices,[5] automated cars,[6] etc.—that both stems from and necessitates the collection, use, and disclosure of consumer data. At the same time, however, news headlines highlight potentially problematic privacy practices: a dating app's disclosure of HIV status to software vendors,[7] a tracking firm's inadvertent exposure of the real-time geolocation data of 200 million people,[8] or an IoT firm's decision to track sex toy use without users' consent.[9] These twin trends—data-driven innovation and increasing data privacy concerns—have raised important questions about the ability of the existing legal landscape to protect consumers' privacy interests. In addition, as

---

Competition and Consumer Protection in the 21st Century, Fed. Trade Comm'n (Nov. 6-8, 2018), https://www ftc.gov/system/files/documents/public_events/1418633/hearings-agenda-au_0.pdf. We will be holding additional hearings on data security and privacy in December 2018 and February 2019, respectively. Press Release, Fed. Trade Comm'n, FTC Announces Sessions on Consumer Privacy and Data Security As Part of its Hearings on Competition and Consumer Protection in the 21st Century, Oct. 26, 2018, https://www ftc.gov/news-events/press-releases/2018/10/ftc-announces-sessions-consumer-privacy-data-security-part-its. All of these hearings, as well as the public comments we have received and expect to receive in the future, serve as an opportunity for the Commission to explore the issues further and develop greater expertise.

[3] Eric Rosenbaum, *The Most Popular Free Apps to Keep You Healthy in 2018*, CNBC, Jan. 5, 2018, https://www.cnbc.com/2018/01/05/top-5-free-apps-to-keep-you-healthy-in-2018.html.

[4] Michael Muchmore, *The Best Mobile Payment Apps of 2018*, PC MAGAZINE, Apr. 2, 2018, https://www.pcmag.com/roundup/358553/the-best-mobile-payment-apps.

[5] Charlie Osborne, *The Best IoT, Smart Home Gadgets in 2018*, ZDNET, Apr. 24, 2018, https://www.zdnet.com/pictures/the-best-iot-smart-home-gadgets-in-2018/.

[6] Marco della Cava, *What's It Like to Run Errands in a Self-driving Car? Some Phoenix Regulars Are Sold on Waymo*, USA TODAY, Oct. 10, 2018, https://www.usatoday.com/story/money/2018/10/10/waymo-self-driving-cars-hit-10-million-road-miles-they-aim-public-debut/1536441002/.

[7] Natasha Singer, *Grindr Sets Off Privacy Firestorm After Sharing Users' H.I.V.-Status Data*, N.Y TIMES, Apr. 3, 2018, https://www.nytimes.com/2018/04/03/technology/grindr-sets-off-privacy-firestorm-after-sharing-users-hiv-status-data html.

[8] Brian Barrett, *A Location Sharing Disaster Shows How Exposed You Really Are*, WIRED, May 19, 2018, https://www.wired.com/story/locationsmart-securus-location-data-privacy/.

[9] Alex Hern, *Vibrator Maker Ordered to Pay Out C$4m for Tracking Users' Sexual Activity*, THE GUARDIAN, Mar. 14, 2017, https://www.theguardian.com/technology/2017/mar/14/we-vibe-vibrator-tracking-users-sexual-habits.

the RFC notes,[10] the emergence of new legal frameworks at the state and international levels presents the question of whether a new national approach would benefit consumers and competition.

As described below, the Commission has deep experience in protecting consumer privacy and fostering innovation. For decades, the Commission has enforced our existing consumer protection laws, which take a flexible, risk-based approach to consumer privacy that "balance[s] business needs, consumer expectations, legal obligations, and potential privacy harms, among other inputs."[11] In this comment, we first describe our experience in protecting consumers' privacy interests through enforcement, education, and policy work. We then discuss the guiding principles of our current approach: balancing risk of harm with the benefits of innovation and competition. After laying this groundwork, the comment applies this approach of balancing risks and benefits to address four specific areas highlighted in the RFC: security, transparency, control, and FTC enforcement. Finally, the comment looks to the future, considering potential directions for privacy policy in the United States.

II. Background on the FTC

The FTC is an independent administrative agency responsible for protecting consumers and promoting competition. The Commission has proven itself a government leader in privacy, through enforcement actions, consumer and business education, and policy efforts.

On the enforcement front, the FTC conducts investigations and brings cases under a wide range of laws. First and foremost, the Commission enforces the FTC Act, which prohibits unfair and deceptive acts or practices—including unfair and deceptive privacy and security practices—

[10] RFC, *supra* note 1 at 48600.

[11] *Id.* at 48602.

in or affecting commerce.[12] The FTC enforces specific statutes that protect a host of consumer data, including certain health information (via the Health Breach Notification Rule),[13] credit information (through the Fair Credit Reporting Act ("FCRA")),[14] financial data (as described in the privacy and security rules implementing the Gramm-Leach-Bliley ("GLB") Act),[15] and children's information (as defined in the Children's Online Privacy Protection Act ("COPPA")).[16] The Commission also enforces laws that protect consumers from certain intrusions, such as unwanted phone calls or emails, including the Telemarketing Sales Rule ("TSR"),[17] CAN-SPAM Rule,[18] and the Fair Debt Collection Practices Act ("FDCPA").[19]

[12] 15 U.S.C. § 45(a). The FTC's unfairness cases have challenged privacy and security practices that cause or are likely to cause substantial harm to consumers. *See, e.g.*, Aaron's, Inc., No. C-442 (F.T.C. Mar. 10, 2014), https://www ftc.gov/system/files/documents/cases/140311aaronscmpt.pdf (Complaint); FTC v. Ruby Corp. No. 1:16-cv-02438 (D.D.C. Dec. 14, 2016), https://www ftc.gov/system/files/documents/cases/161214ashleymadisoncmplt1.pdf (Complaint). And, when businesses present otherwise beneficial products and services in a deceptive manner, consumers lose the opportunity to make informed choices and may be injured. *See, e.g.*, Practice Fusion, Inc., No. C-4591 (F.T.C. Aug. 15, 2016), https://www ftc.gov/system/files/documents/cases/160816practicefusioncmpt.pdf (Complaint) (alleging that the company deceived consumers about why it was collecting potentially sensitive healthcare information); FTC v. Vizio, Inc., No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017), https://www ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf (Complaint) (Smart TV manufacturer Vizio offered consumers an innovative TV, but allegedly misled consumers about the extent to which Vizio's TVs collected and used consumer viewing information).

