ConsumersUnion®

THE ADVOCACY DIVISION OF CONSUMER REPORTS

August 20, 2018

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW
Suite CC-5610 (Annex C)
Washington, DC 20580

Re: Competition and Consumer Protection in the 21st Century Hearings, Project Number P1812201

1. The state of antitrust and consumer protection law and enforcement, and their development, since the Pitofsky hearings;

Antitrust Law and Enforcement

For Consumers Union's[1] comments pertaining to antitrust law and enforcement please see: *Comments of Consumers Union—Antitrust and Competition Issues*.

Consumer Protection Law and Enforcement

The Federal Trade Commission (FTC) has served US consumers well by bringing enforcement actions and offering guidance for decades. However, consumers lack critical protections especially in regards to safeguarding their privacy. In order for consumers to be effectively protected, the FTC needs more staff, civil penalty authority, administrative rulemaking authority, and newer consumer protection laws, including a dedicated privacy and security law.

In the meantime, we encourage the FTC to pursue robust enforcement of the Federal Trade Commission Act in order to hold companies accountable for the numerous privacy harms that have proliferated in the marketplace. Although the FTC's privacy and security work has been affected by cases like *LabMD, Inc. v. FTC* and *D-Link Corp. v. FTC*, we urge the Commission to develop a clear public policy on how it will continue to issue strong, enforceable orders. We also urge the Commission to adopt an expansive view of what constitutes an unwarranted intrusion.

[1] Consumers Union is the advocacy division of Consumer Reports, an expert, independent, non-profit organization whose mission is to work for a fair, just, and safe marketplace for all consumers and to empower consumers to protect themselves. Consumers Union works for pro-consumer policies in the areas of antitrust and competition policy, privacy and data security, financial services and marketplace practices, food and product safety, telecommunications and technology, travel, and other consumer issues, in Washington, DC, in the states, and in the marketplace. Consumer Reports is the world's largest independent product-testing organization, using its dozens of labs, auto test center, and survey research department to rate thousands of products and services annually. Founded in 1936, Consumer Reports has over 6 million members and publishes its magazine, website, and other publications.

Limits on the Federal Trade Commission

Consumers Union has always regarded the FTC as a leader in ensuring that consumers are protected in the marketplace, and that they have the accurate information needed to make informed decisions. Every year, the FTC returns millions of dollars to consumers and saves billions more through its law enforcement efforts. Every year, it halts ongoing fraud and deception, and helps legitimate companies that offer consumers valuable products and services compete on a level playing field. Every year, it educates the public through consumer and business education, public workshops, and policy reports. And it does so on a shoestring, compared with the budgets of many other federal agencies, and without many of the tools and remedies that other agencies routinely employ.

In addition, the FTC recently created an Office of Technology Research and Investigation, and has appointed a series of Chief Technologists, to ensure that the Commission thoroughly understands new and emerging technologies as it seeks to address consumer protection issues in our increasingly connected world.

Although the FTC has worked tirelessly to protect consumers, the agency's effectiveness is limited by certain restrictions on its authority. Notably, for historical reasons that no longer make sense, the FTC lacks authority to address unfair or deceptive practices by "common carriers" and nonprofit entities. It has very limited rulemaking authority. And it can only seek penalties for law violations in very specific instances. The FTC needs more authority to protect consumers, not less, including stronger tools to protect consumers from privacy and security threats; broader jurisdiction over common carriers and other entities currently shielded from liability; stronger remedies to hold wrongdoers accountable; and greater resources to address consumer harms across the entire marketplace.[2]

With the favorable ruling in the Ninth Circuit preserving the traditional understanding of the limits of the common carrier exemption,[3] we also urge the FTC to press forward protecting consumers in the area of broadband service, especially with the privacy rollbacks at the FCC. However, in light of the recent the decision by the Northern District of California in the *D-Link Corp. v. FTC*[4] case and the decision in the *LabMD* case,[5] it is clear that the FTC is hampered by the constraints of its existing authority. For this reason, the Commission should petition Congress for an expansion of the FTC's authority so the Commission can more effectively protect consumers.

In the meantime, we also urge the FTC to adopt an expansive view of what constitutes an "unwarranted intrusion"[6] sufficient to constitute substantial injury under its Section 5 unfairness

---

[2] For further discussion of the FTC's authority, please see Consumer Union's response to Topic 11: *The agency's investigation, enforcement, and remedial processes*.

[3] Lesley Fair, *En Banc Court of Appeals Rules in FTC's Favor on Common Carrier Issue*, FED. TRADE COMM'N (Feb. 28, 2018), https://www.ftc.gov/news-events/blogs/business-blog/2018/02/en-banc-court-appeals-rules-ftcs-favor-common-carrier-issue.

[4] *D-Link*, FED. TRADE COMM'N (May 22, 2017), https://www.ftc.gov/enforcement/cases-proceedings/132-3157/d-link.

[5] *LabMD, Inc., In the Matter of,* FED. TRADE COMM'N (Sept. 26, 2016), https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter.

[6] In her September 19, 2017 speech announcing the December 2017 Informational Injury Workshop, Acting Chairman Maureen Ohlhausen identified five types of consumer informational injury: deception injury or subverting consumer

authority. For example, in the *Vizio* case, second-by-second information about the video displayed on a consumer's TV was collected and then combined with specific demographic information, such as sex, age, income, marital status, household size, education level, home ownership, and household value.[7] And in a series of cases involving *Aaron's* rent-to-own computers, the companies enabled spyware on the rentals that monitored computers in consumers' homes.[8] We encourage the Commission to expand on these cases to challenge similar practices that are harmful and highly invasive as violative of the unfairness prong of Section 5 of the FTC Act.

