CENTER FOR DEMOCRACY & TECHNOLOGY

Aug. 20, 2018

Joseph J. Simons
Chairman

Maureen K. Ohlhausen
Commissioner

Noah Joshua Phillips
Commissioner

Rohit Chopra
Commissioner

Rebecca Kelly Slaughter
Commissioner

Re: Competition and Consumer Protection in the 21st Century

Chairman Simons and Commissioners,

The Center for Democracy & Technology (CDT) is pleased to comment on the privacy and data security authority of the Federal Trade Commission (FTC or Commission) ahead of the Commission's upcoming hearings on competition and consumer protection in the 21st century. CDT is a nonprofit technology advocacy organization dedicated to promoting public policies that preserve privacy, promote innovation, and enhance individual liberties in the digital age. The following comments address (1) how the Commission can use its Section 5 authority to address the role of design in privacy, (2) the Commission's rulemaking and enforcement under COPPA, (3) the tools and resources necessary for the Commission to effectively hold industry accountable, and (4) recommendations for developing the Commission's data security regime.

I. The Commission should use its Section 5 authority to address the role of design in privacy

A. Making privacy-by-design a reality

User control – or lack thereof – has been at the center of the U.S. privacy framework,[1] but the primacy placed on users' abilities to self-manage their own privacy ignores how design decisions and privacy

[1] Ctr. for Democracy & Tech., Comments to the FTC re: Informational Injury Workshop 3-4 (Oct. 27, 2017), https://cdt.org/files/2017/10/2017-1027-CDT-FTC-Informational-Injury-Comments.pdf; see also CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY, THE EXECUTIVE OFFICE OF THE PRESIDENT (2012).

defaults can thwart users' intentions.[2] Privacy self-management (or notice-and-choice) fails to account for the effects of user interface and product design on how individuals understand and manage their privacy.[3] Given the amount of data collecting entities and "choices" each person encounters everyday, it is unreasonable to expect individuals to be able to process the relevant information and accurately weigh the risks and benefits of each disclosure.[4] Absent comprehensive federal privacy protections, the Commission's privacy enforcement must fill this critical gap.

In order to shift the responsibility for data protection onto companies, the Commission has embraced the notion of privacy by design. Specifically, the FTC has called on companies to promote privacy throughout their organization and throughout the entire lifecycle of products and services, which includes data security, reasonable collection limits, sound retention and disposal practices, and data accuracy.[5] However, privacy by design has historically been understood as a "back-end" process governed by security engineers and legal terms. As Ira Rubinstein and Nathan Good detailed in 2013, major technology companies have long committed to embedding privacy into their development processes, but a narrow construction of privacy by design cannot account for more nuanced violations of individuals' privacy expectations and perceptions.[6] The result has been a continuous stream of privacy violations in spite of any commitment to privacy by design.

There have been several major failures of privacy by design since the FTC held its workshop on informational injuries last fall. In January, fitness data company Strava revealed sensitive information about the location and movements of military service members in conflict zones.[7] Researchers also demonstrated that Strava's privacy features could be easily circumvented to reveal the precise center

---

[2] *See, e.g.,* Mark MacCarthy, Online Manipulation is the Latest Data Protection Debate, CIO (Aug. 14, 2018), https://www.cio.com/article/3297536/e-commerce/online-manipulation-is-the-latest-data-protection-debate.html (where "consumer choice is the primary means of ensuring consumer protection . . . it turns out to be a very poor way to protect them from abuse when consumer information is collected in such a variety of ways and used for such a variety of purposes.").

[3] Daniel Solove, *Should Privacy Law Regulate Technological Design? An Interview with Woodrow Hartzog*, Teach Privacy (April 12, 2018), https://teachprivacy.com/should-privacy-law-regulate-technological-design-an-interview-with-woodrow-hartzog/.

[4] Woodrow Hartzog, Privacy's Blueprint: The Battle to Control the Design of New Technologies 143 (2018).

[5] Federal Trade Comm'n, Protecting Consumer Privacy in an Era or Rapid Change 13 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [hereinafter "FTC Privacy Report"].

[6] Ira S. Rubenstein & Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 Berkeley Tech. L.J. 1333, 1352 (2013).

[7] Liz Sly, *U.S. soldiers are Revealing Sensitive and Dangerous Information by Jogging*, Wash. Post (Jan. 29, 2018), https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html?utm_term=.a900c75b84f7.

of locations that users designated as protected "zones of privacy."[8] While Strava was applauded for offering granular privacy settings, the company ultimately acknowledged that it needed to devote engineering and user experience teams to simplifying the multiple layers of privacy settings offered by the company.[9] More recently, since the EU General Data Protection Regulation (GDPR) went into effect, the Norwegian Consumer Council critically examined the transparency and consent dialogs of Facebook, Google, and Microsoft.[10] U.S.-based Consumer Reports subsequently encouraged the Commission to investigate the coercive default settings, lack of ease of use, and framing of options presented to users.[11] Google's location privacy settings have also been subject to scrutiny. A recent Associated Press report concluded that many Google services store location data even after users turn off Google's "Location History" service, which was interpreted by many to be an overarching privacy setting.[12] These examples highlight the importance of usability and user experience to privacy protection – and their absence from existing conversations about legal compliance and engineering systems in privacy by design.[13]

While the FTC continues to embrace and recommend privacy by design, it has not done enough to elaborate on the design practices it believes are important to protect privacy. Rubinstein and Good have specifically called on regulators to convene workshops, identify best practices, and fund more research in privacy engineering and usability studies.[14] The Commission can also bring enforcement actions that address design deficiencies.

