PSYCHOGRAPHICS, PREDICTIVE ANALYTICS, ARTIFICIAL INTELLIGENCE, & BOTS: IS THE FTC KEEPING PACE?

Terrell McSweeny*

CITE AS: 2 GEO. L. TECH. REV. 514 (2018)

INTRODUCTION

Election meddling, state-sponsored disinformation campaigns, and the potential manipulation of platform users is provoking intense reactions to technology around the world.[1] The outrage following news reports that the data of millions of people were used without their knowledge to train sophisticated targeting tools that may have manipulated voters suggests that consumers expectations of how their data are collected and used do not correspond with the reality of the business models of many data-driven platforms.[2] The allegations, if true, underscore the power of increasingly sophisticated predictive technology and the limitations of the United States' largely self-regulatory approach to consumer data rights, privacy, and security. These allegations also raise the possibility that regulators,

* Terrell McSweeny was Commissioner of the Federal Trade Commission until April 2018. Prior to serving as a Commissioner, she held numerous positions in government including Chief Counsel, United States Department of Justice Antitrust Division and Deputy Assistant to President Obama and Domestic Policy Advisor to Vice President Joe Biden.

[1] *See* Giovanni Buttarelli (European Data Protection Supervisor), *EDPS Opinion On Online Manipulation and Personal Data*, EUROPA (Mar. 19, 2018), https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf [https://perma.cc/6KLZ-HWGE].

[2] *See, e.g.*, Kim Hart & Ina Fried, *Exclusive Poll: Facebook Favorability Plunges*, AXIOS (Mar. 26, 2018), https://www.axios.com/exclusive-poll-facebook-favorability-plunges-1522057235-b1fa31db-e646-4413-a273-95d3387da4f2.html [https://perma.cc/98GS-JWKT] (an axios.com poll found Facebook's favorability significantly decreased following reports of Cambridge Analytica's use of Facebook data); *see also* Chris Kahn & David Ingram, *Americans Less Likely to Trust Facebook than Rivals on Personal Data: Reuters/Ipsos Poll,* REUTERS (Mar. 25, 2018), https://www.reuters.com/article/us-usa-facebook-poll/americans-less-likely-to-trust-facebook-than-rivals-on-personal-data-reuters-ipsos-poll-idUSKBN1H10K3 [https://perma.cc/T8XN-ZT9L] (Similarly, a Reuters/Ipsos poll found sixty-three percent of respondents would like to see "less targeted advertising.").

policymakers, consumers, and even the platforms themselves[3] may be significantly underestimating the risks of data-fueled analytics and automated technology. In the last year new risks emerged including the use of technology to: manipulate perceptions and emotion; rapidly disseminate "fake news;" and deceive people through AI-driven systems that can create "deepfakes" (fake video and audio in which a person's face is substituted). Technology is also being deployed to undermine democratic processes. For example, millions of fake comments were filed with the Federal Communications Commission during its proceeding revising the Open Internet rules, and bad actors used social network platforms to engage in widespread propaganda and disinformation campaigns.[4]

The Federal Trade Commission (FTC), the nation's primary consumer data protection agency, is at the center of the debate over whether the United States' approach to consumer protection is adequate for the digital age. Under Section 5 of the FTC Act, the agency is charged with protecting consumers from unfair and deceptive acts and practices in or affecting commerce.[5] The agency also has enforcement authority related to privacy and data security under several specific statutes, including the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, the Truth in Lending Act, the CAN-SPAM Act, the Telemarketing and Consumer Fraud and Abuse Prevention Act, and the Children's Online Privacy Protection Act (COPPA).[6] The FTC's first Internet-related

---

[3] Mike Isaac, *Facebook, in Cross Hairs after Election, Is Said to Question Its Influence,* N.Y. TIMES (Nov. 12, 2016), https://www.nytimes.com/2016/11/14/technology/facebook-is-said-to-question-its-influence-in-election.html [https://perma.cc/7H39-2GQL].

[4] *See, e.g.*, Issie Lapowsky, *How Bots Broke the FCC's Public Comment System*, WIRED (Nov. 28, 2017), https://www.wired.com/story/bots-broke-fcc-public-comment-system/ [https://perma.cc/5NDG-A9U4]; *see also* Kelly Truesdale, *Can You Believe Your Eyes? Deepfakes and the Rise of AI-Generated Media,* GEO. L. TECH. REV. (Mar. 2018), https://www.georgetownlawtechreview.org/can-you-believe-your-eyes-deepfakes-and-the-rise-of-ai-generated-media/GLTR-03-2018/ [https://perma.cc/64GL-GGWC]; Molly Mckew, *How Liberals Amped Up A Parkland Shooting Conspiracy Theory,* WIRED (Feb. 27, 2018), https://www.wired.com/story/how-liberals-amped-up-a-parkland-shooting-conspiracy-theory/ [https://perma.cc/SA5E-AGFW] (The role of automation in the rapid spread of "fake news" has been documented outside of political context. This report, for example, followed the spread of the "crisis actors" narrative that was spawned following the school shooting in Parkland, Florida.).

[5] 15 U.S.C. § 45.

[6] *Statutes Enforced or Administered by the Commission*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/statutes [https://perma.cc/PT76-XKDP]. Though the subject of this essay is the FTC, it is important to note that there are other federal agencies, such as the Consumer Financial Protection Bureau and Federal Communications Commission, with relevant authorities. In addition, each state has its

consumer protection cases involved Internet-enabled fraud,[7] harmful software installed under false pretenses,[8] and, by the turn of the century, privacy.[9] Over the last two decades, as consumers moved online, the FTC evolved into the nation's chief data protection and privacy enforcement agency.[10]

The FTC has been critical in filling the gaps left by the United States' sectoral regulatory approach to consumer privacy and data security. But its incremental, harms-based approach is reactive and remains heavily rooted in the rational choice theory assumption that properly informed individuals will make reasonable decisions regarding their data. These decisions, in turn, affect demand and cause the markets to react, thereby balancing the interests of consumers with business. This essay will examine whether this framework, which depends heavily on individual consent, can keep pace with increasingly powerful targeting and technology and how the FTC must continue to evolve.