Consumers' Concern for Their Privacy

Despite the Commission's efforts to protect consumers, consumers face enormous challenges navigating today's marketplace, making it harder than ever to avoid fraud, deception, and other harms. Every day, they face 24-hour data collection and advertising, phishing attempts, imposter scams, massive data breaches, highly sophisticated frauds, and confusion about who they can trust. Although consumers are increasingly interested in protecting their privacy and the security of their data, they are unable to do so, because it is too time-consuming and hard for consumers to effectively manage the amount of data that is collected about them.[9]

Consumer Reports' 2015 survey showed that 88 percent of individuals say it is important that they not have someone watch or listen to them without their permission.[10] A Mozilla study found that a third of people feel like they have no control of their information online;[11] and, a study from Pew noted that respondents "regularly expressed anger about the barrage of unsolicited emails, phone calls, customized ads, or other contacts that inevitably arises when they elect to share some information about themselves."[12] The majority of consumers (74 percent) find it is "very important" to be in control over who can get information about them.[13] In addition, 67 percent of consumers highly value not having "someone watch you or listen to you without your permission" and 65 percent of consumers think it is "very important" to control what information is collected

---

choice, financial injury, health or safety injury, unwarranted intrusion injury, and reputational injury. Maureen K. Ohlhausen, *Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases*, FED. TRADE COMM'N (Sept. 19, 2017), https://www.ftc.gov/system/files/documents/public_statements/1255113/privacy_speech_mkohlhausen.pdf.

[7] *VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent*, FED. TRADE COMM'N (Feb. 6, 2017), https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it.

[8] *See, e.g., Aaron's*, FTC File No. 122-3264 (2013), https://www.ftc.gov/enforcement/cases-proceedings/122-3256/aarons-inc-matter.

[9] Unfortunately, consumers typically remain unaware of when their data has been compromised until they are notified or leaked information alerts the general population to data and privacy concerns. This is why data breach notifications are so important and why third parties like Consumer Reports works to keep consumers informed about their data privacy choices and methods to have more control over their privacy and data security. *See, e.g.*, Tericus Bufete, *How to Use Facebook Privacy Settings*, CONSUMER REPORTS (Apr. 4, 2018), https://www.consumerreports.org/privacy/facebook-privacy-settings/.

[10] Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security, and Surveillance*, PEW RESEARCH CTR. (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

[11] *Hackers, Trackers, and Snoops: Our Privacy Survey Results*, MOZILLA (Mar. 9, 2017), https://medium.com/mozilla-internet-citizen/hackers-trackers-and-snoops-our-privacy-survey-results-1bfa0a728bd5.

[12] Lee Rainie & Maeve Duggan, *Privacy and Information Sharing*, PEW RESEARCH CTR. (Jan. 14, 2016), http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/.

[13] *See Americans' Attitudes*, *supra* note 10.

about them.[14] Indeed, this is not a new sentiment for consumers: a Pew research poll in 2014 found that 91 percent of adults "'agree' or 'strongly agree' that consumers have lost control over how personal information is collected and used by companies."[15] Consumers desire the ability to limit data collection, detrimental uses, and unnecessary retention and sharing, but lack the ability to easily and efficiently exercise those preferences.

These concerns have a tangible effect on how consumers conduct themselves online. The National Telecommunications & Information Administration's analysis of recent data shows that Americans are increasingly concerned about online security and privacy, at a time when data breaches, cybersecurity incidents, and controversies over the privacy of online services have become more prominent.[16] These concerns are even prompting some Americans to limit their online activity.[17]

Notice and Choice is Insufficient to Protecting Consumer Privacy

Unfortunately, the FTC's historical notice-and-choice approach to safeguarding personal privacy has proven ineffective.[18] Privacy policies are an ineffective method of providing information directly to consumers. Because the law does not clearly mandate specific disclosures, and because most FTC privacy cases are predicated upon a specific misstatement in a privacy policy or elsewhere, privacy policies tend to be vague and expansive. But even if they were more precise, it would not be efficient for consumers to read them: a study by Aleecia McDonald and Lorrie Cranor estimated that reading every site's privacy policy would take users over 244 hours per year, at a collective societal cost in wasted opportunity of over $600 billion.[19]

Despite these issues, privacy policies have a role to play. Companies should be required to provide more detailed information about their actual practices within their privacy policies—not so much for consumers, but for regulators, journalists, civil society, and ratings services such as Consumer Reports. As such, privacy policies would function more like financial filings, which are important accountability documents, and which are not necessarily read by ordinary investors, but which are processed by intermediaries to convey meaningful information to the marketplace.

In light of the issues posed by privacy policies—and because consumers strongly desire the ability to control their data and protect their privacy, but lack the means to do so—consumers need better information and tools to evaluate and compare privacy choices. To that end, Consumer Reports and its partners have developed The Digital Standard,[20] an open standard for testing products for

---

[14] *Id*.

[15] Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RESEARCH CTR. (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

[16] Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NAT'L TELECOM. & INFO. ADMIN. (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

[17] *Id*.

[18] *See* Terrell McSweeny, *Psychographics, Predictive Analytics, Artificial Intelligence, & Bots: Is the FTC Keeping Pace?*, 2 GEO. L. TECH. Rev. 514 (2018), *available at* https://www.georgetownlawtechreview.org/wp-content/uploads/2018/07/2.2-McSweeny-pp-514-30.pdf.

[19] Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, J. OF LAW & POLICY FOR THE INFO. SOCIETY (2008), https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf.

[20] The Digital Standard (theDigitalStandard.org) was launched on March 6th, 2017 and is the result of a collaboration

privacy and security in order to help consumers make informed decisions in the marketplace. The testing includes assessments of a company's stated privacy practices in both the user interfaces and in their privacy policies. This effort depends on the transparency that privacy policies and user interfaces provide consumers.