The FTC has already brought enforcement actions that touch upon problematic design decisions. For example, the FTC alleged that smart television manufacturer Vizio engaged in television tracking practices that were both deceptive and unfair. The enforcement action raised a number of important issues,[15] but considerable discussion focused on the default settings Vizio used and the methods in

[8] Rob Pegoraro, *The Strava Social Exercise App Can Reveal Your Home Address*, Yahoo Finance (Feb. 7, 2018), https://finance.yahoo.com/news/social-exercise-app-can-give-away-home-address-182247535.html.
[9] James Quarles, *A Letter to the Strava Community*, Strava Blog (Jan. 29, 2018), https://blog.strava.com/press/a-letter-to-the-strava-community/.
[10] Norwegian Consumer Council, Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Protecting Our Rights to Privacy (June 27, 2018), https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.
[11] Ltr to Maneesha Mithal, Federal Trade Comm'n, from Katie McInnis and Gabrielle Rothschild, Consumers Union (June 27, 2018), https://consumersunion.org/wp-content/uploads/2018/06/CU-to-the-FTC-Facebook-Dark-Patterns-6.27.18-1.pdf.
[12] Ryan Nakashima, *AP Exclusive: Google Tracks Your Movements, Like it or Not* (Aug. 13, 2018), https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb/AP-Exclusive:-Google-tracks-your-movements,-like-it-or-not.
[13] Rubinstein & Good, *supra* note 6, at 1408.
[14] *Id.*
[15] Joseph Jerome, *From Televisions to Telescreens: Video Viewing Habits Are Sensitive Information*, Ctr. for Democracy & Tech. (Feb. 14, 2017), https://cdt.org/blog/from-televisions-to-telescreens-video-viewing-habits-are-sensitive-information/.

which these settings were conveyed to viewers. As the Commission noted, the generic way Vizio described its practices provided limited actionable information to viewers, and the complaint against the company detailed how Vizio deployed pop-up notifications that could quickly time out and failed to provide easy access to the television's settings menu.[16]

Section 5's deception prong grants the FTC authority to act on representations *and* omissions that are false and misleading. Design decisions can clearly fall under this standard of review. The FTC's enforcement action against Google Buzz highlights the use of its "deception" authority to address misleading design. The Commission not only alleged that users' options for declining to join Google's social network were ineffective, but also that the controls for limiting the sharing of personal information were both confusing and difficult to find.[17] CDT believes the Commission can more explicitly detail via its enforcement activities the types of design and usability decisions that rise to the level of being deceptive representations and omissions.

The larger issue is whether dark design patterns can also be unfair to individuals. Manipulative and exploitative design choices are not only misleading. They also promote the surreptitious overcollection of data, raising both unwanted secondary uses and real privacy risks to individuals. "Unfairness" authority should be used to address design decisions where just-in-time notices, signals, or unclear opt-outs are insufficient to address these risks. This especially includes design that exploits users' vulnerabilities, as well as circumstances where no clear relationship exists between the consumer and the company (where the consumer is not a "user" in the traditional sense).

B. Addressing unfair design

The Commission's previous unfairness cases have often involved "practices that prey on particularly vulnerable consumers, coercive or fraudulent conduct, and significant information deficits that cause consumers to be unfairly victimized."[18] Unfair design can undermine privacy by taking advantage of consumers' vulnerabilities and interfering with their ability to weigh the benefits and risks of a transaction. When it comes to managing privacy, consumers have real cognitive limits. As Woodrow Hartzog writes, "There is simply no way for users to weight all of the available pieces of information to

[16] Fed. Trade Comm'n et al. v. VIZIO, Inc., Case 2:17-cv-00758 ¶ 21 (Feb. 06, 2017), https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf.
[17] Complaint, Federal Trade Comm'n v. Google, Docket No. c-4336 (Oct. 24, 2011), https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz.
[18] Thomas B. Leary, Fed. Trade Comm'n, Unfairness and the Internet (Apr. 13, 2000), https://www.ftc.gov/public-statements/2000/04/unfairness-and-internet.

get an accurate risk assessment for every personal disclosure they make."[19] For example, an app that asks users for the same permission over and over even after it has been declined can overwhelm and wear down a user with notice fatigue until permission is finally granted. An offer to provide customers with some benefit in exchange for access to personal data may become unfair if it is so coercive as to undermine any notice provided and interfere with consumers' ability to make a rational choice.