[13] 16 C.F.R. Part 318.

[14] 15 U.S.C. § 1681 *et seq*.

[15] 15 U.S.C. § 6801 *et seq*.; Privacy of Consumer Financial Information, 16 C.F.R. Part 313 ("GLB Privacy Rule"); Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 ("GLB Safeguards Rule").

[16] 15 U.S.C. § 6501 *et seq*. and Children's Online Privacy Protection Rule, 16 C.F.R. Part 312 ("COPPA Rule").

[17] Telemarketing Sales Rule, 16 C.F.R. Part 310, implementing Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. § 6101 *et seq*.

[18] CAN-SPAM Rule, 16 C.F.R. Part 316, implementing Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM") of 2003, 15 U.S.C. § 7701 *et seq*.

[19] 15 U.S.C. § 1692 *et seq*.

The FTC has brought hundreds of cases protecting the privacy and security of consumer information—both on and offline—held by companies large and small.[20] FTC enforcement actions have addressed a variety of illegal privacy and security practices, such as:

- collecting information from children online without parental consent;[21]
- deceiving consumers about collection, use, and/or disclosure of their financial, health, video, or other personal information;[22]
- making false promises about compliance with the EU-U.S. Privacy Shield (and the predecessor U.S.-EU Safe Harbor);[23]
- deceptively tracking consumers online;[24]
- disclosing highly sensitive, private consumer data to unauthorized third parties;[25]

---

[20] 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.

[21] United States v. VTech Elec. Ltd., No. 1:18-cv-114 (N.D. Ill. Jan. 8, 2018), https://www ftc.gov/system/files/documents/cases/vtech_file_stamped_stip_order_1-8-18.pdf (Stipulated Order).

[22] *See, e.g.*, PayPal, Inc., No. C-4651 (F.T.C. May 23, 2018), https://www ftc.gov/system/files/documents/cases/1623102-c4651_paypal_venmo_decision_and_order_final_5-24-18.pdf (Decision and Order); Practice Fusion, Inc., No. C-4591 (F.T.C. Aug. 15, 2016), https://www ftc.gov/system/files/documents/cases/160816practicefusiondo.pdf (Decision and Order); FTC v. Vizio, No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017), https://www ftc.gov/system/files/documents/cases/170206_vizio_stipulated_proposed_order.pdf (Stipulated Order); Snapchat, Inc., No. C-4501 (F.T.C. Dec. 23, 2014), https://www ftc.gov/system/files/documents/cases/141231snapchatdo.pdf (Decision and Order); *see generally* Fed. Trade Comm'n, Privacy and Security Cases, https://www ftc.gov/datasecurity (last visited Nov. 5, 2018).

[23] Decusoft, LLC, No. C-4630 (F.T.C. Nov. 20, 2017), https://www ftc.gov/system/files/documents/cases/1723173_c4630_decusoft_decision_and_order_11-29-17.pdf (Decision and Order); Tru, Comm., Inc., No. C-4628 (F.T.C. Nov. 20, 2017), https://www ftc.gov/system/files/documents/cases/1723171_c4628_tru_communication_decision_and_order_11-29-17.pdf (Decision and Order); Md7, LLC, No. C-4629 (F.T.C. Nov. 20, 2017), https://www ftc.gov/system/files/documents/cases/1723172_c4629_md7_decision_and_order_11-29-17.pdf (Decision and Order); ReadyTech Corp., No. 1823100 (F.T.C. July 2, 2018), https://www ftc.gov/system/files/documents/cases/1823100_readytech_corp_decision_and_order_7-2-18.pdf (Decision and Order).

[24] *See, e.g.*, Compete, Inc., No. C-4384 (F.T.C. Feb. 20, 2013), https://www ftc.gov/enforcement/cases-proceedings/102-3116/compete-inc (Decision and Order); Upromise, Inc., No. C-4351 (F.T.C. Mar. 27, 2012), https://www ftc.gov/enforcement/cases-proceedings/102-3116/upromise-inc (Decision and Order); Sears Holding Mgt. 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 (Decision and Order).

[25] *See, e.g.*, FTC v. Accusearch, Inc., 570 F.3d 1187, 1195 (10th Cir. 2009).

- publicly posting private data online without consumers' knowledge or consent;[26]
- installing spyware or other malware on consumers' computers;[27]
- failing to provide reasonable security for consumer data, including children's information;[28]
- spamming and defrauding consumers;[29]
- making harassing calls about phantom debt and leaving threatening voicemails about debt collection;[30]
- failing to comply with legal requirements when generating automated data used to deny housing to applicants;[31] and
- violating Do Not Call and other telemarketing rules.[32]

These enforcement actions send an important message: the FTC holds companies accountable for their information practices.

---

[26] *See, e.g.*, Jerk, LLC, No. 9361 (F.T.C. Apr. 2, 2014), https://www ftc.gov/system/files/documents/cases/140407jerkpart3cmpt.pdf (Complaint); Craig Brittain, No. C-4564 (F.T.C. Dec. 28, 2015), https://www.ftc.gov/system/files/documents/cases/160108craigbrittaindo.pdf (Decision and Order).

[27] *See generally*, Fed. Trade Comm'n, Spyware and Malware, https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security/spyware-and-malware (last visited Nov. 5, 2018).

