Comments of the Consumer Federation of America

to the

Federal Trade Commission

Competition and Consumer Protection in the 21st Century Hearings,

Project No. P181201

August 20, 2018

RE: Topic 5) The Commission's remedial authority to deter unfair and deceptive conduct in privacy and data security matters.

Consumer Federation of America (CFA), an association of more than 250 nonprofit consumer organizations across the United States, welcomes the request from the Federal Trade Commission (FTC) for comments in advance of public hearings that will examine "whether broad-based changes in the economy, evolving business practices, new technologies, or international developments might require adjustments to competition and consumer protection enforcement law, enforcement priorities, and policy."[1] We have joined with the Electronic Privacy Information Center and other consumer and privacy organizations in separate comments about the intersection between privacy, big data and competition.

An important and related question is whether the FTC has adequate remedial authority to deter unfair and deceptive conduct in privacy and security matters. Our answer is that it does not. While the FTC has taken hundreds of successful actions to address privacy and security issues such as VIZIO's collection of viewing data from millions of consumers without their knowledge or consent and the failure of Uber Technologies, Inc. to reasonably secure consumers' sensitive data stored in the cloud[2] using its authority under Section 5 (a) of the FTC Act, which declares that unfair or deceptive acts or practices in or affecting commerce are unlawful,[3] this has sometimes been a struggle.

---

[1] Federal Trade Commission, *Hearings On Competition and Consumer Protection in the 21st Century*, File No. P181201, 83 Fed. Reg. 3807, (Aug. 6, 2018), https://www.ftc.gov/system/files/documents/federal_register_notices/2018/07/p181201_fr_notice_announcing_competition_and_consumer_protection_hearings.pdf.

[2] These and other examples of privacy and security-related enforcement actions last year are detailed in the Federal Trade Commission's report, *Privacy and Security Update: 2017*, available at https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf.

[3] 15 U.S.C. Sec. 45(a)(1). The agency provides "A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority" at https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

For instance, the hospitality company Wyndham Worldwide challenged the FTC's allegation that its lack of adequate security, which exposed consumers' unencrypted personal data to hackers, constituted an unfair practice. The company asserted that the FTC did not have the authority to bring the claim, violated fair notice principles because it had not promulgated regulations concerning data security, and failed to sufficiently plead its unfairness and deception claims.[4]

While the FTC ultimately prevailed in this case, it serves as an example of why the agency's ability to protect consumers' privacy and security should be strengthened. Specifically:

- The FTC should have rulemaking authority in regard to privacy and security.
- The FTC should be able to levy significant civil penalties for unfair or deceptive acts or practices and violations of its rules.
- The FTC should not be hamstrung by a requirement to show "substantial injury" to consumers which is "not reasonably avoidable" by them and "not outweighed by countervailing benefits"[5] in unfairness claims related to privacy and security.

<u>The FTC should have rulemaking authority in regard to privacy and security.</u>

Absent legislation that empowers the FTC to promulgate specific rules, the agency must go through an extremely cumbersome and time-consuming rulemaking process.[6] Therefore, many of the FTC rules that we rely on to protect consumers, such as those concerning children's online privacy[7] and telemarketing abuses,[8] have been promulgated at the direction of Congress.

These rules are issued to implement the underlying statutes, which typically set out the public policy objectives at a high level. They describe in more granular detail which entities are covered and under what circumstances, and what is expected of them. FTC rules help businesses and consumers understand their rights and responsibilities.

The FTC has not been empowered to promulgate general rules concerning the privacy and security of consumers' personal information, or even rules specifically pertaining to online privacy (other than for children). This is astounding, since privacy and security have been growing areas of concern in the United States for many years and the FTC, which has studied

---

[4] *See FTC v. Wyndham Worldwide Corp*, February 10, 2016, 129 Harv. L. Rev. 1120, available at https://harvardlawreview.org/2016/02/ftc-v-wyndham-worldwide-corp/.