One area ripe for enforcement is unfair default settings. The default settings that are preselected for users in an app or piece of hardware or software are "sticky" – individuals are less likely to use their scarce cognitive resources and time to change them, particularly if the settings are complex or numerous.[20] Unfair default settings are not a concept that is foreign to the Commission. Its enforcement action against FrostWire noted that the peer-to-peer file-sharing network's default settings were configured such that they would publicly share user data immediately upon installation and use. The FTC alleged that this constituted an "unfair design" because it was "likely to cause a significant number of consumers installing and running [the software] on their mobile computing devices to unwittingly share files stored on those devices."[21]

Permissive default settings repeatedly result in unexpected secondary uses of information. Recently, payment app Venmo has faced criticism for publicly sharing users' money-sharing transactions by default. This allowed a bot to collect and Tweet out transactions that appeared to involve drugs, alcohol, or sex.[22] This comes after FTC's February 2018 settlement with Venmo over its deceptive privacy settings. The complaint alleged that the settings were confusing to change and misleading, since a user's contacts could essentially override the user's privacy settings.[23] However, the FTC did not go so far as to allege that Venmo's default settings were unfair because they were likely to expose users' financial transactions. Even if users do put the time and resources into changing their default settings, harmful disclosures can occur before the user has time to change them.

[19] Woodrow Hartzog, Privacy's Blueprint: The Battle to Control the Design of New Technologies 43 (2018).
[20] *Id.* at 53.
[21] Complaint, Federal Trade Comm'n v. Frostwire, Case 1:11-cv-23643-DLG at 13 (Oct. 7, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111011frostwirecmpt.pdf.
[22] *See* David Z. Morris, *Venmo's Privacy Settings Could Be Exposing Your Biggest Secrets*, Fortune (July 22, 2018), http://fortune.com/2018/07/22/venmo-privacy-settings-risks/.
[23] Complaint, Federal Trade Comm'n v. PayPal, 162-3102 (May 24, 2018), https://www.ftc.gov/system/files/documents/cases/1623102_c-4651_paypal_venmo_complaint_final.pdf. *See also* Natasha Duarte, *The FTC-Venmo Privacy Settlement is All About Design*, Ctr. for Democracy & Tech. (March 1, 2018), https://cdt.org/blog/the-ftc-venmo-privacy-settlement-is-all-about-design/.

A company's privacy design may also be unfair if it harms users who never had an opportunity to opt out of the objectionable data practices.[24] A company's design decisions can create risks for people other than its users or customers or that cannot be addressed through individual choice. This was the case with Strava, where the decision to visualize data through heat maps revealed secret military locations and put people at risk who never used the app and could not have objected. Similar harm can occur when third parties access social media users' personal information – notwithstanding privacy settings – by getting consent from others with whom they are connected.[25]

II. The Commission's rulemaking and enforcement under COPPA

CDT commends the FTC for using its rulemaking authority to enforce the Children's Online Privacy Protection Act (COPPA) without stifling innovation and growth in the educational technology (EdTech) sector. The Commission has an established record of enforcing COPPA and has, to date, brought 30 cases while the EdTech sector has continued to grow.[26] The Commission was proactive in updating COPPA[27] in 2013 to take into account the changing nature of the internet and the new ways data is collected.

However, the FTC must ensure that its enforcement efforts keep pace as EdTech continues to grow and data and technology evolve. CDT recommends the following actions to maximize the FTC's rulemaking authority related to COPPA:

- Continue to work with the U.S. Department of Education to provide guidance;
- Investigate companies proactively;
- Strengthen communications and outreach when FTC takes enforcement actions; and
- Provide ongoing monitoring, training, and evaluation to Safe Harbor organizations.

---

[24] *See* Leary, *supra* note 18 ("[Unfairness] cases may include harmful conduct by third parties with whom consumers have no privity, and therefore they cannot be said to involve deception in the usual sense.").

[25] *See, e.g.*, Kurt Wagner, *Here's How Facebook Allowed Cambridge Analytica to Get Data for 50 Million Users*, Recode (March 17, 2018), https://www.recode.net/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data ("Back in 2015, though, Facebook also allowed developers to collect some information on the friend networks of people who used Facebook Login. That means that while a single user may have agreed to hand over their data, developers could also access some data about their friends.").

[26] PR Newswire, Press Release, *2017 Global Edtech Investment Reaches Record $8.1 Billion* (Nov. 14, 2017), https://www.bizjournals.com/seattle/prnewswire/press_releases/Washington/2017/11/14/MN43889.

[27] 16 CFR § 312. *See also* Federal Trade Comm'n, *Revised Children's Online Privacy Protection Rule Goes Into Effect Today* (July 1, 2013), https://www.ftc.gov/news-events/press-releases/2013/07/revised-childrens-online-privacy-protection-rule-goes-effect.

A. Continue to work with the U.S. Department of Education to provide guidance

Traditionally, COPPA has only applied to operators of commercial websites, online services, and mobile apps, while schools, districts, and states are subject to the Family Educational Rights and Privacy Act (FERPA). CDT commends the FTC on conducting a joint workshop with the U.S. Department of Education to examine student privacy and EdTech.[28] It is imperative that the FTC continue to work with the U.S. Department of Education to provide guidelines and best practices for EdTech vendors and education practitioners on how COPPA applies in the school context and its relationship with FERPA.