[28] *See, e.g.*, Accretive Health, Inc., No. C-4432 (F.T.C. Feb. 24, 2014), https://www ftc.gov/system/files/documents/cases/140224accretivehealthdo.pdf (Decision and Order); FTC v. Neovi Inc., 604 F.3d 1150 (9th Cir. 2010); *see generally* FTC Privacy and Security Cases, *supra* note 22.

[29] *See, e.g.*, CPATank, Inc., No. 1:14-cv-01239 (N.D. Ill. Feb. 25, 2014), https://www ftc.gov/system/files/documents/cases/140228cpatankorder.pdf (Stipulated Final Judgment); FTC v. INC21.com Corp., 688 F. Supp. 2d 927 (N.D. Cal. 2010), *aff'd*, 475 Fed. Appx. 106 (9th Cir. 2012); *see generally* Fed. Trade Comm'n, Online Advertising and Marketing, https://www ftc.gov/tips-advice/business-center/advertising-and-marketing/online-advertising-and-marketing (last visited Nov. 5, 2018).

[30] FTC v. Global Processing Solutions, LLC, No. 1:17-cv-04192-MHC (N.D. Ga. July 17, 2018), https://www ftc.gov/system/files/documents/cases/advanced_mediation_group_stip_order_re_snow_redacted.pdf (Stipulated Order).

[31] RealPage, Inc., No. 3:18-cv-02737-N (N.D. Tex. Oct. 16, 2018), https://www ftc.gov/system/files/documents/cases/152_3059_realpage_inc_stipulated_order_10-16-18.pdf (Stipulated Order).

[32] *See, e.g.*, FTC. v. Christiano, No. SA CV 18-0936, (C.D. Cal. May 31, 2018) https://www ftc.gov/system/files/documents/cases/netdotsolutions_complaint.pdf (Complaint); Credit Protection Ass'n, No. 3:16-cv-01255-D (N.D. Tex. May 9, 2016), https://www ftc.gov/system/files/documents/cases/160509cpaorder.pdf (Stipulated Final Order); FTC v. E.M.A. Nationwide, Inc., 767 F.3d 611 (6th Cir. 2014).

The FTC also engages in consumer and business education to increase the impact of its enforcement actions. The FTC uses a variety of tools—such as blogging, distributing educational materials, and connecting through social media—to educate consumers and businesses on a wide range of topics. Recent topics have included information security,[33] credit freezes,[34] mobile apps and health data,[35] geolocation and children's privacy,[36] and the privacy of genetic information.[37]

Finally, the FTC has undertaken numerous policy initiatives designed to promote the privacy and security of consumer data. Workshops have delved into technology-specific topics, such as connected cars,[38] education technology,[39] drones,[40] and smart TVs.[41] The Commission has issued reports that address timely issues, such as facial recognition technology,[42] the data

---

[33] Fed. Trade Comm'n, Cybersecurity for Small Business, FTC Business Center, https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity (last visited Nov. 5, 2018); Thomas B. Pahl, Stick With Security, FTC Business Blog (Sept. 22, 2017, 11:32 AM), https://www.ftc.gov/news-events/blogs/business-blog/2017/09/stick-security-put-procedures-place-keep-your-security.

[34] Fed. Trade Comm'n, Credit Freeze FAQs, https://www.consumer ftc.gov/articles/0497-credit-freeze-faqs (last visited Nov. 5, 2018).

[35] Fed. Trade Comm'n, Mobile Health Apps Interactive Tool (Apr. 2016), https://www ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool.

[36] Press Release, Fed. Trade Comm'n, FTC Warns Gator Group, Tinitell that Online Services Might Violate COPPA, Apr. 27, 2018, https://www.ftc.gov/news-events/press-releases/2018/04/ftc-warns-gator-group-tinitell-online-services-might-violate.

[37] Lesley Fair, DNA Test Kits: Consider the Privacy Implications, FTC Consumer Information Blog, Dec. 12, 2017, ttps://www.consumer ftc.gov/blog/2017/12/dna-test-kits-consider-privacy-implications.

[38] Event Announcement, 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.

[39] Event Announcement, Student Privacy and Ed. Tech., Fed. Trade Comm'n (Dec. 1, 2017), https://www.ftc.gov/news-events/events-calendar/2017/12/student-privacy-ed-tech.

[40] Event Announcement, Fall Technology Series: Drones, Fed. Trade Comm'n (Oct. 13, 2016), https://www.ftc.gov/news-events/events-calendar/2016/10/fall-technology-series-drones.

[41] Event Announcement, Fall Technology Series: Smart TV, Fed. Trade Comm'n (Dec. 7, 2016), https://www.ftc.gov/news-events/events-calendar/2016/12/fall-technology-series-smart-tv.

[42] FED. TRADE COMM'N, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES (Oct. 2012), https://www ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

broker industry,[43] and the privacy and security implications of the Internet of Things.[44] Currently, the Commission is holding a series of Hearings on Competition and Consumer Protection in the 21st Century, which will include hearings focused specifically on privacy and data security.[45]

III. Guiding Principles

The FTC supports a balanced approach to privacy that weighs the risks of data misuse with the benefits of data to innovation and competition. Striking this balance correctly is essential to protecting consumers and promoting competition and innovation, both within the U.S. and globally. The FTC has brought cases under various statutes addressing privacy-related harms that fall into at least four categories:

- **Financial Injury:** Financial injury can manifest in a variety of ways: fraudulent charges, delayed benefits, expended time, opportunity costs, fraud, and identity theft, among other things.[46]

- **Physical Injury:** Physical injuries include risks to individuals' health or safety, including the risks of stalking and harassment.[47] Physical safety concerns also helped to drive Congress's enactment of COPPA in 1998.[48]

---

[43] FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (May 2014), https://www ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[44] *See, e.g.*, FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD (Jan. 2015), https://www ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (Staff Report); *see also* Event Announcement, Internet of Things: Privacy and Security in a Connected World, Fed. Trade Comm'n (Nov. 19, 2013), https://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world.