Consumers Deserve Stronger Privacy Rights Under the Law

While transparency is important, Consumers Union continues to support broader legislation that would provide increased protections for consumer data security and privacy.[21] We urge the FTC to renew its support for stronger, clearer authority in this area as well. Such a law should require:

- Clear information about data practices;
- Simple and easy-to-use consumer choices;
- The collection and retention of only the data necessary—and the disposal of old data;
- Explicit mandate to use reasonable security practices;
- Ways for consumers to get easy access to their information; and
- Strong enforcement tools to ensure accountability.[22]

Unfortunately, legal protections at the federal level are currently getting weaker.[23] In response, the states are leading the way on advancing legislation to safeguard consumer privacy and security. For example, the recently passed California Consumer Privacy Act[24] will give consumers control over the sale of their data, in addition to new access and transparency rights.

Just as states have determined the legal landscape for data breach notification,[25] states seem poised to set more comprehensive standards for security and data privacy. While Consumers Union supports many of these state legislative initiatives, a strong federal law ensuring privacy and security protections for all personal data is still needed. Importantly, however, federal legislation should serve as a floor—not a ceiling—for legal protections, and should allow the states to continue to iterate over time to protect their citizens' personal information. Federal legislation must not simply codify weak rules while preventing the states from imposing more meaningful protections.

---

with our cybersecurity partners, Disconnect, Ranking Digital Rights, and the Cyber Independent Testing Lab. The Standard is designed to hold companies accountable and equip Consumer Reports and other organizations to test and rate products for how responsibly they handle our private data. This is a collaborative and open source effort. The Standard is designed to empower consumers to make informed choices about the connected products, apps, and services consumers use everyday.

[21] Jessica Rich, *Beyond Facebook, It's High Time for Stronger Privacy Laws*, WIRED (Apr. 8, 2018), https://www.wired.com/story/beyond-facebook-its-high-time-for-stronger-privacy-laws/.

[22] Consumers Union, *Where We Stand: Congress Should Pass a Strong Privacy Law, Now*, CONSUMER REPORTS (Apr. 9, 2018), https://www.consumerreports.org/privacy/its-time-for-congress-to-pass-a-strong-privacy-law/

[23] Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 356-74 (2015), http://harvardlpr.com/wp-content/uploads/2015/07/9.2_3_Brookman.pdf.

[24] Unfortunately, industry groups are working to weaken the bill. Susan Grant, *Consumer and Privacy Groups Urge California Lawmakers Not to Weaken Recently-Enacted Privacy Law*, CONSUMER FED. OF AMERICA (Aug. 13, 2018), https://consumerfed.org/testimonial/consumer-and-privacy-groups-urge-california-lawmakers-not-to-weaken-recently-enacted-privacy-rules/ *AB-375*, CALIF. STATE LEGISLATURE, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 (last visited July 30, 2018).

[25] *Data Breach Notification Laws: Now in All 50 States*, PRIVACY RIGHTS CLEARINGHOUSE (May 9, 2018), https://www.privacyrights.org/blog/data-breach-notification-laws-now-all-50-states.

2. Competition and consumer protection issues in communication, information, and media technology networks;

Competition Issues in Communication, Information, and Media Technology Networks

For Consumers Union's comments on competition issues pertaining to communication, information, and media technology networks please see: *Comments of Consumers Union—Antitrust and Competition Issues*.

Consumer Protection Issues in Communication, Information, and Media Technology Networks

Our comments to this topic address specific privacy issues in the technology marketplace on which the Federal Trade Commission (FTC) has focused in recent years, including in its seminal 2012 Privacy Report.[1] The first is the online advertising industry which has been a significant focus for the Commission for nearly two decades.[2] We describe how despite numerous calls for meaningful self-regulation, industry frameworks still suffer from the same endemic weaknesses (and in the meantime, online tracking has become far more sophisticated and invasive). We also examine the data broker industry which similarly is largely unreformed despite extensive FTC attention.[3] While Consumers Union supports the enactment of comprehensive privacy legislation, if instead the Commission opts to select specific industries for targeted legislation, these two industries are both excellent options given strong (and currently frustrated) consumer preferences with regard to these industries, coupled with the long history of failed self-regulation. Finally, we look at broadband privacy, which is now within the authority of the Federal Trade Commission.[4] In our view, the

---

[1] *Protecting Consumer Privacy in an Era of Rapid Change*, FED. TRADE COMM'N (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[2] *See Turn, Inc., In the Matter of*, FED. TRADE COMM'N (Apr. 21, 2017), https://www.ftc.gov/enforcement/cases-proceedings/152-3099/turn-inc-matter; *FTC Puts an End to Tactics of Online Advertising Company that Deceived Consumers Who Wanted to "Opt Out" from Targeted Ads*, FED. TRADE COMM'N (Mar. 14, 2011), https://www.ftc.gov/news-events/press-releases/2011/03/ftc-puts-end-tactics-online-advertising-company-deceived; *Mobile Advertising Network InMobi Settles FTC Charges it Tracked Hundreds of Millions of Consumers' Locations Without Permission*, FED. TRADE COMM'N (June 22, 2016), https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked; *Google will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser*, FED. TRADE COMM'N (Aug. 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented/.

[3] DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY, FED. TRADE COMM'N (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf; *and*, *see*, *FTC Puts an End to Data Broker Operation that Helped Scam More than $7 Million from Consumers' Accounts*, FED. TRADE COMM'N (Nov. 30, 2016), https://www.ftc.gov/news-events/press-releases/2016/11/ftc-puts-end-data-broker-operation-helped-scam-more-7-million; *FTC Charges Data Broker with Facilitating the Theft of Millions of Dollars from Consumers' Accounts*, FED. TRADE COMM'N (Dec. 23, 2014), https://www.ftc.gov/news-events/press-releases/2014/12/ftc-charges-data-broker-facilitating-theft-millions-dollars.