[5] 15 U.S.C. § 45(n)

[6] For an enlightening perspective on the history of the FTC's rulemaking ability, see the speech by FTC Commissioner Mary L. Azcuenaga to the Society of Consumer Affairs Professionals in Business on September 12, 1985, available at https://www.ftc.gov/system/files/documents/public_statements/509781/ma91285.pdf.

[7] Children's Online Privacy Protection Rule, 16 CFR Part 312, promulgated under the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501-6505.

[8] Telemarketing Sales Rule, 16 CFR Part 310, promulgated under the Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. 6101-6108.

these issues intensively, is often touted as the premier agency for privacy and security at the federal level.

In 2009 the FTC announced that it would hold a series of roundtables "to explore the privacy challenges posed by the vast array of 21st century technology and business practices that collect and use consumer data".[9] The FTC has also hosted a number of public workshops and issued several reports.[10] Over time, the FTC recognized that self-regulation was not enough to protect consumers' privacy and security and in its seminal 2012 report, *Protecting Consumer Privacy in an Era of Rapid Change*, the FTC said Congress should "consider enacting baseline privacy legislation and reiterates its call for data security legislation."[11] No such legislation has been enacted. Meanwhile, other developed countries are leaving the United States far behind. For instance, in May 2018 the General Data Protection Regulation (GDPR)[12] went into effect in European Union member companies, providing strong privacy and security protections for consumers and strong enforcement tools for data protection authorities (DPAs).

Many good privacy and security bills have been proposed in the United States. Last year, for instance, Senator Patrick Leahy introduced the "Consumer Privacy Protection Act of 2017"[13] which would direct the FTC to promulgate regulations to implement the privacy and security requirements outlined in the legislation. CFA supports this measure. Many other privacy and security bills, such as the "Balancing the Rights of Web Surfers Equally and Responsibly Act of 2017"[14] introduced by Representative Marsha Blackburn, charge the FTC with enforcement responsibility but fail to provide it with any rulemaking authority. Ironically, Ms. Blackburn's bill was introduced after Congress repealed the Federal Communication Commission's (FCC) broadband privacy rule, an effort that she led.[15]

The FCC rule applied only to broadband service providers, which in their positions as gatekeepers to the internet can glean a tremendous amount of personal information about their customers due to their ability to see everywhere they go and everything they do online. The Blackburn bill would apply to both internet service providers and "edge providers." While edge providers can also collect a substantial amount of personal information about consumers (though not as much as internet service providers), there are some important differences,

---

[9] *See* FTC press release, September 15, 2009, available at https://www.ftc.gov/news-events/press-releases/2009/09/ftc-host-public-roundtables-address-evolving-consumer-privacy.
[10] A comprehensive list of FTC privacy reports, events, comments and testimony is available at https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/ftc-privacy-report.
[11] *See* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf at i.
[12] Information about the GDPR is available from the European Commission at https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.
[13] Available at https://www.congress.gov/bill/115th-congress/senate-bill/2124/text?format=txt.
[14] Available at https://www.congress.gov/bill/115th-congress/house-bill/2520/text?q=%7B%22search%22%3A%5B%22browser+act%22%5D%7D&r=1.
[15] H.J. Res.86, available at https://www.congress.gov/bill/115th-congress/house-bill/2520/text?q=%7B%22search%22%3A%5B%22browser+act%22%5D%7D&r=1.

including the fact that users may not have accounts with them. Among the many concerns we have about this bill, it is unclear to us how the goals of the legislation could be implemented without FTC rules specifying how the notice and other provisions of it would actually work.

Privacy and security are complex issues. They involve many different types of entities that have variety of relationships with each other and with consumers, and many different types of personal data that are collected and used for a variety of purposes. While general principles concerning privacy and security should apply across the board,[16] the FTC needs to be empowered to provide clear "rules of the road" to help businesses and consumers understand their rights and responsibilities in specific circumstances.

The FTC should be able to levy significant civil penalties for unfair or deceptive acts or practices and violations of its rules.