B. Proactively investigate companies

In its first children's privacy case involving internet-connected toys, FTC settled with the electronic toy manufacturer VTech for $650,000 for collecting the personal information of hundreds of thousands of children without providing direct notice to parents or obtaining verifiable parental consent, and then failing to use reasonable and appropriate data security measures to protect personal information it collected.[29] However, this violation was only discovered after a public data breach involving the company. CDT acknowledges that the FTC has limited resources to proactively investigate companies; however, proactive investigations that provide clarity on nuanced complaints and do not rely on blatant privacy violations are essential for the FTC to keep pace with the growth in the EdTech sector.

C. Strengthen communications and outreach when FTC takes enforcement actions

The EdTech sector would benefit from the FTC being more proactive in its communication and outreach on the enforcement actions it has taken. Raising awareness around enforcement actions is important as it gives guidance about what is considered unacceptable practices and deters other companies from taking similar actions. An example of improving communications and outreach is making public by default the Safe Harbors' annual reports to the FTC, which describe all disciplinary actions taken by the Safe Harbors, so other companies are deterred from committing future violations.

D. Provide ongoing monitoring, training, and evaluation of Safe Harbors

[28] Federal Trade Comm'n, Student Privacy and Ed Tech (Dec. 1, 2017), https://www.ftc.gov/news-events/events-calendar/2017/12/student-privacy-ed-tech.
[29] Complaint, U.S. v. VTech Electronics Ltd., Case No : 1:18-cv-114 (N.D. Ill. 2018), https://www.ftc.gov/system/files/documents/cases/vtech_file_stamped_complaint_w_exs_1-8-18.pdf.

The FTC has, to date, approved seven Safe Harbor organizations,[30] which enable industry groups and other organizations to submit for Commission approval self-regulatory guidelines that implement the protections of the Commission's final rule. CDT recommends that the FTC provide ongoing monitoring, training, and evaluation to ensure these Safe Harbors are effectively enforcing COPPA and applying the same enforcement rigor entrusted to the FTC. For example, the FTC takes enforcement action on the first offense if a company violates COPPA whereas a Safe Harbor organization might permit multiple violations before taking enforcement action and referring companies to the FTC.

III. The FTC needs more tools for holding industry accountable for unfair and deceptive privacy and data security practices.

A. The FTC needs initial civil penalty authority to effectively enforce against unfair and deceptive privacy and data security practices

CDT supports the Commission's continued requests for civil penalty authority.[31] We have long recommended that any reasonable response to addressing business use of personal information requires civil penalty authority.[32] Because much of the Commission's privacy and data security enforcement falls under Section 5, which does not provide for civil penalties, companies are functionally afforded one free "bite at the apple."[33] Before a company may be fined for violating individuals' privacy, it must first agree to and be placed under a consent decree *and then* subsequently violate that agreement. Each violation of an order may then result in a civil penalty of up to $40,654.

This process has been inadequate either to protect user privacy or meaningfully punish companies for violations. The resulting penalties can be so miniscule as to ensure the penalties are simply the cost of doing business.[34] For instance, when Google agreed to pay a $22.5 million penalty for violating the terms of its consent order in 2012, this was approximately five hours worth of Google's revenue at the

[30] Federal Trade Comm'n, COPPA Safe Harbor Program, https://www.ftc.gov/safe-harbor-program.
[31] Press Release, Fed. Trade Comm'n, *FTC Testifies before House Energy and Commerce Subcommittee about Agency's Work to Protect Consumers, Promote Competition, and Maximize Resources* (July 18, 2018), https://www.ftc.gov/news-events/press-releases/2018/07/ftc-testifies-house-energy-commerce-subcommittee-about-agencys (noting that Section 5 does not provide for civil penalties, "reducing the Commission's deterrent capability" and seeking "civil penalties to effectively deter unlawful conduct").
[32] Ctr. for Democracy & Tech., Refocusing the FTC's Role in Privacy Protection (2009), https://www.cdt.org/files/privacy/20091105_ftc_priv_comments.pdf.
[33] Dissenting Statement of Commissioner J. Thomas Rosch, In the Matter of Google Inc., FTC Docket No. C-4336 (Aug. 9, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809googleroschstatement.pdf.
[34] *Id.* Commissioner Rosch noted that a $22.5 million fine "represents a *de minimis* amount of Google's profit or revenues."

time.[35] Often times no penalty is forthcoming. Facebook has been under a consent decree throughout the entire duration of its dealing with Cambridge Analytica, as well as its merger of data between its Facebook platform and WhatsApp, and it is unclear whether the FTC is actually in a position to obtain any penalties from the company.[36] More recently, Uber Technologies was forced to amend its consent order with the FTC after the company failed to disclose a consumer data breach during the Commission's investigation into the company. As Acting Chairman Ohlhausen noted, Uber first misled consumers about its privacy and security practices and then subsequently "compounded its misconduct by failing to inform the Commission that it suffered another data breach in 2016 while the Commission was investigating the company's strikingly similar 2014 breach."[37] While FTC investigations can drive business accountability, these examples do serve to highlight the potential limits of FTC enforcement without adequate fining authority.

B. Absent fining authority, consent decrees can also be improved.

In addition to increasing resultant penalties for violations of its orders, CDT recommends that the Commission strengthen its consent decree model by increasing public transparency and requiring more robust privacy assessments.