[4] *FTC, FCC Outline Agreement to Coordinate Online Consumer Protection Efforts Following Adoption of the Restoring Internet Freedom Order*, FED. TRADE COMM'N (Dec. 11, 2017), https://www.ftc.gov/news-events/press-releases/2017/12/ftc-fcc-outline-agreement-coordinate-online-consumer-protection; *and*, *see*, Brian Fung, *Trump has Signed Repeal of the FCC Privacy Rules, Here's What Happens Next*, WASH. POST (Apr. 4, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/04/04/trump-has-signed-repeal-of-the-fcc-privacy-rules-heres-what-happens-next/?utm_term=.2609c0ebf81c; CONGRESSIONAL REVIEW OF AGENCY RULEMAKING, 5

Commission's Section 5 authority under the FTC Act is inadequate to provide sufficient privacy protections given the unique role that ISPs play, and we urge the Commission to call for ISP-specific legislation to enhance its (or the Federal Communications Commission's) authority.

Failure of Do Not Track and of Self-Regulation in the Online Advertising Ecosystem

The digital advertising ecosystem has become more complex in recent years, leaving consumers with little information or agency over how to safeguard their privacy. Consumers are no longer just tracked through cookies in a web browser: instead, companies are developing a range of novel techniques to monitor online behavior, and to tie that to what consumers do on other devices and in the physical world. While some companies have reformed their offerings in response to consumer privacy concerns, ad tracking companies have by and large taken advantage of opacity and consumer confusion to evade scrutiny—and have backtracked from prior commitments to offer better protections. Consumers want more and better privacy protections, but do not have the practical ability to take action. In light of the failure of the industry to effectively self-regulate, the FTC should ask Congress to give the Commission rulemaking authority in order to ensure that consumers' tracking and data collection preferences are honored. In the meantime, the FTC should continue to examine online advertising practices closely.

In response to long-standing consumer concerns,[5] some market actors have made significant changes to limit data collection on their platforms. Apple, for example, in 2013 introduced a mandatory "Limit Ad Tracking" setting for iPhone applications, and recently improved that tool to further limit the information advertisers can receive when the setting is activated.[6] Mozilla too has taken efforts to differentiate its Firefox web browser, by adopting policies to limit cross-site data collection.[7] Services like DuckDuckGo have found some success in marketing themselves as the tracking-free alternative to larger companies that rely on data for advertising.[8] And a number of private entities have developed ad blockers that stop many online tracking techniques, such as Disconnect.me, EFF's Privacy Badger, and uBlock. Industry analysts expect ad blocker adoption to reach 30 percent this year, led primarily by the youngest internet users.[9] The start-up Brave has also developed browsers that block ads by default, and is exploring alternative web funding models based on privacy-friendly ads and micropayments of cryptocurrency.[10]

For its part, Consumer Reports is taking steps to provide more accountability to the market and to give consumers actionable information about which companies do a better job of privacy. To help consumers make decisions in the marketplace, Consumer Reports has developed, and is actively

---

U.S.C. §§801-808.

[5] For more on this topic, please see Consumer Union's comments pertaining to Topic 1: *The state of antitrust and consumer protection law and enforcement, and their development, since the Pitofsky hearings.*

[6] Lara O'Reilly, *Apple's Latest iPhone Software Update Will Make it a lot Harder for Advertisers to Track You,* BUS. INSIDER (Sept. 10, 2016), http://www.businessinsider.com/apple-ios10-limit-ad-tracking-setting-2016-9.

[7] Monica Chin, *Firefox's Quantum Update will Block Websites from Tracking You 24/7*, MASHABLE (Jan. 23, 2018), https://mashable.com/2018/01/23/firefox-quantum-releases-update/#yPrZ0O74MqqQ.

[8] Apekshita Varshney, *Hey Google, DuckDuckGo Reached 25 Million Daily Searches*, TECHWEEK (June 4, 2018), https://techweek.com/search-startup-duckduckgo-philadelphia/.

[9] *30% of All Internet Users Will Ad Block by 2018*, BUS. INSIDER (Mar. 21, 2017), http://www.businessinsider.com/30-of-all-internet-users-will-ad-block-by-2018-2017-3.

[10] Stephen Shankland, *Ad-blocking Brave Browser to Give Crypto-payment Tokens to Everyone*, CNET (Apr. 19, 2018), https://www.cnet.com/news/ad-blocking-brave-browser-to-give-crypto-payment-tokens-to-everyone/

testing products under, the Digital Standard.[11] The Digital Standard is an open standard for testing products and services for privacy and security. Our testing under the Standard includes assessments of a company's stated privacy practices in both its user interfaces and in its privacy policies, as well as analysis of traffic flows. And the Standard examines such questions as: does the company tell the consumer what information it collects? Does it only collect information needed to make the product or service work correctly? And does the company explicitly disclose every way it uses the individual's data?[12] While we are currently conducting case studies under the Standard to ensure that the process is scientific and repeatable, we plan to eventually include privacy and digital security in our comparative testing of products where there is potential market differentiation. Our ultimate goal is to enable consumers to make better, more informed privacy choices, and to spur improvements and greater competition among companies on the privacy safeguards they provide.[13]

Despite the improvements by some user-facing companies discussed above, tracking technology has largely gotten more invasive in recent years. Moreover, industry efforts to self-regulate have largely failed. Five years ago, ad tracking self-regulatory programs had the following weaknesses: the rules only applied to coalition members, industry opt-outs were fragile and easily overridden, industry opt-outs only addressed usage and did not impose meaningful collection or retention limitations, and notice and privacy interfaces were seriously flawed.[14] Unfortunately, these criticisms largely remain intact today, before even considering the dramatic expansion of tracking technologies in recent years.