[45] Press Release on FTC Hearings, *supra* note 2.

[46] *See, e.g.*, TaxSlayer, LLC, No. C-4626 (F.T.C. Oct. 20, 2017), https://www ftc.gov/system/files/documents/cases/1623063_c4626_taxslayer_complaint.pdf (Complaint) (alleging delayed benefits, expended time, risk of identity theft).

[47] *See* FTC v. Accusearch, Inc., No. 06-CV-0105 (D. Wyo. May 3, 2006), https://www.ftc.gov/sites/default/files/documents/cases/2006/05/060501accusearchcomplaint.pdf (Complaint) (alleging that telephone records pretexting endangered consumers' health and safety); FTC v. EMP Media, Inc., No. 2:18-cv-00035 (D. Nev. Jan. 9, 2018) https://www ftc.gov/system/files/documents/cases/1623052_myex_complaint_1-9-18.pdf (Complaint) (alleging revenge porn website led to threats and harassment against individuals depicted).

- **Reputational Injury:** Reputational injury involves disclosure of private facts about an individual that damages the individual's reputation. Tort law recognizes reputational injury.[49] The FTC has brought cases involving this type of injury, for example, in a case involving public disclosure of individuals' Prozac use[50] and public disclosure of individuals' membership on an infidelity-promoting website.[51] Participants in the FTC's December 2017 workshop on informational injury elaborated on the reputational injury (among other harms) that can result from disclosure of private data.[52]

- **Unwanted Intrusion:** Unwanted intrusions involve two categories. The first includes activities that intrude on the sanctity of people's homes and their intimate lives. The FTC's cases involving a revenge porn website, an adult-dating website, and companies spying on people in their bedrooms through remotely-activated webcams fall into this category.[53] The second category involves unwanted commercial intrusions, such as telemarketing, spam, and harassing debt collection calls. As noted above, the FTC enforces laws addressing each of these categories of harm.

In addition to considering the risks identified above, any approach to privacy must also consider how consumer data fuels innovation and competition. The digital economy has benefitted consumers in many ways, saving individuals' time and money, creating new opportunities, and conferring broad social and environmental benefits. For example, recent innovations have enabled:

---

[48] *See* COPPA Legislative History, 105th Congress, 2nd Session, Vol. 144 (Oct. 21, 1998), https://www.congress.gov/congressional-record/1998/10/21/senate-section/article/S12741-4.

[49] Under the tort of public disclosure of private facts (or publicity given to private life), a plaintiff may recover where the defendant's conduct is highly offensive to a reasonable person. Restat. 2d of Torts, § 652D (1977).

[50] Eli Lilly and Co., No. 4047 (F.T.C. May 8, 2002), https://www ftc.gov/sites/default/files/documents/cases/2002/05/elililly do htm (Decision and Order).

[51] FTC v. Ruby Corp., No. 1:16-cv-02438 (D.D.C. Dec. 14, 2016), https://www ftc.gov/system/files/documents/cases/161214ashleymadisoncmplt1.pdf (Complaint).

[52] Transcript, Informational Injury Workshop, Fed. Trade Comm'n (Dec. 12, 2017), https://www ftc.gov/system/files/documents/public_events/1256463/informational_injury_workshop_transcript_with_index_12-2017.pdf (citing "doxing," the practice of deliberately releasing private information to encourage harassment, and relaying information about shaming, harassment, and discrimination after disclosure of individuals' HIV status); FTC INFORMATIONAL INJURY WORKSHOP: BE AND BCP STAFF PERSPECTIVE, FED. TRADE COMM'N (Oct. 2018), https://www ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf.

[53] *See* Press Release, FTC Halts Computer Spying, Fed. Trade Comm'n, Sept. 25, 2012, https://www ftc.gov/news-events/press-releases/2012/09/ftc-halts-computer-spying. *See also* Aaron's, Inc., No. C-442 (F.T.C. Mar. 10, 2014), https://www ftc.gov/system/files/documents/cases/140311aaronsdo.pdf (Decision and Order) (similar case involving similar software).

- Better predictions about and planning for severe weather events, including updated flood warnings, real-time evacuation routes, and improved emergency responses and measures, that can allow people to plan for and avoid dangerous conditions.[54]

- Improved consumer fraud detection in the financial and banking sector, as institutions can obtain insights into consumers' purchasing and behavior patterns that will allow them to proactively identify and immediately stop fraudulent transactions when they are discovered. [55]

- Free or substantially discounted services, including free communications technologies (email, VoIP, etc.), inexpensive and widely available financial products, and low-cost entertainment.

- Safer, more comfortable homes, as IoT devices detect flooding in basements, monitor energy use, identify maintenance issues, and remotely control devices such as lights and ovens.[56]

- Better health and wellness, as a variety of diagnostics, screening apps, and wearables enable richer health inputs, remote diagnosis by medical professionals, and virtual consultations.[57]

- More convenient shopping, as retail stores track both sales and inventory in real-time via shopping data to optimize product inventory in each store.[58]

---

[54] *See, e.g.*, Ali McConnon, *AI Helps Cities Predict Natural Disasters*, WALL ST. J., June 26, 2018, https://www.wsj.com/articles/ai-helps-cities-predict-natural-disasters-1530065100; *New Research Leverages Big Data to Predict Severe Weather*, SCIENCE DAILY, June 21, 2017, https://www.sciencedaily.com/releases/2017/06/170621145133.htm; Mark Puleo, *Esri Mapping, Waze Partner to Aid Emergency Responders, Residents Navigate amid Hurricane Florence*, ACCUWEATHER, Sept. 14, 2018, https://www.accuweather.com/en/weather-news/esri-mapping-waze-partner-to-aid-emergency-responders-residents-navigate-amid-hurricane-florence/70006063.