Many FTC investigations concerning privacy and security result in settlements containing a "consent order" in which the companies typically agree, without necessarily admitting that they have done anything wrong, to resolve the allegations. Sometimes these orders include provisions that the companies will take certain steps to improve their practices, and there may also be monitoring and reporting requirements.

The FTC can only seek civil penalties, however, in certain situations. One is when an order is violated, as illustrated last year when Upromise,[17] a membership award service, paid $500,000 in civil penalties for failing to comply with an order to clearly and prominently disclose the collection and use of data when consumers use its "RewardU" toolbar and to have third parties assess and certify that the toolbar meets certain requirements to safeguard consumers' personal information. The FTC can also ask a court to assess civil penalties when a defendant fails to respond to an adjudication against it. Furthermore, the FTC can sue for injunctive relief and consumer redress in some instances.

Importantly, the FTC can seek civil penalties when a company violates FTC rules without having to give it a "first bite of the apple" by simply agreeing do better in the future. For instance, the FTC, working with several state attorneys general, obtained $280,000 million in civil penalties from satellite TV provider Dish Network to resolve allegations that the company made 66 million sales calls to consumers in violation their do-not-call rights under the Telemarketing Sales Rule.[18]

---

[16] The Privacy Guidelines developed by the Organization for Economic Cooperation and Development are widely respected as the best principles, see http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm.

[17] Federal Trade Commission, *Privacy and Security Update: 2017*, available at https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf, at page 3.

[18] https://www.ftc.gov/news-events/blogs/business-blog/2017/06/court-orders-280-million-dish-network-largest-ever-do-not.

In cases where there is no relevant FTC rule, the agency's inability to seek civil penalties immediately when consumers are treated unfairly or deceptively diminishes its effectiveness. For example, in 2011 the FTC reached a settlement with Google to resolve charges that the company used deceptive tactics and violated its own privacy promises to consumers when it launched its social network, Google Buzz.[19] The following year, the FTC took further action when Google violated the terms of that order, resulting in the company paying $22 million in civil penalties.[20] Yet concerns about Google's privacy practices persist. Last year CFA joined several consumer and privacy organizations in a complaint to the FTC alleging that Google's YouTube online service and advertising practices are violating the Children's Online Privacy Protection Act.[21] Earlier this year, a study[22] released by the Norwegian Consumer Council shows how Google and Facebook (and to a lesser extent, Windows 10) use "default settings and dark patterns, techniques and features of interface design meant to manipulate users" into privacy intrusive options, while hiding away privacy-friendly choices. And just last week, the Associated Press released the result of an investigation showing that many Google services on Android devices and iPhones continue to store users' locations even after they have turned location tracking off.[23]

The FTC needs to be able to levy civil penalties, not just after a company has violated an agreement to resolve issues concerning unfair or deceptive acts or practices (and not only in cases involving privacy and security) but whenever the agency believes that such action is warranted. Furthermore, the amount of civil penalties must be substantial enough to encourage companies to take their obligations seriously to begin with as well as to deter repeat violations.

In Europe, the DPA's can fine companies of up to four percent of their total annual worldwide turnover or 20 million Euros, whichever is higher, for violations of the GDPR (this is not per violation; it is assessed on the basis of the gravest violation). There is no requirement that the DPAs give the companies a first bite of the apple without penalty. The fines can be lower (there is a minimum amount) and the DPAs have other options as well, such as sending a warning letter to the company, which the FTC also does in some cases. In contrast, even when the FTC can seek civil penalties, the maximum amount for unfair or deceptive acts or practices and violations of trade rules such as the Children's Online Privacy Protection Rule is $41,484 per

---

[19] *See* press release, https://www.ftc.gov/news-events/press-releases/2011/10/ftc-gives-final-approval-settlement-google-over-buzz-rollout.

[20] *See* press release, https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented

[21] In the Matter of Request to Investigate Google's YouTube Online Service and Advertising Practices for Violating the Children's Online Privacy Protection Act, available at https://consumerfed.org/wp-content/uploads/2018/04/ftc-complaint-youtube-violating-privacy-violations.pdf.