The Commission accomplishes most of its privacy and data security enforcement through settlements that place companies under consent decrees. The Commission has regularly held up its consent orders as an essential pillar of its privacy enforcement activities and their terms have been interpreted by the privacy profession writ large as creating a sort of privacy "common law."[38] Consent decrees typically impose lengthy terms of FTC oversight, require companies to implement privacy and security programs, and undergo regular independent assessments of the company's privacy and security practices.

However, there is considerable evidence that the Commission's privacy consent orders permit companies tremendous flexibility to satisfy the terms without improving privacy practices internally.

---

[35] Megha Rajagopalan, *Is $22.5 Million a Big Enough Penalty for Google?*, Business Ethics (Aug. 14, 2012), http://business-ethics.com/2012/08/14/10058-is-22-5-million-dollars-a-big-enough-penalty-for-google/.

[36] Laura Sydell, *FTC Confirms It's Investigating Facebook for Possible Privacy Violations*, NPR (March 26, 2018), https://www.npr.org/sections/thetwo-way/2018/03/26/597135373/ftc-confirms-its-investigating-facebook-for-possible-privacy-violations.

[37] Federal Trade Comm'n, Press Release, *Uber Agrees to Expanded Settlement with FTC Related to Privacy, Security Claims* (Apr. 12, 2018), https://www.ftc.gov/news-events/press-releases/2018/04/uber-agrees-expanded-settlement-ftc-related-privacy-security.

[38] *See generally, e.g.*, Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Columbia L. Rev. 583 (2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913.

FTC consent decrees, companies' responses, and privacy assessments should be made public by default. The contours and results of companies' responses to consent decrees, including independent privacy assessments, are opaque to the public and to privacy advocates. Public interest groups have had to request assessments under the Freedom of Information Act, only to receive heavily redacted documents that provide little actionable information.[39] While companies have an interest in protecting proprietary information, excessive redaction deprives the public of any meaningful ability to evaluate either the company's or the FTC's response. Additional transparency into the assessment process would help the public police corporate privacy and security practices through law, policy, and public input.[40] The FTC should also include requirements that companies explain and detail to the public how they are complying with the terms of the settlement. One recurring issue is that FTC consent orders come with no admission of wrongdoing,[41] and companies often provide no detail into whether, or how, any of their business practices will be impacted by the FTC's order.[42]

Consent decrees should also require robust independent audits rather than assessments. FTC consent orders almost universally require companies to undergo periodic independent privacy "assessments." However, these assessments are not as rigorous as a formal audit.[43] The independent assessor is, in effect, benchmarking the company's privacy and security practices against the company's own terms, and not any sort of external standard or even requirements set forth by the FTC. Audits should include rigorous tests of companies' privacy safeguards, not just assurances from the company. To maintain the integrity and impartiality of the audit, the FTC should have limited oversight over independent auditors. In addition, specific auditors should be required to personally sign each assessment done in accordance with an FTC consent decree.

IV. Data security

The FTC plays a vital role in keeping information and people secure from lax data security practices. While the Commission has a number of tools it uses to protect personal information, it has singled out its enforcement actions under Section 5 as its principal mechanism to require industry to remediate

[39] Megan Gray, Stanford Ctr. for Internet & Society, Understanding and Improving Privacy Audits Under FTC Orders at 4 (Apr. 18, 2018), http://cyberlaw.stanford.edu/blog/2018/04/understanding-improving-privacy-audits-under-ftc-orders.
[40] *Id.* at 17-18 ("It may redound to the FTC's benefit to have public review and input on assessments, especially if the agency does not have sufficient resources or expertise to evaluate whether the assessors followed applicable auditing or technical standards.").
[41] Dissenting Statement of Commissioner J. Thomas Rosch, In the Matter of Google Inc., FTC Docket No. C-4336 (Aug. 9, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809googleroschstatement.pdf.
[42] *See, e.g.,* Turn Blog, *Moving Forward* (Dec. 16, 2016), https://www.amobee.com/blog/moving-forward.
[43] See Chris Hoofnagle, *Assessing the Federal Trade Comm'n's Privacy Assessments*, 14 IEEE Security & Privacy 58 (2016), https://ieeexplore.ieee.org/document/7448350/.

data insecurity.[44] Robust enforcement is essential. The number of data breaches and security incidents continues to grow year over year. Companies do not have adequate incentives to properly invest in data security, often seeing regular data breaches and security incidents as a cost of doing business.[45]

Yet these costs have real impacts on individuals. Breaches reveal the dignitary and reputational risks that are too often dismissed in privacy debates: the Ashley Madison breach detailed information about individuals' extramarital affairs[46] while the Sony breach made people the subject of ridicule due to employee emails.[47] As the FTC has also acknowledged, the challenge with data security lapses is that while any individual harm may be small, the damage "can add up cumulatively as hundreds and perhaps thousands of organizations cause harm to people. Moreover, a small amount of harm to many people might add up to more harm collectively than a large amount of harm to a few people."[48] Furthermore, as inadequate security measures seep into new connected technologies and the Internet of Things (IoT), routers, IoT devices, and basic digital infrastructure are both vulnerable to hackers and, as seen by the Mirai botnet, weaponizable on a global scale.[49]