I. INCREASINGLY POWERFUL TECHNOLOGY AND THE LIMITATIONS OF THE FTC'S CONSUMER PROTECTION FRAMEWORK

The FTC's most powerful tool in shaping consumer protection is enforcement. While the agency does have some authority to regulate data practice through rule-making, such as COPPA, it primarily relies on three methods to develop law and policy around consumer protection in the digital world: studying conduct in the market, writing reports and guidance, and bringing cases through enforcement.[11] The first FTC

own version of consumer protection laws—and, in some cases, specific privacy and data laws.

[7] *See* FTC v. Corzine, CIV-S-94-1446 (E.D. Cal. filed Sept. 12, 1994) (challenging alleged misrepresentations for a credit repair kit advertised on America Online).

[8] *See* FTC v. Audiotex Connection, Inc., No. CV-97-0726 (DRH) (E.D.N.Y. filed Nov. 4, 1997), https://www.ftc.gov/sites/default/files/documents/cases/1997/11/adtxprmford.htm [https://perma.cc/9WW2-44TE] (challenging "modem hijacking" where the defendants allegedly redirected consumers' modem connections, thereby causing them to incur substantial international calling charges).

[9] *See* GeoCities, Dkt. No. C-3850 (Fed Trade Comm'n Feb. 12, 1999), https://www.ftc.gov/sites/default/files/documents/cases/1999/02/9823015cmp.htm [https://perma.cc/L7MM-BRBC] (alleging that a website misrepresented the purposes for which it was collecting personal identifying information from children and adults).

[10] Other federal consumer protection agencies, such as the Consumer Product Safety Commission, the Consumer Financial Protection Bureau, and the Federal Communications Commission, also have related authorities. Though each can and should partner with the FTC to adapt to consumer protection in the digital age, this essay is focused on the evolution of the FTC.

[11] FED TRADE COMM'N, PRIVACY & DATA SECURITY (2017), https://www.ftc.gov/reports/privacy-data-security-update-2017-overview-commissions-

workshops and privacy cases focused on the accuracy of privacy and data sharing representations in privacy policies. In these cases, the FTC relied heavily on its authority to protect consumers from deception.[12] However, as it recognized the shortcomings of relying on a model based on consumer consent to increasingly long and complex privacy policies, the modern FTC refined its approach by targeting enforcement to address reasonable consumer expectations regarding the collection, use, and protection of their data.[13] These cases included the first uses of the FTC's unfairness authority and are arguably a product of the FTC's increased focus on misuses of consumer data.[14]

Traditionally, privacy concerns focused on providing consumers with notice and choice when personal information is collected along with some explanation of how it will be used and by whom.[15] However, this

enforcement-policy-initiatives [https://perma.cc/JBR7-Q8VC] [hereinafter FTC PRIVACY & DATA SECURITY REPORT].

[12] *See, e.g.*, GeoCities, *supra* note 9; *see also* Liberty Fin. Co., Dkt. No. C-3891 (Fed. Trade Comm'n Aug. 12, 1999), https://www.ftc.gov/enforcement/cases-proceedings/982-3522/liberty-financial-companies-inc [https://perma.cc/RQ43-CC5B] (website directed to children and teens claimed that financial information collected would be anonymized when it was allegedly maintained in personally identifiable form); Nat'l Research Ctr for Coll. and Univ. Admissions et al., Dkt. No. C-4071 (Fed. Trade Comm'n Jan. 29, 2003), https://www.ftc.gov/enforcement/cases-proceedings/022-3005/national-research-center-college-university-admissions-inc [https://perma.cc/NFB5-WX58] (Survey company represented that information gathered from high school students would be shared only with colleges but also allegedly sold that information for marketing purposes.).

[13] *See Prepared Statement of the Federal Trade Commission on Discussion of Draft of H.R.__, Data Security and Breach Notification Act of 2015, Hearing Before the Subcomm. on Commerce, Manufacturing, and Trade of the H. Comm. on Energy and Commerce,* 114th Cong. (Mar. 18. 2015), https://www.ftc.gov/public-statements/2015/03/prepared-statement-federal-trade-commission-discussion-draft-hr__-data [https://perma.cc/JC7U-ZNNN].

[14] *See, e.g.*, Gateway Learning Corp., Dkt. No. 0423047 (Fed. Trade Comm'n Dec. 28, 2004), https://www.ftc.gov/enforcement/cases-proceedings/042-3047/gateway-learning-corp-matter [https://perma.cc/W82P-E32H] (alleged that retroactive material changes to privacy policy were unfair); *see also* FTC v. Integrity Sec. & Investigation Serv., Inc., No. 206-CV-241-RGD-JEB (E.D. Va. filed Oct. 6, 2006), https://www.ftc.gov/enforcement/cases-proceedings/062-3101/integrity-security-investigation-services-inc [https://perma.cc/7QZK-94HB] (alleged use of false pretenses to obtain confidential consumer phone records for sale to third parties without consumers' knowledge or consent was unfair); BJ's Wholesale Club, Inc., Dkt. No. 0423160 (Fed. Trade Comm'n Sept. 23, 2005), https://www.ftc.gov/enforcement/cases-proceedings/042-3160/bjs-wholesale-club-inc-matter [https://perma.cc/4XHS-4D7F] (company's alleged failure to employ reasonable and appropriate security measures to protect personal information was unfair).