[22] *Deceived by Design*, Norwegian Consumer Council, June 27, 2018, available at https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

[23] Ryan Nakashima, "Google tracks your movements, like it or not," Associated Press, August 13, 2108, available at https://apnews.com/828aefab64d4411bac257a07c1af0ecb.

violation.[24] This is not a sufficient deterrent for companies such as Google's owner Alphabet, which made a $9.4 billion profit just in the first quarter of 2018, an 84 percent rise in profits from the last quarter of 2017.[25]

The FTC should not be hamstrung by a requirement to show "substantial injury" to consumers which is "not reasonably avoidable" by them and "not outweighed by countervailing benefits" in unfairness claims related to privacy and security.

Regardless of one's views about the position that the FTC took on interpreting its "unfairness" authority and the subsequent action by Congress in 1994 to codify that three-part test,[26] it is problematic when it comes to privacy and security. What is the injury that individuals suffer when their personal information is collected without their consent, or exposed to others whom they did not intend to provide access to it, or used for purposes other than those they expected or agreed to? Do emotional distress, anxiety, or embarrassment count as injuries? How does one measure "substantial" in those cases? Should consumers be expected not to use a product or service, or to discontinue its use, in order to avoid a privacy or security injury when their only choice is "take-it-or-leave-it" or the options for controlling their information are not clear or easy to use? How can consumers measure the countervailing benefits of getting something "free," or at a lower cost, or of a better quality in exchange for the collection and use of their data? Are there societal values that outweigh any countervailing benefits, and what are they?

Given the inherently subjective nature of privacy, these are difficult questions for the FTC to answer. Indeed, it devoted an entire public workshop in December 2017 to the subject of "informational injury".[27] The workshop came on the heels of a court decision to dismiss some of the FTC's claims in a case[28] against D-Link, which makes internet-connected cameras and routers for use in the home. The FTC alleged that the company did not take reasonable steps to secure the devices, but the court found that the agency failed to show that there was any actual consumer injury, and that the likelihood of risk was not enough.

---

[24] 2902 Federal Register, Vol. 83, No. 14, January 22, 2018, available at https://www.ftc.gov/system/files/documents/federal_register_notices/2018/01/civil_penalty_adj_published_frn_1-22-18.pdf.

[25] See Associated Press article, "Google owner Alphabet reports 84% rise in profits despite privacy concerns," August 23, 2018, available at https://www.theguardian.com/technology/2018/apr/23/google-owner-alphabet-reports-earnings.

[26] 15 U.S.C. § 45(n); for an interesting explanation of how that test came about, see Amy Gerval Dunn, *Bridging the Gap: How the Injury Requirement in FTC Enforcement Actions and Article III Standing are Merging in the Data Breach Realm*, Journal of Consumer and Commercial Law, Vol. 20, Number 1, Fall 2016, available at http://www.jtexconsumerlaw.com/V20N1/V20N1_Datarealm.pdf, page 10-11.

[27] *See* https://www.ftc.gov/news-events/events-calendar/2017/12/informational-injury-workshop.

[28] *See* Sonal Mittal Tolman and Edward Holman, "Northern District of California Drops FTC Unfairness Claim Against D-Link Systems," The WSGR Data Advisor, November 15, 2017, available at https://www.wsgrdataadvisor.com/2017/11/ndcal-ftc-d-link-systems/.

In an article[29] that appeared on the website of the International Association of Privacy Professionals prior to the FTC workshop, the authors noted that even if the court was right about what is needed to make an unfairness claim, no privacy professional would advise a client that it's OK to wait until harm has occurred to address a risk. "This disconnect between the law applicable to the security of consumer IoT devices and good security practice illustrates why IoT security will be a public policy challenge going forward, even as IoT devices proliferate," they said. They also observed that "people have a hard time deciding rationally what to do in the face of relatively remote, technically complicated risk scenarios." We agree. Putting the burden on consumers to weigh privacy and security risks and benefits is unreasonable and poor public policy.