[55] *See* Mark Labbe, *Credit Card Giants Step Up AI Fraud Detection*, TECHTARGET, Sept. 20, 2018, https://searchenterpriseai.techtarget.com/news/252449044/Credit-card-giants-step-up-AI-fraud-detection; *MIT Researchers Use Machine Learning for Credit Card Fraud Detection*, INNOVATION ENTERPRISE CHANNEL, Sept. 24, 2018, https://channels.theinnovationenterprise.com/articles/mit-researchers-use-machine-learning-for-credit-card-fraud-detection.

[56] *See generally* INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD, *supra* note 44 at 8-9; *A Smarter World: How AI, The IoT And 5G Will Make All The Difference*, FORBES, Sept. 21, 2018, https://www forbes.com/sites/intelai/2018/09/21/a-smarter-world-how-ai-the-iot-and-5g-will-make-all-the-difference/.

[57] Peter H. Diamandis, *Three Huge Ways Tech Is Overhauling Healthcare*, SINGULARITY HUB, July 6, 2018, https://singularityhub.com/2018/07/06/three-huge-ways-tech-is-overhauling-healthcare/. Indeed, "[d]espite patient privacy risks that collecting health data on . . . wearable devices could pose, the number of U.S. consumers tracking their health data with wearables has more than doubled since 2013 . . . ." Fred Donovan, *Despite Patient Privacy Risks, More People Use Wearables for Health*, HEALTH IT SECURITY, Oct. 1, 2018, https://healthitsecurity.com/news/despite-patient-privacy-risks-more-people-use-wearables-for-health.

- More relevant online experiences, as retailers provide customized offers and video services recommend new shows.

- Easier-to-find parking, as cities deploy smart sensors to provide residents with real-time data about available parking spots.[59]

- Increased connectivity, as consumers can get immediate answers to questions by asking their digital voice assistants and can remotely operate devices, such as lights and door locks, with a voice command or single touch on a phone.[60]

Privacy standards that give short shrift to the benefits of data-driven practices may negatively affect innovation and competition. Moreover, regulation can unreasonably impede market entry or expansion by existing companies; the benefits of privacy regulation should be weighed against these potential costs to competition.[61]

The FTC is uniquely situated to balance consumers' interests in privacy, innovation, and competition for four reasons. First, a risk-based approach is in the FTC's institutional DNA. The FTC Act prohibits unfair or deceptive acts or practices; Congress defined "unfair" acts or practices as those in which consumer harm outweighs the benefits.[62] In other words, according

---

[58] *See* Bernard Marr, *The Brilliant Ways Kimberly-Clark Uses Big Data, IoT & Artificial Intelligence To Boost Performance*, FORBES, July 13, 2018, https://www.forbes.com/sites/bernardmarr/2018/07/13/the-brilliant-ways-kimberly-clark-uses-big-data-iot-artificial-intelligence-to-boost-performance/#23eda32c36d7.

[59] *See* Teena Maddox, *Big Data Takes a Big Leap in Kansas City with Smart Sensor Info on Parking and Traffic*, TECH REPUBLIC, Apr. 20, 2017, https://www.techrepublic.com/article/big-data-takes-a-big-leap-in-kansas-city-with-smart-sensor-info-on-parking-and-traffic/.

[60] Forbes Agency Council, *How Voice Technology Is Changing The Way We Work*, FORBES, July 27, 2018, https://www forbes.com/sites/forbesagencycouncil/2018/07/27/how-voice-technology-is-changing-the-way-we-work/#3d4894bc4a4d; Marc Zao-Sanders, *The Productivity Booster You Have in Your Pocket, But Probably Don't Use*, HARV. BUS. REV., July 19, 2018, https://hbr.org/2018/07/the-productivity-booster-you-have-in-your-pocket-but-probably-dont-use.

[61] Consider, for example, a small outdoor equipment company trying to expand its customer base. Under current law, the company can use targeted ads to reach consumers who have browsed online for hiking equipment or national park passes. Without the ability to serve these data-driven ads, it would be difficult for the company to insert itself into a market dominated by large, well-entrenched players. The resulting lack of competition could hurt consumers, giving them fewer and more expensive choices.

[62] Fed. Trade Comm'n, Commission Statement of Policy on the Scope of the Consumer Unfairness Jurisdiction, 104 F.T.C. 1070, 1071 (1984) (*appended to* Int'l Harvester Co., 104 F.T.C. 949 (1984)); Section 15 U.S.C. § 45(n) ("The Commission shall have no authority . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not

to the FTC's enabling statute, the FTC is *required* to perform a cost-benefit analysis before finding a practice is unfair.[63] Second, the FTC is the only U.S. federal agency with both competition and consumer protection jurisdiction. Thanks to this dual expertise, the FTC has a rich understanding of the benefits and costs to consumers of restricting commercial data flows. Third, the Commission has demonstrated its ability to conduct rulemaking to safeguard consumer privacy and security and provide guidance to businesses. For example, the Commission responded to the Congressional mandate to issue rules on children's and financial privacy by issuing the COPPA Rule,[64] the GLB Privacy Rule,[65] and the GLB Safeguards Rule.[66] Finally, the FTC has the institutional expertise: in addition to the litigating staff who have brought the agency's enforcement actions in privacy and data security, its Bureau of Economics has more than 75 economists who provide independent policy advice to the Commission on both competition and consumer protection matters. The Commission has used these and other tools to balance consumers' privacy interests with business' need for flexibility since the inception of its privacy program over 20 years ago.

IV. The FTC's Comments on Topics Identified in the NTIA's Request for Comment

We offer our observations in four areas: security, transparency, choice, and FTC enforcement. We note that although the RFC encompasses a wide range of social, political, and economic goals, our comments focus on discrete items related to ensuring that markets work for consumers by preventing unfair, deceptive, and anticompetitive conduct.