[15] *See, e.g.*, FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), [hereinafter FTC CONSUMER PRIVACY REPORT],

framework does not address the use of personal information by third parties and data brokers who have no direct consumer-facing relationship,[16] nor does it adequately reach unanticipated uses of data as inputs for complex algorithms or by the increasingly powerful platforms that mediate most consumers' Internet experience. Recent revelations regarding the potential role that consumer data played in training sophisticated targeting tools used to manipulate voters underscores the weakness of consumers to adequately anticipate the consequences and risks of sharing data at the time they are using a service.[17] In fact, there is very little evidence that consumers understand how their data are being used to curate their online experience.[18] And they may be manipulated by the choices they are offered.[19] Moreover, there is little incentive for companies to adopt more privacy- and security-protective designs.[20] As Woodrow Hartzog points out, "The value of personal data has led most companies to adopt a 'collect first, ask questions later' mentality. This

https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/4U6B-3PRA].

[16] *See, e.g.*, FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES, (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf [https://perma.cc/HHD3-KQYR]; *see also* CHRIS HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 146 (2016) [hereinafter FTC BIG DATA REPORT].

[17] *See, e.g.*, *Cambridge Analytica CEO Claims Influence on U.S. Election, Facebook Questioned,* REUTERS (Mar. 21, 2018), https://www.reuters.com/article/us-facebook-cambridge-analytica/cambridge-analytica-ceo-claims-influence-on-u-s-election-facebook-questioned-idUSKBN1GW1SG [https://perma.cc/ZU23-MLA4]; *see also* The Editorial Board, *Facebook Leaves Its Users' Privacy Vulnerable,* N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/opinion/facebook-cambridge-analytica-privacy.html [https://perma.cc/DAA5-59LB]; Craig Timberg & Tony Romm, *U.S. and British Lawmakers Demand Answers from Facebook Chief Executive Mark Zuckerberg,* WASH. POST (Mar. 18, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/03/18/u-s-and-british-lawmakers-demand-answers-from-facebook-chief-executive-mark-zuckerberg/ [https://perma.cc/QF4A-FDWW].

[18] HOOFNAGLE, *supra* note 16, at 148.

[19] Lauren Willis, *When Nudges Fail: Slippery Defaults*, 80 UNIV. CHI. L. REV. 1155 (2013) (finding that policy defaults intended to protect individuals when firms have the motivation and means to move consumers out of the default are unlikely to be effective).

[20] HOOFNAGLE, *supra* note 16, at 147 ("But for it [privacy by design] to be successful, companies have to embrace the underlying values that privacy attempts to protect. Since these values continue to be contested, companies are likely to continue to engage in surveillance by design – the tailoring of systems in order to collect as much data as possible.").

mentality incentivizes design choices that marginalize users' interests in opacity and controls over how their data is collected and used."[21]

Against this backdrop, the FTC advocated for more consumer-oriented policies in design. But repeated failures by Congress to strengthen the agency have left it with little choice but to continue to pursue an incremental, case-by-case approach focused on protecting consumer access to correct, non-deceptive information about data collection and use.[22] For example, in August 2017, Uber Technologies, Inc., agreed to settle charges that the company falsely claimed that it strictly prohibited its own employees from accessing rider data and monitored internal access to such information.[23] Further, the FTC alleged that the company deceptively claimed that it provided reasonable security for rider and driver's personal information when it actually failed to do so; as a result of the company's failures, a file containing personal information pertaining to more than 100,000 Uber drivers was breached.[24] In some cases, the FTC has also used its deception authority to police the design of privacy settings and options. For example, in February 2018, the FTC announced a settlement resolving charges that Venmo, a peer-to-peer payment service now owned by PayPal, Inc., among other things, misled consumers about the extent to which transactions on the platform could be made private.[25] On the platform, users had to navigate multiple settings to prevent participants in their transactions from overriding their choice to make a transaction private.[26] This case builds on other deception cases

---

[21] WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 5 (2018).

[22] *See, e.g.*, United States v. InMobi Pte Ltd., No. 3:16-cv-3474 (N.D. Cal. filed June 22, 2016), https://www.ftc.gov/system/files/documents/cases/160622inmobicmpt.pdf [https://perma.cc/37JW-Y7D8] (operator of a mobile advertising network allegedly deceptively tracked the locations of hundreds of millions of consumers—including children—without their knowledge or consent to serve them geo-targeted advertising); *see also* Goldenshores Technologies, LLC., Dkt. No. 1323087, (Fed. Trade Comm'n Apr. 9, 2014), https://www.ftc.gov/system/files/documents/cases/140409goldenshorescmpt.pdf [https://perma.cc/4TD3-SR2D] (smartphone app developer allegedly deceived consumers as to how their geolocation information would be shared with advertising networks and other third parties).

[23] Uber Technologies, Inc., Dkt. No. 1523054 (Fed. Trade Comm'n Aug. 21, 2017), https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_revised_complaint_0.pdf [https://perma.cc/86A4-CW3G].

[24] *Id.*

[25] Paypal, Inc., Dkt. No. 1623102 (Fed. Trade Comm'n Mar. 5, 2018), https://www.ftc.gov/system/files/documents/cases/venmo_complaint.pdf [https://perma.cc/9MC9-CJPK].

[26] *Id.*

before it in which the FTC considered whether the design of consumer interfaces were misleading. For example, in a case involving Snapchat, the FTC alleged that consumers were misled into believing messages were ephemeral and would "disappear forever" even though they did not.[27] And, in its first Internet of Things (IoT)-related privacy case, the FTC alleged that VIZIO's "Smarty Interactivity" interface on its smart TVs did not adequately disclose that consumers' precise television viewing activities would be collected and shared with third parties.[28]

The FTC has also used its authority to protect consumers from unfair practices in the privacy and security context, though it has used that authority more sparingly. The FTC's first unfairness privacy case was a case in which the company, Gateway, allegedly retroactively changed its privacy policy. Consumers were only offered an opt-out when their data gathered under one set of terms (a promise not to sell it to third parties) was sold to third parties.[29] The FTC made similar allegations against Facebook in a subsequent case,[30] underscoring that a company cannot collect information for a particular stated purpose and unilaterally decide later to use it for a broader purpose without first obtaining affirmative consumer consent. In the privacy and data security context, the FTC has alleged unfairness in the following situations: collecting and using information obtained through a client's website in knowing violation of that client's privacy policy;[31] selling confidential phone records without consent;[32] designing software causing consumers to unwittingly share files

[27] Snapchat, Inc., Dkt. No. C-4501 (Fed Trade Comm'n Dec. 23, 2014) https://www.ftc.gov/system/files/documents/cases/141231snapchatcmpt.pdf [https://perma.cc/K9JV-JTJT].