CFA, along with other consumer and privacy groups, provided comments[30] to the FTC after the workshop in which we said that what is really needed is legislation and robust rulemaking to set the public policy parameters around the collection and use of personal information.

A more recent defeat for the FTC reinforces the argument that legislation would be helpful to dispel questions about its remedial authority in regard to unfair and deceptive conduct in privacy and data security matters. In early June of this year, the 11th U.S. Circuit Court of Appeals ruled that the FTC's cease and desist order against LabMD, a cancer screening company that experienced a breach of patient records, was unenforceable because it required the firm to meet a vague standard of reasonableness for its data security.[31]

A thoughtful paper [32]about the need for privacy legislation by Harold Feld at the nonprofit organization Public Knowledge provides a brief explanation of how privacy law and policy have evolved in the United States over the past century and the FTC's role in protecting consumers' privacy and security. Among the many salient points he makes are that consumers are unable to protect themselves without clear, enforceable rights, the market doesn't allow consumers to avoid sharing their personal information or to punish companies that don't adequately protect it, and existing laws are "poorly designed to protect consumers in the digital age."

---

[29] Christin McMeley and Chris Savage, "Consumer injury and the challenge of IoT data security," IAAP, December 12, 2017, available at https://iapp.org/news/a/consumer-injury-and-the-challenge-of-iot-data-security/.

[30] *See* comments at https://consumerfed.org/wp-content/uploads/2018/01/joint-comments-from-cfa-et-al-to-ftc-on-informational-injury-workshop.pdf.

[31] *See* Alison Frankel, "There's a big problem for the FTC lurking in the 11th Circuit's LabMD data-security ruling," Reuters, June 7, 2018, available at https://www.reuters.com/article/us-otc-labmd/theres-a-big-problem-for-the-ftc-lurking-in-11th-circuits-labmd-data-security-ruling-idUSKCN1J32S2.

[32] Harold Feld, *Principles for Privacy Legislation: Putting People Back in Control of Their Information*, Public Knowledge, December 2017, available at https://www.publicknowledge.org/assets/uploads/documents/Principles_for_Privacy_Legislation_Public_Knowledge_Paper_12.8.17.pdf.

Feld contends that the history of American privacy law provides the framework that we can use for future privacy regulation and recommends that it should be guided by four basic principles:

1. Recognize the basic principle that Americans have a fundamental right to control their personal information, and to expect that third parties will provide adequate protection for personal information.
2. Recognize that context and service matters.
3. First do not harm: Avoid preemption.
4. New federal laws must be compatible and complement existing federal privacy protections.

We agree. While the FTC is not the only federal agency that has an interest in protecting consumers' privacy and security, it has a vital role to play in that regard, and it must be empowered to promulgate rules, levy civil penalties, and take other action as appropriate (and as other agencies, such as the FCC, can do) in order to fill that role more effectively.

Furthermore, to strengthen consumers' ability to protect themselves, we believe they should have private rights of action for violations of their privacy and security and that there should be strict liability standards to hold businesses accountable.[33]

The FTC should continue to use the tools it presently has to the fullest extent it can in order to protect consumers' privacy and security. At the same time, however, the FTC should reiterate its calls for privacy and security legislation and work closely with members of Congress, consumer and privacy organizations, and far-sighted companies to gain meaningful legal reforms that will improve its ability to meet the competition and consumer protection challenges of the 21st century.

Respectfully submitted by:

Susan Grant
Director of Consumer Protection and Privacy
Consumer Federation of America
1620 I Street NW, Suite 200
Washington, DC 20006

[33] For an interesting exploration of how strict products liability could be applied to protect consumers in the Internet of Things, *see* Benjamin C. Dean, *Strict Products Liability and the Internet of Things*, Center for Democracy & Technology, April 2018, available at https://cdt.org/files/2018/04/2018-04-16-IoT-Strict-Products-Liability-FNL.pdf.