---

reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.").

[63] Of course, the FTC also challenges deceptive practices, which does not involve an explicit cost-benefit analysis. 15 U.S.C. § 45(a).

[64] 16 C.F.R. Part 412, *supra* note 16.

[65] 16 C.F.R. Part 313, *supra* note15.

[66] 16 C.F.R. Part 314, *supra* note 15.

A. Security

The FTC has been very active in data security, bringing over 60 cases alleging that companies did not maintain reasonable security. The FTC has taken enforcement action when it has determined that data security is inadequate or disclosures about data security are misleading.[67] The Commission has long issued calls for comprehensive data security legislation, so as to obtain additional tools.[68] The Commission is also exploring its remedial authority during the upcoming hearings relating to data privacy.[69]

B. Transparency

Transparency is another longstanding privacy tenet championed by the FTC.[70] The challenge is *how* and *when* to be transparent—how and when to provide important information about data collection and use in a way that it is accessible and meaningful to consumers.[71] The

---

[67] FED. TRADE COMM'N, PRIVACY AND DATA SECURITY UPDATE: 2017, at 4-5 (Jan. 2018), https://www ftc.gov/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives.

[68] *Id.*

[69] *See supra* note 2.

[70] *See, e.g.*, FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY (Feb. 2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf (Staff Report).

[71] Consistent with observed consumer behavior, some surveys suggest that consumers are willing to share their information with companies to personalize experiences as long as companies are transparent about their information practices. *See* John Hall, *What You Should Know About Privacy That Will Help Consumers Trust Your Brand*, FORBES, Apr. 4, 2018, https://www forbes.com/sites/johnhall/2018/04/25/what-you-should-know-about-privacy-that-will-help-consumers-trust-your-brand/#472a4bf3135a (describing research). In other surveys, respondents report a willingness to leave brands that use their personal data without their knowledge. *See* Kevin Cochrane, *To Regain Consumers' Trust, Marketers Need Transparent Data Practices*, HARV. BUS. REV., June 13, 2018, https://hbr.org/2018/06/to-regain-consumers-trust-marketers-need-transparent-data-practices (describing research showing that 79% of consumers will leave a brand if their personal data is used without their knowledge).

Although consumers report placing a high value on transparency, some empirical studies raise questions about whether consumers, in fact, want more information when making decisions. *See, e.g.*, Omri Ben-Shahar & Carl E. Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure* (Princeton Univ. Press 2014) (arguing that consumers make choices by stripping information away).

This disconnect between consumers' stated and revealed preferences is an example of the so-called "privacy paradox." *See, e.g.*, Alessandro Acquisti et al., *Privacy and Human Behavior in the Age of Information*, SCIENCE 347 (6221), 509-514 (2015) (describing privacy paradox and potential explanations).

RFC rightfully notes that the hallmarks of many current privacy policies (which are typical of efforts to respond to calls for transparency) are not salutary: many are characterized by their bloat, opacity, and legalese.[72] Despite these weaknesses, privacy policies and other disclosures do provide accountability.[73] Within an organization, drafting privacy policies helps companies understand their information practices. Outside the organization, the disclosures give interested consumers more information. They also give the press, advocacy organizations, and regulators information about the company's practices, enabling them to expose problematic practices, and helping regulators to hold companies to their promises.[74]

To retain the accountability-promoting benefits of transparency, while minimizing reliance on long, dense privacy policies, a more consumer-oriented approach would address the context, form, and effectiveness of disclosures, and be based on consumer demand for information.[75] The Commission has long been a proponent of context-specific disclosures, at the point at which consumers are making decisions about their data, which could take the form of set-up wizards, dashboards, or other in-line notices.[76] The Commission has also encouraged sector-specific model privacy notices that are clear, conspicuous, and succinct.[77] The FTC could

---

[72] RFC, *supra* note 1 at 48601.

[73] *See, e.g.*, Mike Hintze, *In Defense of the Long Privacy Statement*, 76 MD. L. REV. 1044 (2017).

[74] *Id.* at 1045 (describing how well-drafted privacy statements "create organizational accountability," inform "highly motivated individuals," and enable "those who act on behalf of consumers . . . [to] ask the hard questions . . . [,] raise public awareness and create consequences when an organization has inadequate or problematic privacy practices").

[75] *See generally* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, at i (Mar. 2012), https://www ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[76] *See, e.g.*, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD, supra note 44 at 25-26.

[77] *See, e.g.,* Final Model Privacy Form Under the Gramm-Leach-Bliley Act, 74 Fed. Reg. 62890, 62891 (Dec. 1, 2009) (setting forth the requirements of a model privacy notice). Staff continues to encourage more research about consumer demand for, understanding of, and use of this kind of disclosure. *See, e.g.*, Event Announcement, Putting Disclosures to the Test, Fed. Trade Comm'n (Sept. 15, 2016), https://www.ftc.gov/news-events/events-calendar/2016/09/putting-disclosures-test.

promote accountability under an improved disclosure regime through the exercise of its authority to challenge deceptive disclosures.

C. Control

The FTC has long encouraged a balanced approach to control. Giving consumers the ability to exercise meaningful control over the collection and use of data about them is beneficial in some cases.[78] However, certain controls can be costly to implement and may have unintended consequences. For example, if consumers were opted out of online advertisements by default (with the choice of opting in), the likely result would include the loss of advertising-funded online content.[79]

The proper approach to consumer control—one that balances costs and benefits—takes consumer preferences, context (including risk), and form into account. First, whether choice is necessary depends on the context. If the data use matches the context of the transaction or the company's relationship with the consumer, or is required or authorized by law, choice may be presumed or choice may not be necessary. For example:

- **Product and service fulfillment:** Retailers disclose consumers' contact information to delivery companies that ship their purchases. A connected thermostat collects consumers' temperature preferences to provide automated services.
- **Internal operations:** Hotels and restaurants collect customer satisfaction surveys. Websites collect click-through rates to improve site navigation.
- **Fraud prevention:** Retailers check drivers' licenses at the point of sale to prevent fraud. Online businesses scan ordinary web server logs to detect fraud. Stores use video cameras to spot theft.