Industry had originally committed to addressing these flaws by adopting the Do Not Track web standard to give consumers a more robust opt-out tool. In 2012, industry representatives committed to honoring Do Not Track instructions at a White House privacy event.[15] Over the next few years,

---

[11] The Digital Standard (theDigitalStandard.org) was launched on March 6, 2017 and is the result of a collaboration with our cybersecurity partners, Disconnect, Ranking Digital Rights, and the Cyber Independent Testing Lab. The Standard is designed to hold companies accountable and equip Consumer Reports and other organizations to test and rate products for how responsibly they handle our private data. This is a collaborative and open source effort. The Standard is designed to empower consumers to make informed choices about the connected products, apps, and services consumers use every day.

[12] *Id*.

[13] Consumer Reports recently published its first product review that integrates the Digital Standard into scoring. We tested five peer-to-peer payment applications—Apple Pay, Venmo, Square's Cash App, Facebook P2P Payments in Messenger, and Zelle. The ratings focus on how well the services authenticate payments to prevent fraud and error, secure users' money and protect their privacy, as well as other factors such as the quality of customer support, whether they insure deposits, and how clearly they disclose fees. In this inaugural set of results, Consumer Reports rated Apple Pay excellent or very good in the key consumer protection measures of payment authentication and data privacy, and significantly higher than the other four other popular P2P services. Tobie Stanger, *Why Apple Pay is the Highest-Rated Peer-to-Peer Payment Service*, CONSUMER REPORTS (Aug. 6, 2018), https://www.consumerreports.org/digital-payments/mobile-p2p-payment-services-review/; Earlier this year we also published a report on the privacy and security of five smart TV models that were tested using the Digital Standard. *Samsung and Roku Smart TVs Vulnerable to Hacking, Consumer Reports Finds*, CONSUMER REPORTS (Feb. 7, 2018), https://www.consumerreports.org/televisions/samsung-roku-smart-tvs-vulnerable-to-hacking-consumer-reports-finds/.

[14] *Statement of Justin Brookman before the U.S. Senate Comm. on Commerce, Sci., and Transp.*, CTR. FOR DEMOCRACY & TECH. (Apr. 24, 2013), https://cdt.org/files/pdfs/Brookman-DNT-Testimony.pdf.

[15] Dawn Chmieleski, *How 'Do Not Track' Ended Up Going Nowhere,* RECODE (Jan. 4, 2016), https://arstechnica.com/information-technology/2017/03/how-isps-can-sell-your-web-history-and-how-to-stop-them/; *see* Julia Angwin, *Web Firms to Adopt 'No Track' Button*, WALL ST. J. (Feb. 23, 2012),

however, as regulatory pressure and the prospect of new legislation faded, industry backed away from its commitment, with trade groups publicly announcing withdrawal from the industry standard process at the World Wide Web Consortium.[16] Today, seven years after Do Not Track settings were introduced into all the major browser vendors, few ad tracking companies meaningfully limit their collection, use, or retention of consumer data in response to consumers' Do Not Track instructions.

Given two decades of insufficient self-regulation, the Commission should consider calling for specific legislation and rulemaking authority to address cross-site, -app, and -service data collection for online advertising and related purposes.

Failure of Self-Regulation by Data Brokers

Unregulated data brokers have been a persistent problem for consumers for years. In 2006, Consumer Reports conducted an investigative report concluding that: "The practices of commercial data brokers can rob consumers of their privacy, threaten them with identity theft and profile them as dead beats or security risks…"[17] Despite these concerns, the report also concluded that "current federal laws do not adequately safeguard Americans' sensitive information."[18] More than a decade has passed since the publication of our report, yet consumers remain vulnerable to the near-constant collection of information about them by data brokers and the inability to correct the accuracy of this information or stop the sale of their personal data.

Consumer Reports is not alone in noting the risk data brokers pose to consumer privacy and the lack of federal law protecting consumers against data brokers: In the Commission's 2014 *Data Broker* report, the FTC recommended that "Congress consider legislation requiring data brokers to give consumers (1) access to their data and (2) the ability to opt out of having it shared for marketing purposes."[19] The US Senate Commerce Committee 2013 report on data brokers likewise concluded that data brokers provide little transparency or control to consumers and thus "it is important for policymakers to continue vigorous oversight to assess the potential harms and benefits of evolving industry practice and to make sure appropriate consumer protections are in place."[20] Despite this recommendation, data brokers remain largely unregulated and unrestricted. And no new federal laws or rules have been adopted to restrict these activities or protect consumers. FTC Commissioner Julie Brill also called for substantial reforms as part of her "Reclaim Your Name" initiative in 2013; again, however, no such transparency project exists, and consumers remain in the dark about data brokers' collection and dispersal of their personal data.[21]

---

https://www.wsj.com/articles/SB10001424052970203960804577239774264364692.

[16] Kate Kaye, *Do-Not-Track on the Ropes as Ad Industry Ditches W3C*, ADAGE (Sept. 17, 2013), http://adage.com/article/privacy-and-regulation/ad-industry-ditches-track-group/244200/.

[17] *Consumer Reports Investigation Warns Your Privacy is For Sale*, CONSUMERS UNION (Aug. 31, 2006), https://consumersunion.org/research/consumer_reports_investigation_warns_your_privacy_is_for_sale/.

[18] *Id*.

[19] DATA BROKERS, *supra* note 3, at 49.