[28] FTC v. VIZIO, Inc. et al., No. 2:17-cv-00758 (D.N.J filed Feb 3, 2017) https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf [https://perma.cc/923L-DHPP] ("Defendants failed to adequately disclose that the "Smart Interactivity" feature comprehensively collected and shared consumers' television viewing activity from cable boxes, DVRs, streaming devices, and airwaves, which Defendants then provided on a household-by-household to third parties.").

[29] Gateway Learning Corp., *supra* note 14.

[30] Facebook, Inc., Dkt. No. 0923184 (Fed. Trade Comm'n Aug. 10, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf [https://perma.cc/SZ7K-3L9U].

[31] *See* Vision I Properties, LLC, Dkt. No. 0423068 (Fed. Trade Comm'n Apr. 26, 2005), https://www.ftc.gov/sites/default/files/documents/cases/2005/04/050426comp0423068.pdf [https://perma.cc/9TCR-DTLM].

[32] *See, e.g.*, Accusearch, Inc., No. 06-CV-0105 (D. Wyo. filed June 29, 2009), https://www.ftc.gov/sites/default/files/documents/cases/2006/05/060501accusearchcomplaint.pdf [https://perma.cc/A32H-8B9Y].

publicly;[33] defeating asserted privacy choices by consumers;[34] installing spyware or man-in-the-middle software without notification or consent;[35] selling information to businesses using it for fraud;[36] unfair tracking (collecting and sharing sensitive data without consumers' consent);[37] revenge porn;[38] and failure to maintain reasonable security practices.[39]

---

[33] *See* FTC v. Frostwire LLC., No. 111-cv-23643 (S.D. Fla. filed Oct. 12, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111011frostwirecmpt.pdf [https://perma.cc/D2ZN-DE8T].

[34] *See* United States v. InMobi Pte Ltd., No. 3:16-cv-3474 (N.D. Cal. filed June 22, 2016), https://www.ftc.gov/system/files/documents/cases/160622inmobicmpt.pdf [https://perma.cc/KG6D-AUZA].

[35] *See, e.g.*, Compl., DesignerWare, LLC, et al., Dkt. C-4390 (Fed. Trade Comm'n Apr. 15, 2013), http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415designerwarecmpt.pdf [https://perma.cc/H5WM-2UWY]; *FTC Approves Final Order Settling Charges Against Software and Rent-to-Own Companies Accused of Computer Spying*, FED. TRADE COMM'N (Apr. 15, 2013), https://www.ftc.gov/news-events/press-releases/2013/04/ftc-approves-final-order-settling-charges-against-software-and [https://perma.cc/J697-NVJS] (announcing seven cases against rent-to-own companies that allegedly spied on consumers through rental laptops); Lenovo, Inc., Dkt. No. 1523134 (Fed. Trade Comm'n Jan. 2, 2018), https://www.ftc.gov/system/files/documents/cases/1523134_c4636_lenovo_united_states_complaint.pdf [https://perma.cc/8XWT-Y35B].

[36] *See, e.g.*, FTC v. Action Research Group, Inc., No. 607-CV-0227-ORL-22JGG (M.D. Fla. filed May 28, 2008), https://www.ftc.gov/sites/default/files/documents/cases/2007/02/070214actionresearchgrpcmplt.pdf [https://perma.cc/CU5G-WVZ3]; *see also* FTC v. Integrity Sec. & Investigation Serv., Inc., No. 206-CV-241-RGD-JEB (E.D. Va. filed Oct. 6, 2006), https://www.ftc.gov/enforcement/cases-proceedings/062-3101/integrity-security-investigation-services-inc [https://perma.cc/8QQY-5XXZ]; FTC v. Sitesearch Corp. (LeapLab), No. CV-14-02750-PHX-NVW (D. Ariz. filed on Feb. 18, 2016), https://www.ftc.gov/system/files/documents/cases/141223leaplabcmpt.pdf [https://perma.cc/H3VB-AV6J].

[37] *See* Goldenshores, *supra* note 22; *see also* FTC v. VIZIO, Inc. et al., No. 2:17-cv-00758 (D.N.J filed Feb. 3, 2017), https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf [https://perma.cc/M9C9-CK67].

[38] *See, e.g.*, Craig Britton, Dkt. No. 1323120 (Fed. Trade Comm'n Jan. 8, 2016), https://www.ftc.gov/system/files/documents/cases/160108craigbrittaincmpt.pdf [https://perma.cc/DV86-7SS6]; *see also* FTC v. Emp. Media Inc. (MyEx.com), No. 2:18-cv-00035 (D. Nev. filed Jan. 10, 2018), https://www.ftc.gov/system/files/documents/cases/1623052_myex_complaint_1-9-18.pdf [https://perma.cc/2CEM-7DQY].

[39] *See, e.g.*, Compl., FTC v. Wyndam Worldwide Corp., No. 2:13-CV-01887-ES-JAD (D.N.J. filed June 26, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/06/120626wyndamhotelscmpt.pdf [https://perma.cc/PUJ8-UDST].