---

[78] *See, e.g.*, Anita L. Allen, *Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861 (2000) (discussing longstanding conception of privacy as control over one's data).

[79] Interactive Survey of U.S. Adults, DIGITAL ADVERTISING ALLIANCE, Apr. 2013, http://www.aboutads.info/resource/image/Poll/Zogby_DAA_Poll.pdf (reporting that 92% of respondents agreed that free content is important to the value of the Internet).

- **Legal compliance and public purpose:** Search engines disclose customer data in response to legal process. A business reports a consumer's delinquent account to a credit bureau.

- **First-party marketing:** Retailers recommend products based upon consumers' prior purchases and collect data for loyalty programs.[80]

Choice also may be unnecessary when companies collect and disclose de-identified data,[81] which can power data analytics and research (potentially benefiting consumers and society), while minimizing privacy concerns. For example, consumer appliance companies can collect data about smart device usage in homes, publicize usage data in aggregate form, and encourage energy savings in households. Medical researchers can collect data from wearable devices in de-identified form to improve health outcomes for a larger patient population.

By contrast, choice is important when the risk of harm might significantly increase, such as where the data is sensitive (as in cases involving information about children, financial and health information, and Social Security numbers). Consumers should also be given a choice when a company uses the data in a manner inconsistent with its original representations. For example, the FTC brought an action against Gateway Learning, a vendor of children's educational products, when the company disclosed information about children to marketers despite the fact that the privacy policy in place at the time of the data's collection stated the

[80] Providing choices in some of these contexts may have negative effects. For example, consumers inundated by obvious or seemingly insignificant choices may become less attentive to choices that are important to them. Likewise, offering choices in some instances may undermine social benefits. Bart P. Knijnenburg, Simplifying Privacy Decisions: Towards Interactive and Adaptive Solutions, Decisions@RecSys 2013: 40-41; Sheena S. Iyengar & Mark R. Lepper, *When Choice Is Demotivating: Can One Desire Too Much of a Good Thing?*, J. OF PERSONALITY & SOC. PSYCHOL. 79, 6 (2000), 995–1006, https://faculty.washington.edu/jdb/345/345%20Articles/Iyengar%20%26%20Lepper%20(2000).pdf. For example, people who refuse to pay their bills should not be able to opt out of having that information included in credit reports, to the detriment of future creditors.

[81] A key caveat, however, is that data must be effectively de-identified, and any company that is using de-identified data should take sufficient steps to ensure that it cannot be reasonably re-identified. *See* PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, *supra* note 75 at 21.

company would not share such information.[82] Similarly, the Commission has charged companies with violations of Section 5 when they allegedly collected certain sensitive information in contravention of privacy policies or otherwise without adequate consumer notice.[83]

When offering choice, companies should consider the context in which the consumer actually makes the choice and design the choice mechanism to fit that context. For example, the FTC staff's report on the Internet of Things cites to innovative ways in which companies are offering these just-in-time choices, including through set-up wizards for devices, privacy "dashboards" or "command centers" that consumers can revisit at any time, or video or in-store tutorials that take place at the point of sale.[84] Some websites and apps have adopted similar mechanisms for providing just-in-time choices about, for example, online behavioral advertising.[85] Some platforms have developed browser-based tools for web surfing that give consumers control over collection of sensitive information (such as geolocation) on an app-by-

[82] Gateway Learning Corp., No. C-4120 (F.T.C. Sept. 10, 2004), https://www ftc.gov/sites/default/files/documents/cases/2004/09/040917do0423047.pdf (Decision and Order).

[83] *See, e.g.*, Blu Products, Inc., No. C-4657 (F.T.C. Sept. 6, 2018), https://www ftc.gov/system/files/documents/cases/172_3025_c4657_blu_decision_and_order_9-10-18.pdf (Decision and Order) (alleging that a mobile phone manufacturer collected contents of text messages and real-time location information despite having promised purchasers to limit data collection to what was needed to provide services); Goldenshores Tech., LLC, No. C-4446 (F.T.C. Mar. 31, 2014), https://www ftc.gov/system/files/documents/cases/140409goldenshoresdo.pdf (Decision and Order) (alleging that the privacy policy of the Android flashlight app developer deceptively failed to disclose that the app transmitted users' precise location and unique device identifier to third parties, including advertising networks); Designerware, LLC, No. C-4390 (F.T.C. Apr. 11, 2013), https://www ftc.gov/sites/default/files/documents/cases/2013/04/130415designerwaredo.pdf (Decision and Order) (alleging that the company designed software to collect the computer's location and created a "Detective Mode" that could log computer keystrokes, take photos of anything within the web cam's view, and capture screen shots of users' activities, all without notice to the computer user).

[84] INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD, *supra* note 44 at 25-26.

[85] *See, e.g.*, What Control Do I Have?, TRUSTARC, https://www.trustarc.com/consumer-privacy/about-oba/#&panel1-2 (last visited Nov. 5, 2018).

app basis.[86] Tools in some app settings allow users to exercise choices about the ads they receive.[87] These innovations may lead to choices that are more consistent with consumer preferences and risk.

D. FTC Enforcement

As discussed above, the FTC has used its enforcement authority vigorously to combat harms and the likelihood of harm from misuse of consumer data and failures adequately to secure sensitive information. Given the agency's leadership and expertise on privacy and security issues, the FTC should continue to be the primary enforcer of laws related to information flows in markets, whether under the existing privacy and security framework or under a new framework. If given additional authority in this area, the Commission may require resources commensurate with exercising that authority.