Since 2002, the FTC has brought over sixty enforcement actions against companies under a theory that Section 5 of the FTC Act requires industry to deploy reasonable security measures to protect information. For years, the FTC has viewed as an unfair business practice the failure to implement protections "appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities."[50] Resulting complaints and consent decrees allowed the FTC to develop de facto

[44] FTC Privacy & Security Update 2017 at 1, 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.
[45] Benjamin Dean, *Why Companies Have Little Incentive to Invest in Cybersecurity* (Mar. 4, 2015), http://www.theconversation.com/why-companies-have-little-incentive-to-invest-in-cybersecurity-37570; *see also* Sasha Romanosky, *Cost of Cyber Incidents Not Large Compared with Other Business Losses; May Influence Responses by Businesses*, Rand (Sept. 20, 2016), https://www.rand.org/news/press/2016/09/20/index1.html.
[46] *See* Kim Zetter, *Hackers Finally Post Ashley Madison Data*, Wired (Aug. 18, 2015), https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/; Laurie Segall, *Pastor Outed on Ashley Madison Commits Suicide*, CNN (Sept. 8, 2015), https://money.cnn.com/2015/09/08/technology/ashley-madison-suicide/index.html.
[47] *See* Amanda Hess, *Inside the Sony Hack*, Slate (Nov. 22, 2015), http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html.
[48] Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 Tex. L. Rev. 737, 783 (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885638.
[49] Michelle De Mooy, *#IoTFail*, Ctr. for Democracy & Tech. (Oct. 26, 2016), https://cdt.org/blog/iotfail/.
[50] Federal Trade Comm'n, Statement Marking the FTC's 50th Data Security Settlement (Jan. 31, 2014), https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

security standards and practices,[51] but this approach has received growing criticism and has been put under legal scrutiny as a result of the Eleventh Circuit's decision in support of LabMD,[52] as well as ongoing litigation involving insecure D-Link routers.[53]

Despite these legal challenges, it is clear that Section 5 grants the authority to enforce data security as an unfair act or practice.[54] The emerging issue is now what constitutes "reasonable" data security under the law and what serves as notice from the FTC to provide sufficient guidance to businesses.

Data security often has to thread the competing goals of flexibility and specificity, but recent court cases may help better delineate just how specific FTC data security requirements should be.[55] In *LabMD*, the Eleventh Circuit suggested that allowing the FTC to broadly require that companies institute comprehensive information security programs opened the door to ongoing "micromanaging" of a company's practices by the Commission,[56] and *LabMD* seems to require the FTC to now include more detailed and specific data security guidance in its consent orders.[57] If constructed properly, these more specific consent orders would not only meet legal standards set by *LabMD* but advance good security practices by more strictly enforcing practices that are widely accepted across the technology sector and endorsed by professional organizations, think tanks, government agencies, and others.

CDT believes there are two approaches the FTC can concurrently consider as it continues data security enforcement work after *LabMD*.

A. Promote Expectations for Industry Standards Setting and Security Disclosures

[51] Daniel Solove, *Did the LabMD Case Weaken the FTC's Approach to Data Security*, Teach Privacy (June 8, 2018), https://teachprivacy.com/did-labmd-case-weaken-ftc-approach-to-data-security/.
[52] LabMD, Inc. v. Fed. Trade Comm'n, Case: 16-16270 (11th Cir. June 6, 2018), http://www.media.ca11.uscourts.gov/opinions/pub/files/201616270.pdf.
[53] Mallory Locklear, *FTC Lawsuit over D-Link's Lax Router Security Just Took a Big Hit*, Engadget (Sept. 21, 2017), https://www.engadget.com/2017/09/21/ftc-lawsuit-d-link-lax-router-security-took-hit/.
[54] Two circuits have now upheld the FTC's authority to do so. In FTC v. Wyndham Worldwide Corporation, the Third Circuit held that allegations of repeated data security incidents by Wyndham did not "fall[] outside the plain meaning of 'unfair.'" FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 243 (3rd Cir. 2015). More recently, in LabMD v. FTC., the Eleventh Circuit found against the FTC but assumed that "negligent failure to implement and maintain a reasonable data-security program constituted an unfair act or practice under Section 5(a)." LabMD v. Federal Trade Comm'n, Case No. 16-16270 (11th Cir. 2018).
[55] Solove, *supra* note 51.
[56] LabMD at 30.
[57] Solove & Hartzog, *supra* note 38.

Previously, the FTC has looked at various security lapses as indicators that company data security practices were deficient as a whole. After *LabMD*, the FTC will be encouraged to point to specific problematic conduct. In the case against LabMD, this arguably might have limited the FTC to an order that only prohibited the downloading and inappropriate use of peer-to-peer file sharing without further requirements, including employee training or access controls.[58]

Moving forward, the FTC will need to look to existing industry standards as a baseline, encourage companies to be more explicit in what steps they actually take to protect information and systems, and then use the FTC's ability to police deceptive statements under Section 5 as an enforcement tool. Indeed, the Commission's recent complaint against Uber Technologies highlighted public pronouncements about the company's security practices and controls, and its amended order is narrowly focused to address specific risks related to the company's use of third-party cloud service providers and its bug bounty program.[59] Frequently, however, companies provide only boilerplate language in their privacy policies and terms of use that reference the use of "reasonable precautions" and "reasonable measures" to protect information without further detail,[60] which inappropriately limits both insight into company security practices and potential enforcement activity by the Commission.