The FTC has pursued approximately 40 privacy and security cases in the last decade using its unfairness authority—the majority involving unreasonable data security practices.[40] However, a close examination of these cases reveals that the FTC uses its unfairness authority cautiously in data privacy and security cases. While FTC enforcement can help police the most pernicious and deceptive practices in the marketplace, the agency must develop a clear theory of substantial likelihood of harm to consumers that is not outweighed by any countervailing benefits when using its unfairness authority.[41] The harm requirement imposes some limitations around how far the FTC can pursue aggressive uses of sensitive data.[42] Harms—particularly data harms—are "often remote, diffuse, risk oriented, or difficult to ascertain."[43] As Chris Hoofnagle explains, "So far, the thin edge of the unfairness wedge has been used to police noxious problems such as cyber exploitation, also termed revenge pornography, and spyware."[44] For the most part, the FTC continues to rely primarily on its deception authority when policing consumer privacy and the use of consumer data.

The FTC itself has noted that, especially in light of consumers' ever-expanding connectedness, consumers need additional protections. The agency has repeatedly called for baseline privacy and data security legislation that would be flexible and technology-neutral but would also require breach notification and provide clear rules of the road for companies regarding when they must provide privacy notices to consumers and offer choices about data collection and use.[45]

---

[40] FED. TRADE COMM'N, PRIVACY & DATA SECURITY (2017), 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 [https://perma.cc/WTQ3-G3E3].

[41] *FTC Policy Statement on Unfairness*, appended to *International Harvester Co*., 104 F.T.C. 949, 1070 (1984), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness [https://perma.cc/D5JJ-NHPM]; *see also* 15 U.S.C. § 45(n).

[42] Concurring Statement of Acting Chairman Maureen Ohlhausen In the Matter of VIZIO, Inc., https://www.ftc.gov/public-statements/2017/02/concurring-statement-acting-chairman-maureen-k-ohlhausen-matter-vizio-inc [https://perma.cc/5E5L-4X4S] ("But, under our statute, we cannot find a practice unfair based primarily on public policy…This case demonstrates the need for the FTC to examine more rigorously what constitutes 'substantial injury' in the context of information about consumers.").

[43] HARTZOG, *supra* note 21, at 71.

[44] HOOFNAGLE, *supra* note 16, at 347.

[45] *See* FED. TRADE COMM'N, THE INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD 49–51 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/7V43-98JN] [hereinafter FTC INTERNET OF THINGS REPORT]; *see also* FTC CONSUMER PRIVACY REPORT, *supra* note 15.

In its 2014 report on data brokers, the FTC highlighted the complex ecosystem of data broker firms, which not only collect data from numerous sources—largely without consumers' knowledge—but also provides data to each other and make inferences about consumers. The e-data they collect includes sensitive categories pertaining to income level, ethnicity, or health conditions.[46] The FTC enforces the Fair Credit Report Act ("FCRA"), which covers the use of consumer data for decisions about credit, employment, housing, and similar eligibility determinations.[47] But the FCRA "generally does not cover the sale of consumer data for marketing and other purposes."[48] The FTC identified potential risks to consumers from some of the uses of consumer data and profiles by data brokers. For example, the report noted that storing massive amounts of data may expose consumers to security risks if that information is breached and that risk mitigation and scoring products, *i.e.*, products used to verify consumers' identities or detect fraud, may be used to deny consumers the ability to complete a transaction.[49] To address that gap, the FTC recommended Congress enact legislation that would require data brokers selling marketing products to give consumers access to their data at a reasonable level of detail and to provide the ability to opt out of having it shared for marketing purposes.[50] The agency further recommended that Congress enact transparency obligations on data brokers who sell risk-mitigation products and impose requirements on data brokers selling people search products that would allow consumers to access and suppress their information.[51]

The FTC's 2016 report on Big Data examined the benefits and risks of big data analytics, among them the potential to harm consumers, including underserved and low-income populations.[52] The report discussed several laws that could be potentially applicable to the use of big data—including not just the FTC Act but also the FCRA, equal opportunity laws such as the Equal Credit Opportunity Act and Fair Housing Act, and civil rights laws. However, the report noted that determining which law(s)

---

[46] FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY at i (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/Q8V6-MR68] [hereinafter FTC DATA BROKER REPORT].

[47] *See* 15 U.S.C. §§ 1681–1681x (2014).

[48] FTC DATA BROKER REPORT, *supra* note 46, at i.

[49] *See id.* at 32, 48–49.

[50] *Id.* at 50.

[51] *See* FTC CONSUMER PRIVACY REPORT, *supra* note 15, at 14.

[52] FTC BIG DATA REPORT, *supra* note 16, at i.

might apply is a fact-specific determination and highlighted the potential for gaps in the enforcement regime.

Congress has shown its willingness to provide the FTC with additional enforcement authority to cabin harmful uses of automated technology or unreasonable limitations on users. Namely, Congress gave the FTC the responsibility to enforce the Consumer Review Fairness Act[53] and the Better Online Ticket Sales ("BOTS") Act,[54] both of which were enacted in late 2016. These laws ban the use of contract provisions that prohibit or penalize consumers who provide honest reviews, and the use of ticket-buying "bots," respectively.