While the FTC has enforced Congress's risk-based approach, this approach is not without limitations. First, the Commission lacks authority over non-profits and common carrier activity,[88] even though the acts or practices of these market participants often have serious implications for data security.[89] In addition, under the FTC Act the FTC lacks civil penalty authority, reducing the Commission's deterrent capability.[90] Finally, the FTC lacks broad

---

[86] Jacob Kastrenakes, *How to Increase Your Privacy Online*, THE VERGE, June 7, 2018, https://www.theverge.com/2018/6/7/17434522/online-privacy-tools-guide-chrome-windows.

[87] *Id.*

[88] 15 U.S.C. § 45(a)(2) (exempting common carriers); *id.* § 44 (defining "corporations" covered in Section 5 to exclude non-profits).

[89] *See, e.g.*, Dan Patterson, *How Nonprofits Use Big Data to Change the World, Tech Republic*, TECH REPUBLIC, Feb. 8, 2017, https://www.techrepublic.com/article/how-nonprofits-use-big-data-to-change-the-world/ (describing importance of "big data" to non-profits' work).

[90] Prepared Statement of the Fed. Trade Comm'n, Oversight of the Federal Trade Commission, Committee on Energy and Commerce, at 6, July 18, 2018, https://www ftc.gov/system/files/documents/public_statements/1394526/p180101_ftc_testimony_re_oversight_house_07182018.pdf.

rulemaking authority under the Administrative Procedures Act ("APA")[91] for consumer protection issues such as privacy and data security.[92]

Second, the privacy and security statutes the FTC does enforce (such as COPPA and the GLB Act) have their own limitations because they are targeted to particular privacy risks. For example, COPPA provides robust protections for information collected from children online, but it does not address *offline* data or data *about* children. Third, there are limitations to existing laws when data collection does not fit neatly within statutory definitions. For example, HIPAA protects health information collected by doctors' offices, insurance companies, hospitals, and a limited set of other entities, but the law does not apply to entities such as health apps, websites, data brokers, or ad networks that collect identical data directly from consumers. Although Section 5, state statutes, and common law torts may address many of these limitations, this approach likely creates uncertainty for regulated entities and uneven levels of protection for consumers.

Concerns about the limitations of current law must be balanced against the need to preserve flexibility to address complex and evolving issues related to consumer privacy and data collection, and broader impacts on innovation and competition. As noted above, these issues are the subject of the Commission's ongoing hearings.

V. The Future of U.S. Privacy Policymaking

As we look to the future of privacy policymaking in the United States, the FTC brings an unwavering commitment to protecting consumers' privacy while promoting competition and

[91] 5 U.S.C. § 500 *et seq*.

[92] Prepared Statement of the Fed. Trade Comm'n, *supra* note 67 at 6. The Commission has been granted APA rulemaking authority for discrete topics such as children's privacy, financial data security, and certain provisions of credit reporting.

innovation. Pursuant to the existing risk-based scheme, the FTC will continue to use Section 5 to police deceptive and unfair conduct to address new consumer protection issues as they arise, as well as the specific statutes it enforces to protect consumer privacy.[93]

Where companies participate in voluntary codes of conduct, the FTC has held and will continue to hold those companies accountable for the promises they make. For example, the FTC has brought more than 45 cases against companies that failed to abide by their promises to adhere to the EU-U.S. Privacy Shield or its predecessor program.[94] Similarly, when Google allegedly did not fulfill its promises to follow the Network Advertising Initiative's Self-Regulatory Code of Conduct, the FTC filed suit.[95]

Data security concerns are an important part of the privacy debate and, in light of the issues described above, the FTC continues its longstanding call that Congress consider enacting legislation that clarifies the FTC's authority and the rules relating to data security and breach notification. The FTC also understands that both Congress and the Administration are considering federal privacy legislation, and the Commission strongly supports those efforts. Any legislation should balance consumers' legitimate concerns about the protections afforded to the collection, use, and sharing of their data with business' need for clear rules of the road, consumers' demand for data-driven products and services, and the importance of flexible frameworks that foster innovation. Should Congress decide to pursue such legislation or

---

[93] *See supra* discussion at 4.

[94] *See, e.g.*, *supra* note 23 (collecting cases); *see also* Comment Filed by Director of Bureau of Consumer Protection Jessica Rich on Privacy Enforcement Implications of FCC's Proposed Set-Top Box Rulemaking, FED. TRADE COMM'N, at 4 (Apr. 22, 2016), https://www ftc.gov/system/files/documents/advocacy_documents/comment-filed-jessica-rich-privacy-enforcement-implications-fccs-proposed-set-top-box-rulemaking/160422fccsettopltr.pdf (describing cases under the U.S.-EU Safe Harbor Framework); PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, *supra* note 75 at 14 (noting that the FTC could enforce against companies that "fail[] to abide by the self-regulatory programs they join.").

[95] United States v. Google, Inc., 5:12-cv-04177-HRL (N.D. Cal. Aug. 8, 2012) https://www ftc.gov/sites/default/files/documents/cases/2012/08/120809googlecmptexhibits.pdf (Complaint).

otherwise expand the FTC's enforcement authority, the Commission is prepared to share its expertise and assist with formulating appropriate legislation. That said, any such process will involve difficult value judgements that are appropriately left to Congress. Ultimately, no matter the specific laws Congress enacts in the privacy or data security area, the Commission commits to using its extensive expertise and experience to enforce them vigorously, consistent with its ongoing and bipartisan emphasis on privacy and security enforcement.

VI. CONCLUSION

We appreciate the opportunity to comment on ways to advance consumer privacy while fostering prosperity and innovation. The FTC continues to devote substantial resources to this important topic and looks forward to working with NTIA to encourage competition and innovation while protecting consumers.