[20] A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES, US SENATE COMM. ON COMMERCE, SCI., AND TRANSP. p. 36 (Dec. 18, 2013), https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf.

[21] *Reclaim Your Name*, FED. TRADE COMM'N (June 26, 2013), https://loadtest.ftc.gov/public-

In addition, as the examples detailed below demonstrate, there has been no clear examples of industry-wide plans to reform these data brokers' practices.

Despite the fact that data brokers often behave like credit bureaus by selling information that is used to make employment or credit decisions about consumers, many incorrectly claim that they are exempt from the requirements of the Fair Credit Reporting Act (FCRA).[22] For example, the FTC has taken action against the data broker Spokeo for its failure to comply with the FCRA.[23] The FCRA requires these companies to release the consumer's file to them upon request;[24] holds them to accuracy requirements;[25] and even places limits on with whom the information may be shared.[26] Recent changes to the FCRA, which will go into effect later this year, also give every consumer the option of placing a "security freeze," at no charge, with the major credit bureaus, so that they can further limit the disclosure of their information.[27]

Still, there are limits to the FCRA's ability to regulate data brokers. The FCRA only applies when companies sell data for certain purposes, such as for extending employment or credit. Thus, many data brokers are not covered by that law and are not subject to accuracy and transparency requirements. Many individuals do not even know which data brokers are collecting information about them, or how to contact them. Although some data brokers offer some consumer access to their data, these reports are highly curated and thus include some facts about the consumer, but not the conclusions that the data brokers' algorithms have drawn from their data. For instance:

> Someone who takes the trouble to see her file at one of the many brokerages, for example, might see the home mortgage, a Verizon bill, and a $459 repair on the garage door. But she won't see that she's in a bucket of people designated as "Rural and Barely Making It," or perhaps "Retiring on Empty."[28]

This secrecy about data brokers' business practices extends to their responses to lawmakers as well. As the 2013 US Senate Commerce report notes:

> The responses also underscore that consumers have minimal means of learning—or providing input—about how data brokers collect, analyze, and sell their information. The wide variety of consumer access and control policies provided by the representative companies show that consumer rights in this arena are offered virtually entirely at the companies' discretion. The contractual limitations imposed by companies regarding customer disclosures of their data sources place additional

---

statements/2013/06/reclaim-your-name.

[22] BIG DATA: A BIG DISAPPOINTMENT FOR SCORING CONSUMER CREDIT RISK, NAT'L CONSUMER LAW CTR. pp. 22, 25 (2014), *available at* https://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf.

[23] *Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA*, FED. TRADE COMM'N (June 12, 2012), https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed.

[24] 15 U.S.C §1681g.

[25] 15 U.S.C. § 1681e.

[26] 15 U.S.C. § 1681b.

[27] S. 2155 (2018), *available at* https://www.congress.gov/bill/115th-congress/senate-bill/2155.

[28] CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY p. 152 (2016) [hereinafter WEAPONS OF MATH DESTRUCTION].

> barriers to consumer transparency. And the refusal by several major data broker companies to provide the Committee complete responses regarding data sources and customers only reinforces the aura of secrecy surrounding the industry.[29]

Data brokers are taking advantage of an unregulated market in order to exploit the sensitive details they have about most Americans. Data brokers have sold the following lists that contain highly sensitive consumer data: rape survivors; HIV/AIDS sufferers; people with addictive behaviors, and alcohol, gambling, and drug addictions; genetic disease sufferers; police officers' and state troopers' home addresses; and consumers who might take out payday loans, including targeted minority groups.[30] The sensitivity and undesired proliferation of this data has prompted some groups to provide specific guidance to their members in order to prevent harassment or stalking. For instance, the National Network to End Domestic Violence provides guidance to show survivors how they can remove themselves from some data broker lists in order to prevent past abusers from locating them.[31] However, most people are unaware of these resources.

Data brokers also work with the health insurance industry in order to track an individual's education level, marital status, net worth, online orders, race, social media use and content, the status of bill payments, and TV habits.[32] For instance, if a consumer buys plus-sized clothing the data broker could conclude that the consumer is at risk for depression, which entails expensive mental healthcare expenses.[33] These assessments are not only privacy invasive, but also possibly incorrect.[34] Consumers are doubly harmed by this type of data collection when they can neither review nor correct the health information that is collected and assigned to them.[35]

Exacerbating this problem is the fact that the information data brokers store about individuals is often not properly secured or shared. Data brokers' handling of personal consumer data is concerning due to (1) the lack of sufficient data security practices and (2) data brokers' deliberate misuse of the sensitive data they collect.

Although data brokers collect and store an immense amount of personal data about consumers, they do not sufficiently protect the data they store. In 2003, Acxiom was hacked and over 1.6 billion records, which included names, addresses, and email addresses, were stolen.[36] In 2011, the hack of data broker Epsilon exposed the names and email addresses of millions of consumers who

---

[29] A REVIEW OF THE DATA BROKER INDUSTRY, *supra* note 20 at 36.

[30] *What Information Do Data Brokers Have on Consumers, and How Do They Use It?*, TESTIMONY OF PAM DIXON, EXECUTIVE DIRECTOR, WORLD PRIVACY FORUM, BEFORE THE SENATE COMM. ON COMMERCE, SCIENCE, & TRANSP. (Dec. 18, 2013), https://www.worldprivacyforum.org/wp-content/uploads/2013/12/WPF_PamDixon_CongressionalTestimony_DataBrokers_2013_fs.pdf.

[31] *People Searches & Data Brokers*, NAT'L NETWORK TO END DOMESTIC VIOLENCE (2013), https://nnedv.org/mdocs-posts/people-searches-data-brokers/.