The FTC's enforcement actions are an important basis for the privacy best practices the FTC has endorsed, including: privacy by design, where firms promote consumer privacy throughout their organizations and at every stage of the development of their products and services;[55] security by design;[56] transparency and choice;[57] data minimization;[58] and enhanced protection for sensitive data.[59]

But in the data-driven digital economy, the incentive to gather as much data as possible is powerful and often conflicts with these best practices. As Woodrow Hartzog explains, "data is fuel for industry . . . . Manipulative and leaky design can net companies more data. Add to the mix the fact that pernicious design is difficult for people to recognize—it is often opaque and sometimes completely invisible. This is a recipe for exploitation."[60]

---

[53] Consumer Review Fairness Act of 2016, Pub. L. No. 114–258, 130 Stat. 1355 (2016).
[54] Better Online Ticket Sales Act of 2016, Pub. L. No. 114–274, 130 Stat. 1401 (2016).
[55] FTC CONSUMER PRIVACY REPORT, *supra* note 15, at 22–32.
[56] *See, e.g.*, FTC INTERNET OF THINGS REPORT, *supra* note 45, at 28.
[57] *See* FED. TRADE COMM'N, CROSS-DEVICE TRACKING 11–15 (2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf [https://perma.cc/4ZP3-ZYDR] [hereinafter FTC CROSS-DEVICE TRACKING REPORT]; *see also* FTC CONSUMER PRIVACY REPORT, *supra* note 15; FTC INTERNET OF THINGS REPORT, *supra* note 45.
[58] *See, e.g.*, FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [https://perma.cc/W9SR-XSCX] [hereinafter FTC START WITH SECURITY GUIDE]; *see also* FTC CONSUMER PRIVACY REPORT, *supra* note 15; FTC CROSS-DEVICE TRACKING REPORT, *supra* note 57; FTC INTERNET OF THINGS REPORT, *supra* note 45.
[59] *See, e.g.*, FTC CROSS-DEVICE TRACKING REPORT, *supra* note 57, at 15; *see also* FTC START WITH SECURITY GUIDE, *supra* note 58.
[60] HARTZOG, *supra* note 21, at 74.

II. FTC 2.0: CONSUMER PROTECTION FOR THE DIGITAL AGE

The growing power of the technology we are all using in our daily lives—which now includes many more connected and increasingly autonomous things—raises the question of whether consumer protection agencies like the FTC can adapt quickly enough to keep pace with it. As discussed above, the FTC's data protection framework continues to rely heavily on its deception authority and, therefore, the principle that sufficient transparency enables consumers to make informed choices about when to share their data. The idea that privacy controls such as notice and choice are adequate to protect consumers in the current environment has been described as quaint.[61] The FTC has used its unfairness authority to police some data practices, though cautiously and incrementally. Technology is becoming both more powerful and more ingrained in all aspects of our life. Adequately protecting consumers requires a more proactive approach.

One solution is for the FTC to use its unfairness authority more aggressively, and perhaps even its Magnuson-Moss rulemaking authority, to push industry norms toward the best practices that the FTC itself articulates. But this may be easier said than done. Although FTC has used its unfairness authority relatively cautiously, it is constantly called on to defend its use of the authority when it does use it. The FTC won a critical case protecting the use of its unfairness authority in data security cases in *Wyndham*, but the agency's authority has continued to be the subject of litigation in *D-Link* and *LabMD*.[62] In a recent ruling in the LabMD case the 11th Circuit did not directly address the scope of the FTC's unfairness authority – but nevertheless vacated the FTC's order.[63] In a somewhat unusual move, the court ruled on the appropriateness of the relief sought by the FTC even though the central dispute in the case was over the FTC's

---

[61] HOOFNAGLE, *supra* note 16, at 333 ("Our regulatory regime, premised on quaint ideas of privacy control and sectoral privacy rules, is simply inadequate to address the kinds of decision making and inferential powers that information-intensive industries now possess.").

[62] FTC v. D-Link, No. 3:17-cv-00039 (N.D. Cal. filed Jan. 5, 2017), https://www.ftc.gov/system/files/documents/cases/d-link_complaint_for_permanent_injunction_and_other_equitable_relief_unredacted_version_seal_lifted_-_3-20-17.pdf [https://perma.cc/3JGF-286M]; *see also* FTC v. Wyndham Worldwide Corp., No. 2:13-CV-01887-ES-JAD (D.N.J. Dec. 11, 2015), https://www.ftc.gov/system/files/documents/cases/150824wyndhamopinion.pdf [https://perma.cc/YC38-YRSY]; LabMD, Inc., Dkt. No 9357 (Fed. Trade Comm'n Sept. 29, 2016), https://www.ftc.gov/system/files/documents/cases/d09351labmdappealorder_0.pdf [https://perma.cc/4D7C-CHE7].

[63] LabMD v. FTC, 2018 WL 3056794 *1 (11th Cir. June 6, 2018).

use of its unfairness authority. The court concluded that the FTC's order requiring LabMD to implement a reasonable security program was not sufficiently specific.[64] The implications of this decision on future FTC data security cases and efforts by the FTC to enforce existing orders are unclear, but it is likely the decision will result in new challenges to the FTC's authority, particularly in data security cases. In addition, the agency has, historically, run into significant resistance from industry and Congress when it is perceived as pushing the bounds of its authority to expand enforcement efforts innovatively. For example, when the agency attempted to regulate the advertising of sugary foods to children in the late 1970s—actions that resulted in advertisers, broadcasters, and the food industry aligning against the FTC, and in the Washington Post labeling the agency the "National Nanny"[65]—Congress stepped in to limit the Commission's authority. The hangover from the so-called "Kidvid" controversy remains a reminder to the FTC today that pushing too aggressively can result in painful consequences.

Others have called for the FTC to use its antitrust authorities more aggressively to limit the power of technology platforms. In the wake of the Facebook-Cambridge Analytica scandal, some even called for Facebook and other technology platforms to be broken up.[66] The FTC should use its competition authority to police dominant platforms aggressively and competition within technology markets, but competition alone is unlikely to discipline harmful data practices. First, not all firms that may engage in harmful data practices will necessarily be large players with market power. Second, absent action on more comprehensive data rights, it is challenging for consumers to differentiate between products based on data policies or withdraw their data from them. Third, the incentives in the marketplace will remain powerful to collect and monetize as much data as possible.[67]

---

[64] *Id.* at *11. ("In the case at hand, the cease-and-desist order contains no prohibitions. It does not instruct LabMD to stop committing a specific act or practice. Rather, it commands LabMD to overhaul and replace its data-security program to meet an indeterminable standard of reasonableness. This command is unenforceable.").