The Commission can also point to external standards to inform its data security enforcement. For example, in its settlement with Wyndham Worldwide, the FTC built upon the Payment Card Industry Data Security Standard (PCI DSS) to require a company to undergo independent, annual PCI DSS audits in order to meet the terms of the FTC order's data security requirements.[61] A bigger project has been to incentivize adoption of the NIST Cybersecurity Framework by industry. The FTC has endeavored to align its data security enforcement with NIST's framework, and the Commission has acknowledged that it effectively serves a model for companies of all sizes to conduct risk assessments and mitigation.[62] It could also look to other models like the Federal Risk and Authorization Management Program (FedRAMP) security assessment framework or the Center for Internet Security Critical Security Controls, which the California Attorney General has stated represent "a minimum level of information

[58] LabMD at 14.
[59] Revised Agreement, Federal Trade Comm'n v. Uber Technologies, No. 1523054 (Apr. 11, 2018), https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_revised_agreement.pdf.
[60] *See, e.g.*, Six Flags, Privacy Policy, https://www.sixflags.com/america/privacy-policy#howweprotect.
[61] Lesley Fair, Federal Trade Comm'n, *Wyndham's Settlement with the FTC: What it Means for Businesses—And Consumers* (Dec. 9, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2015/12/wyndhams-settlement-ftc-what-it-means-businesses-consumers.
[62] Andrea Arias, Federal Trade Comm'n, *The NIST Cybersecurity Framewok and the FTC* (Aug. 31, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc.

security that all organizations that collect or maintain personal information should meet" and concluded that failure to implement such controls "constitutes a lack of reasonable security."[63]

State data security laws may also provide the FTC with a useful template from which to work. The New York Department of Financial Services (NYDFS) has adopted baseline, prescriptive cybersecurity requirements that apply to financial services.[64] The regulation establishes minimum standards including: (1) risk-based standards for IT systems, including encryption, access controls, and penetration testing; (2) funding and personnel requirements; (3) incident response plans; and (4) accountability mechanisms. While there are limits to the regulation's applicability to other types of businesses, it can certainly be used as a potential benchmark for any company that handles financial information, which the FTC has long designated as an especially sensitive category of data. Massachusetts follows a similar model, although it applies to all entities in the state that possess personal information.[65] That regulation includes tech-neutral requirements for a security program that include processes and decisions about access controls, user authentication, incident response, and other core elements of a reasonably secure system.

B. Aggressively Build Out Guidance Materials and Data Security "Common Law"

At issue in both *Wyndham* and *LabMD* was whether companies had sufficient notice of what constitutes reasonable security based off prior FTC activities. Critics have argued that consent orders, written guidance, and complaints affords the Commission entirely too much discretion.[66] Moreover, the Third Circuit cautioned that because consent decrees admit neither liability nor wrongdoing, they cannot be used as an authoritative statement of unfair behaviors.[67] For the FTC to continue to rely on its Section 5 unfairness authority in the case of bad data security, it will be incumbent on the Commission to issue additional guidance to put companies on notice.

The FTC has taken impressive measures to convene regular workshops, issued numerous reports, and worked with industry and other multi-stakeholder efforts to develop self-regulatory codes of conduct and best practices that address data security.[68] It has also recently announced a campaign to improve

[63] Kamala D. Harris, Calif. Dept. of Justice, California Data Breach Report (Feb. 2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.
[64] 23 NYCRR 500.
[65] 201 CMR 17.01-17.05.
[66] Berin Szóka & Geoffrey A. Manne, The Federal Trade Comm'n: Restoring Congressional Oversight of the Second National Legislature (May 2016), https://docs.house.gov/meetings/IF/IF17/20160524/104976/HHRG-114-IF17-Wstate-ManneG-20160524-SD004.pdf.
[67] Wyndham, 799 F.3d at 257 n. 22.
[68] Kenneth A. Bamberger & Deirdre K. Mulligan, Privacy on the Books & On the Ground 286 (2015).

cybersecurity practices among small businesses and non-profit organizations, emphasizing phishing, ransomware, email authentication, cloud and vendor security, among other topics.[69] These types of efforts can help the FTC set minimum expectations, but one common criticism of these activities is that they fail to generate actionable outcomes and instead produce high-level suggestions for industry to consider. Meaningful guidance is needed; for example, the FTC recently offered substantive comment on security update disclosures to the National Telecommunications and Information Administration (NTIA) that was informed by the FTC's general expertise with consumer disclosures.[70]