[32] *Health Insurers are Vacuuming Up Details About You—And it Could Raise Your Rates*, NAT'L PUB. RADIO (July 17, 2018), https://www.npr.org/sections/health-shots/2018/07/17/629441555/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates.

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] John Leyden, *Acxiom Database Hacker Jailed for 8 Years*, THE REGISTER (Feb. 23, 2006), https://www.theregister.co.uk/2006/02/23/acxiom_spam_hack_sentencing/.

were then subjected to spam and targeted phishing attempts.[37] And LexisNexis' parent company, RELX, has been breached at least 59 times, thus exposing Social Security numbers, driver's license data and mailing addresses of over 300 thousand people.[38]

In addition to these examples of poor data security practices, some data brokers have purposely misused the personal information of consumers. For example, data broker Sequoia One, LLC sold payday loan applicants' financial information to scammers who debited individuals' bank accounts and credit cards for at least 7.1 million dollars.[39] (Adding insult to injury, many of these victims were "subsequently charged bank fees for emptying out their account or bouncing checks."[40]) In addition, data broker Spokeo sold personal information to companies in the human resources, background screening, and recruiting industries without complying with the Fair Credit Reporting Act.[41] In 2007, data broker InfoUSA sold lists of consumers with titles such as "Suffering Seniors" (4.7 million people with cancer or Alzheimer's disease) and "Elderly Opportunity Seekers" (3.3 million older people who were "looking for ways to make money") to third parties who then used the lists to target senior citizens with fraudulent sales pitches.[42]

This failure to protect personal data causes real harm to individuals. Nearly 17 million US consumers fell victim to identity theft in 2017, with total US losses approaching $17 billion.[43] Victims spend precious time and money repairing the damage to their credit and accounts. Medical identity theft, in which thieves use personal information to obtain medical services, exhausts consumers' insurance benefits and leaves them with exorbitant bills. Tax identity theft occurs when thieves use consumers' Social Security numbers to obtain their tax refunds. Fraudulent information on credit reports also causes consumers to pay more for a loan or be denied credit. But despite these clear harms, many organizations fail to implement effective measures to protect against these incidents.

Some states have begun to address these data broker problems. California recently passed the California Consumer Privacy Act (CCPA), which will provide their residents with more transparency and control over the sale of their information to data brokers.[44] And Vermont recently

---

[37] Brian Krebs, *Feds Indict Three in 20011 Epsilon Hack*, KREBSONSECURITY (Mar. 6, 2015), https://krebsonsecurity.com/2015/03/feds-indict-three-in-2011-epsilon-hack/.

[38] Heather Timmons, *Security Breach at LexisNexis Now Appears Larger*, N.Y. TIMES (Apr. 13, 2005), https://www.nytimes.com/2005/04/13/technology/security-breach-at-lexisnexis-now-appears-larger.html.

[39] *Sequoia One, LLC*, FED. TRADE COMM'N (Nov. 30, 2016), https://www.ftc.gov/enforcement/cases-proceedings/132-3253-x150055/sequoia-one-llc; *and*, *see*, Doina Chiacu, *U.S. Charges Data Brokers in $7 Million Payday Loan Scam*, REUTERS (Aug, 12, 2015), https://www.reuters.com/article/usa-ftc-fraud-idUSL1N10N1KP20150812.

[40] WEAPONS OF MATH DESTRUCTION, *supra* note 28 at 82.

[41] *Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed information to Employers and Recruiters in Violation of FCRA*, FED. TRADE COMM'N (June 12, 2012), https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed.

[42] Charles Duhigg, *Bilking the Elderly, with a Corporate Assist*, N.Y. TIMES (May 20, 2007), https://www.nytimes.com/2007/05/20/business/20tele.html?mtrref=www.google.com.

[43] *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study*, JAVELIN (Apr. 24, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin&source=gmail&ust=1533316386215000&usg=AFQjCNHG35NLIAox3Tzr9LoEWQjH58LRcw.

[44] AB-375, CALIF. STATE LEGISLATURE, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 (last visited July 30, 2018).

passed a law creating a data broker registry that provides the Attorney General and state residents with more transparency about which data brokers are operating in the state.[45] Despite these advancements, consumers need more robust protection from data brokers, since they still have little to no control of the collection, sale, proliferation, or use of their data by data brokers. The FTC should ask Congress for more authority to specifically address problems in this industry.

Data Brokers and Credit Scores

Lenders are increasingly proposing to use alternative data in order to help the estimated 45 million consumers who lack a traditional credit report or score to develop their credit histories.[46] Despite the potential benefits of such a method, Consumers Union has strong reservations about the use of alternative data, including information collected by data brokers, to evaluate consumers for the purpose of determining creditworthiness, because we have concerns as to the accuracy, transparency, predictive capability, and impact of using such data. This can be a particular concern with regard to communities of color.

Data brokers, such as Acxiom and Intelius, collect a wide variety of information about consumers. Some data brokers collect personal details such as consumers' behavior online, income, and addresses, which are used for marketing purposes and potentially for other purposes, including lending decisions.[47] Lenders increasingly analyze new types of data in their lending processes. Some, like ZestFinance, combine information purchased from data brokers with information they have gathered online.[48] Some lenders incorporate social media analysis into their underwriting processes—not only to verify data supplied by the applicant, but to evaluate consumers based on their personal and professional associations.[49] Facebook has even patented an algorithm for using social media metrics and data to assess creditworthiness.[50]

Much of the information maintained by data brokers is inaccurate. In 2013, National Consumer Law Center had staff members request and analyze the information collected about them by data brokers eBureau, ID Analytics, Spokeo, Intelius, and Acxiom.[51] Most of the reports included multiple errors, including information that belonged to other people.[52] The participants also found it difficult to obtain the data.[53] And since the participants often received only a small amount of information from the data broker, it was not entirely clear whether the company was releasing all

---

[45] ACT 171: DATA BROKER REGISTRY ACT, VT. LEGISLATURE (May 2018), *available at* https://legislature.vermont.gov/bill/status/2018/H.764.