[65] *The FTC as National Nanny*, WASH. POST (Mar. 1, 1978), https://www.washingtonpost.com/archive/politics/1978/03/01/the-ftc-as-national-nanny/69f778f5-8407-4df0-b0e9-7f1f8e826b3b/ [https://perma.cc/9MZX-8G7D].

[66] Siva Vaidhyanathan, Opinion, *Don't Delete Facebook. Do Something About It*, N.Y. TIMES (Mar. 18, 2018), https://www.nytimes.com/2018/03/24/opinion/sunday/delete-facebook-does-not-fix-problem.html [https://perma.cc/HM3S-9HCV].

[67] *See, e.g.*, Allie Bohm, *Here's How Congress Should Respond to Facebook/Cambridge Analytica,* PUB. KNOWLEDGE (Mar. 23, 2018), https://www.publicknowledge.org/news-blog/blogs/heres-how-congress-should-respond-to-facebook-cambridge-analytica [https://perma.cc/9KGJ-X8S9].

The information asymmetry between consumers and the companies collecting and using their data also affects how well competition will work to rebalance the amount of risk consumers bear in sharing their data in the first place. So, the FTC should also advocate for pro-competitive data policies like giving consumers more control over their data. Absent meaningful data portability and interoperability, the power asymmetries between institutions that accumulate data and the people who generate the data are likely to persist.[68] Of course, even with these rights, the asymmetries may even be irreversible since people cannot effectively trade within a system they do not understand. Reforms, including comprehensive data and privacy laws, transparency and accountability for data brokers, and transparency around online political ads and spending, are also necessary.

The FTC can and should continue to build the record for the enactment of meaningful consumer protections for the digital age. In the last five years, it has issued a series of reports identifying troubling practices in the marketplace and, in many cases, accurately predicted harm scenarios before they occurred.[69] For example, in its report on the Internet of Things, the FTC predicted that insecure IoT could be used to attack other systems.[70] At its annual PrivacyCon, the FTC presents cutting edge research on how technology is performing.[71] Its newly formed Office of

---

[68] Robert Seamans, *Data Portability and Competition Between Platforms,* FORBES (Mar. 6, 2018), https://www.forbes.com/sites/washingtonbytes/2018/03/06/data-portability-and-competition-between-technology-platforms/#cc539f0b5bb5 [https://perma.cc/22GZ-SKGJ]; Samuel Himel & Robert Seamans, *Artificial Intelligence, Incentives to Innovate, and Competition Policy,* COMPETITION POL'Y INT'L (Dec. 19, 2017), https://www.competitionpolicyinternational.com/artificial-intelligence-incentives-to-innovate-and-competition-policy/ [https://perma.cc/8V9K-4KFG]; *see also* Alexander Macgillivray, *Summary of Comments Received Regarding Data Portability*, OBAMA WHITE HOUSE BLOG (Jan. 10, 2017, 9:19 AM), https://obamawhitehouse.archives.gov/blog/2017/01/10/summary-comments-received-regarding-data-portability [https://perma.cc/NK7Q-D6J4].

[69] *See* FTC DATA BROKER REPORT, *supra* note 46; *see also* FTC BIG DATA REPORT, *supra* note 16; FTC CROSS-DEVICE TRACKING REPORT, *supra* note 57.

[70] *See* FTC INTERNET OF THINGS REPORT, *supra* note 45, at 11–12 ("Second, security vulnerabilities in a particular device may facilitate attacks on the consumer's network to which it is connected, or enable attacks on other systems. For example, a compromised IoT device could be used to launch a denial of service attack.").

[71] Fed. Trade Comm'n, Press Release, FTC Releases Agenda for PrivacyCon 2018 (Feb. 6, 2018), https://www.ftc.gov/news-events/press-releases/2018/02/ftc-releases-agenda-privacycon- [https://perma.cc/V8VL-BBR2]; *see also* Press Release, Fed. Trade Comm'n, FTC Announces Agenda for PrivacyCon 2017 (Dec. 16, 2016), https://www.ftc.gov/news-events/press-releases/2016/12/ftc-announces-agenda-privacycon-2017 [https://perma.cc/7AMR-NQ2B]; Press Release, Fed. Trade Comm'n, FTC Releases Agenda for PrivacyCon (Dec. 29, 2015), https://www.ftc.gov/news-

Technology, Research, and Investigations—or OTech—has also hosted workshops and presented its own original research, [72] and the office helps support FTC enforcement and investigations.[73]

Even if the FTC's recommendations have not been heeded by lawmakers, the Commission should continue to study the effect of the latest targeting technology—such as custom audience tools and psychographics—to better scope their potential risks and to inform its enforcement. Considerations for the agency include whether advanced targeting technologies and tools that are neutral on their face are, in fact, having disparate impacts in violation of civil rights and equal opportunity laws and whether some of the tools are so manipulative that disclosures are ineffective. For example, not much is known about whether and how psychographic targeting powered by massive amounts of data and automated technology works.[74] It has variously been described as both "powerful enough to influence elections" and "an imprecise science at best and snake oil at worst."[75] The FTC studied the current state of big data and marketing products in its Data Brokers report in 2014 as well as the practice of compiling additional data on users by tracking them on multiple devices in its cross-device tracking report in 2016.[76] But it has not deeply studied the current state of "psychographic" tools. A key question is whether such tools are legitimate advertising and marketing practices or more like subliminal advertising—which the FTC bans.[77]

---

events/press-releases/2015/12/ftc-announces-agenda-privacycon [https://perma.cc/M5FX-GGWJ].