One concrete area where the FTC can build out a data security baseline is via its existing *Start with Security* compendium, which may provide a foundation from which the FTC can advance reasonably security safeguards over time.[71] Cybersecurity training, incident response plans, access controls, and vendor due diligence are all measures the FTC can continue to advance. Vulnerability management and patching issues are also likely to present growing challenges,[72] and the FTC should continue its interagency collaboration with the National Telecommunications and Information Administration (NTIA) on IoT vulnerability disclosure and security updates. Further, CDT has previously encouraged collaborating with the National Highway Traffic Safety Administration with respect to securing connected vehicles[73] and the Consumer Product Safety Commission on connected consumer products.[74]

Rather than creating a stagnant document, however, the evolving nature of security threats suggest that the FTC ought to periodically revisit and interrogate its own findings. CDT would suggest two ways to build out the Commission's existing *Start with Security* guidance. First, it should leverage the

[69] Federal Trade Comm'n, Press Release, *FTC to Launch Campaign to Help Small Businesses Strengthen Their Cyber Defenses* (Apr. 10, 2018), https://www.ftc.gov/news-events/press-releases/2018/04/ftc-launch-campaign-help-small-businesses-strengthen-their-cyber.

[70] Federal Trade Comm'n, Public Comment on Communicating IoT Device Security Update Capability to Improve Transparency for Consumers, in Nat'l Telecomm. & Info. Admin. Multistakeholder Process on Internet of Things Security Upgradability & Patching, https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-comment-national-telecommunications-information-administration-communicating-iot-device-security/170619ntiaiotcomment.pdf. It is worth noting that the FTC did disclaim any suggestion that its comments were "intended to provide a template for FTC law enforcement."

[71] Fed. Trade Comm'n, Start with Security (June 2015), https://www.ftc.gov/tips-advice/business-center/guidance/startsecurity-guide-business.

[72] See generally Ctr. for Democracy & Tech., Comments on the Internet of Things and Consumer Product Hazards, to the Consumer Product Safety Comm'n (June 15, 2018), https://cdt.org/files/2018/06/CDT-CPSC-IoT-Comments-061518.pdf [hereinafter "CDT IoT Comments"].

[73] Ctr. for Democracy & Tech., Comments on Federal Automated Vehicles Policy, to Nat'l Hwy. Traffic Safety Admin (Nov. 22, 2016), https://cdt.org/files/2016/11/NHTSA_FAVP_Comments_11_22_16.pdf.

[74] CDT IoT Comments, *supra* note 72.

technical expertise of the Office of Technology Research and Investigation, as well as the Commission's Section 6(b) reporting authority to collect ongoing information about industry data security practices.[75] While additional investigations by the Commission may be resource and time-intensive, they may be necessary to help the FTC clearly establish what reasonable data security baselines look like across different businesses and industry sectors.

Second, the FTC cannot be chastened against tackling emerging data security problems. *Start with Security* acknowledges that most data security cases continue to involve "basic, fundamental security missteps,"[76] but FTC enforcement activities will send a powerful message to industry regardless of whether individuals companies choose to contest what constitutes reasonable security. Cloud services and the IoT are likely to become significant drivers of data insecurity,[77] and the FTC should aggressively investigate security practices within these industries.

These investigations may not always warrant enforcement actions, and the FTC ought to use investigation closing letters as a mechanism for publicizing adequate security practices. Closing letters can be a useful guide from FTC staff as to what is not unlawful under Section 5, but the Commission has been reluctant to provide analysis of the issues or the facts of its data security investigations.[78] There are exceptions to this rule, however. The FTC's closing letter into Nest's decision to shut down Revolv's "Smart Home Hub" provides a template for how closing letters can inform the Commission's thinking on IoT,[79] and the FTC did promote its closing letter to Morgan Stanley as offering guidance to companies on insider security threats.[80]

Finally, these recommendations focus on what the FTC can do with its current authorities and the understanding that a formal rulemaking process is unlikely in the near future given heightened procedural requirements that would apply. However, given the persistence of security failures, divergent state security laws, and the convergence of best standards and practices within and across

[75] CDT is cognizant that the Commission's Section 6(b) powers may be checked by requirements imposed by the Paperwork Reduction Act, which has been repeatedly raised by former FTC staff as a significant limitation on the agency's ability to conduct empirical work on privacy and data security.
[76] FTC, Start with Security, *supra* note 71, at 1.
[77] Earl Perkins, Gartner, *Top 10 Security Predictions Through 2020*, Forbes (Aug. 18, 2016), https://www.forbes.com/sites/gartnergroup/2016/08/18/top-10-security-predictions-through-2020/#78ad84835b39.
[78] Szoka & Manne, *supra* note 66, at 41.
[79] Ltr. from Mary K. Engle, Federal Trade Comm'n, to Richard J. Lutton, Jr., Nest Labs (July 27, 2016), https://www.ftc.gov/system/files/documents/closing_letters/nid/160707nestrevolvletter.pdf.
[80] Lesley Fair, Federal Trade Comm'n, *Letter to Morgan Stanley Offers Security Insights About Insiders* (Aug. 10, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2015/08/letter-morgan-stanley-offers-security-insights-about.

technology sectors, Congress should consider whether specific and targeted APA rulemaking is appropriate.

Respectfully submitted,

Joseph Jerome, Policy Counsel
Natasha Duarte, Policy Analyst
Michelle Richardson, Director, Privacy & Data
Center for Democracy & Technology