[72] *See, e.g.*, Fed. Trade Comm'n, *Fall Technology Series: Ransomware* (Sept. 7, 2016), https://www.ftc.gov/news-events/events-calendar/2016/09/fall-technology-series-ransomware [https://perma.cc/TJX8-AT22]; *see also* Fed. Trade Comm'n, *FTC Technology Series: Drones* (Oct. 13, 2016), https://www.ftc.gov/news-events/events-calendar/2016/10/fall-technology-series-drones [https://perma.cc/65W6-K6MS]; Fed. Trade Comm'n, *FTC Technology Series: Smart TV* (Dec. 7, 2016), https://www.ftc.gov/news-events/events-calendar/2016/12/fall-technology-series-smart-tv [https://perma.cc/T4E9-FYWU].

[73] *See Office of Technology Research and Investigation*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/office-technology-research-investigation [https://perma.cc/N3KD-72LB].

[74] Antoni Garcia Martinez, *The Noisy Fallacies of Psychographic Targeting*, WIRED (Mar. 19, 2018), https://www.wired.com/story/the-noisy-fallacies-of-psychographic-targeting/ [https://perma.cc/8CN3-HH8J].

[75] Will Oremus, *The Real Scandal Isn't What Cambridge Analytica Did*, SLATE (Mar. 20, 2018), https://slate.com/technology/2018/03/the-real-scandal-isnt-cambridge-analytica-its-facebooks-whole-business-model.html [https://perma.cc/Q698-NNX2].

[76] FTC CROSS-DEVICE TRACKING REPORT, *supra* note 57.

[77] Fed. Trade Comm'n, *Advertising FAQ's: A Guide for Small Business (*2001), https://www.ftc.gov/tips-advice/business-center/guidance/advertising-faqs-guide-small-business [https://perma.cc/F2J7-7P97].

The FTC will also need to stay abreast of the competition and consumer protection issues raised by artificial intelligence (AI). Much has already been written about the transformative potential of AI, its ethical and social implications, and its risks and benefits. While there are several initiatives aimed at creating self-regulatory standards for managing AI, there is not much coordination around AI policy at the federal level. The FTC has identified some areas in which its expertise in consumer privacy and data security can help other regulators address challenges posed by AI. For example, in June 2017 the FTC conducted a workshop with the National Highway Traffic Safety Administration (NHTSA) to discuss connected, automated vehicles.[78] But as AI continues to impact nearly every industry, the FTC should play a more active role in laying the groundwork for the institutional configurations—in government and in industry—that will be both flexible enough and strong enough to govern increasingly sophisticated and autonomous technology. The FTC should draw on its experience promoting privacy by design and security by design frameworks to engage stakeholders and policymakers in expanding these frameworks to include governance and ethics. The goal of governance and ethics by design should be to insure that human designers maintain both accountability and control of predictive technology. Such a framework would include the following considerations: (1) privacy; (2) security; (3) safety; (4) transparency; (5) control; (6) explainability; (7) compliance with existing law; (8) testing; (9) data quality; and (10) mitigation and remediation.

The FTC is capable of continuing to adapt to the digital age, but it must have the resources and tools to do so. As discussed above, Congress should grant the FTC rulemaking and civil penalty authority to protect consumers' privacy, security, and data rights. In addition, Congress should eliminate outdated exemptions to the FTC's authority such as the common carrier exemption[79] and the limitation on enforcement against non-profit entities.[80] Moreover, it must adequately fund the Commission. In FY18,

[78] Press Release, Fed. Trade Comm'n, FTC, NHTSA to Conduct Workshop on June 28 on Privacy, Security Issues Related to Connected, Automated Vehicles (Mar. 20, 2017), https://www.ftc.gov/news-events/press-releases/2017/03/ftc-nhtsa-conduct-workshop-june-28-privacy-security-issues [https://perma.cc/W897-8PM9].

[79] 15 U.S.C. § 45(a)(2) (2012).

[80] 15 U.S.C. §§ 45-46, 53 (empowering the Commission to enforce the FTC Act against "persons, partnerships, or corporations"); 15 U.S.C. § 44 (defining "corporation" as an entity "organized to carry on business *for* its own *profit* or that of its members") (emphasis added); *see* Cmty. Blood Bank of the Kansas City Area, Inc. v. FTC, 405 F.2d 1011, 1022 (8th Cir. 1969) (holding the Act applies to some nonprofit organizations and not others). *But see* Cal. Dental Ass'n. v. FTC, 526 U.S. 756, 766–68 (1999) (finding the Act does apply to a non-profit entity that carries on business for the profit of its members).

the agency's funding decreased slightly from $313 million to $306 million—well below the Obama administration's FY17 proposed level of $342 million.[81] The Commission should also consider scaling up its in-house technology and research expertise by reorganizing and expanding O-Tech into a Bureau of Technology staffed by technologists and investigators which could analyze changing technology, conduct research, and assist with and advise on consumer protection and competition cases.

CONCLUSION

In 2014, when the FTC celebrated its 100th anniversary, it was heralded as the "Federal Technology Commission" because of its role at the intersection of consumer protection and technology policy.[82] In order to remain so, the FTC must continue to keep pace with rapidly changing technology. There is much the agency can do to flex and stretch its existing authorities and resources to meet this challenge, but it would be far better for Congress to strengthen the agency and the protections afforded consumers for their data necessary authorities and resources. At the start of its 104th year, the FTC is again at the epicenter of important questions about the level of risk consumers are bearing in the digital age and limitations of the US's fragmented approach to consumer privacy and data security protection.

[81] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, OMB BUDGET FISCAL YEAR 2017, https://obamawhitehouse.archives.gov/sites/default/files/omb/budget/fy2017/assets/oia.pdf [https://perma.cc/98S3-JD8X].

[82] Omar Tene, *With Ramirez, the FTC Became the Federal Technology Commission,* IAPP (Jan. 18, 2017) https://iapp.org/news/a/with-ramirez-ftc-became-the-federal-technology-commission/ [https://perma.cc/9GWQ-YD7N].