[46] DATA POINT: CREDIT INVISIBLES, CONSUMER FIN. PROT. BUREAU p. 12 (2015), *available at* http://files.consumerfinance.gov/f/201505_cfpb_data-point-credit-invisibles.pdf.

[47] BIG DATA, A BIG DISAPPOINTMENT FOR SCORING CONSUMER CREDIT RISK, NAT'L CONSUMER LAW CTR. pp. 15-16 (2014) [hereinafter BIG DATA], *available at* https://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf.

[48] *Id*.

[49] IS IT TIME FOR CONSUMER LENDING TO GO SOCIAL? HOW TO STRENGTHEN UNDERWRITING AND GROW YOUR CUSTOMER BASE WITH SOCIAL MEDIA DATA, PWC, p. 7 (Feb. 2015), https://www.pwc.com/us/en/consumer-finance/publications/assets/pwc-social-media-in-credit-underwriting-process.pdf.

[50] Robinson Meyer, *Could a Bank Deny Your Loan Based on Your Facebook Friends?*, ATLANTIC MONTHLY (Sept. 25, 2015), https://www.theatlantic.com/technology/archive/2015/09/facebooks-new-patent-and-digital-redlining/407287/.

[51] BIG DATA, *supra* note 47, at 15.

[52] *Id*. at 18.

[53] *Id*. at 16-17.

of the data they had collected about the consumer.[54] Many regulated data brokers fail to comply with the FCRA's accuracy and transparency requirements, leaving consumers without adequate protections. For example, in 2013, the FTC sent warning letters to several online data brokers that were providing information about consumers' rental histories to potential landlords, in order to notify the data brokers of their responsibilities under the FCRA.[55]

The use of opaque big data processing to make credit decisions compounds the existing lack of transparency and accountability in the credit scoring system. While FICO, for example, provides a broad overview of the factors they consider in creating traditional credit scores,[56] the scoring process remains mysterious, and there are many different credit scores. For example, the Consumer Financial Protection Bureau (CFPB) found that about 20-27 percent of the time, different credit scoring models inexplicably put the same consumer into different credit categories.[57] Adding more actors and increased complexity fails to resolve the fundamental problem of a lack of transparency in the use of data in credit scoring. Many consumers do not know how the alternative scores are calculated, or how to improve their creditworthiness. First, as the FTC notes, consumers are "largely unaware that data brokers are collecting and using this information."[58] Moreover, alternative modeling techniques are even more opaque than FICO's scoring metrics—few know or understand the factors that lead to a good alternative score.[59] When it comes to less-understood "health scores,"[60] consumers may be even less likely to understand what health information is being collected, how that information may be used in a health score, and how that score itself could be used; although consumers have the right to correct some types of health information,[61] they do not necessarily have the right to review and correct all the health information collected and shared about them.

For these reasons, Consumers Union has serious reservations about the use of "big data," or information collected by data brokers, for credit decisions, given the potential for this additional data collection to further exact harm on underserved communities. We urge the FTC to work with the CFPB to continue their analysis of data brokers and lenders using alternative modeling techniques and ensure that they are complying with responsibilities under FCRA,[62] particularly with regard to accuracy and transparency of information,[63] and the Equal Credit Opportunity Act

---

[54] *Id*. at 18.

[55] *FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to Fair Credit Reporting Act*, FED. TRADE COMM'N (Apr. 3, 2013), https://www.ftc.gov/news-events/press-releases/2013/04/ftc-warns-data-brokers-provide-tenant- rental-histories-they-may.

[56] MyFICO, WHAT'S IN MY FICO SCORES, http://www.myfico.com/credit-education/whats-in-your-credit-score/.

[57] ANALYSIS OF DIFFERENCES BETWEEN CONSUMER- AND CREDITOR-PURCHASED CREDIT SCORES, CONSUMER FIN. PROT. BUREAU pp. 2, 17 (2012), *available at* http://files.consumerfinance.gov/f/201209_Analysis_Differences_Consumer_Credit.pdf.

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

[59] WEAPONS OF MATH DESTRUCTION, *supra* note 28 at 142-43.

[60] The public is just beginning to understand "health scores," which was recently described in: *Health Insurers are Vacuuming Up Details About You*, *supra* note 32.

[61] Under the HIPAA Privacy Rule, consumers have the right to review their protected health information (PHI) and to have their record amended for accuracy. This right only applies to protected health information, which is generated by a covered entity (healthcare provider, health plan, or healthcare clearinghouse). 45 C.F.R. §164.526.

[62] BIG DATA, *supra* note 48, at 22.

[63] *Id*. at 23-24.

with regard to disparate impact.[64] Finally, the FTC should ask Congress for additional legal protections, such as barring credit bureaus and lenders from using social media and web browsing data in the credit decision process. The chilling effect on free expression and free association is too great—consumers should not have to be worried that the websites they browse and the people they connect with on social media will be used to determine their creditworthiness.

Broadband Privacy and Internet Service Providers

Finally, the Commission's ability to bring enforcement actions against internet service providers (ISPs) under their Section 5 authority is not a sufficient regulatory regime to ensure that consumers have control over their private information. Although the Commission can sue companies under its jurisdiction if they affirmatively mislead the public about their privacy practices, it has no authority to require ISPs to be: transparent about what personal information they collect and what they do with it; to ask for individuals' consent to use or share that information; or to prohibit "take it or leave it" privacy policies. In addition, since Section 5 of the FTC Act is designed to be broadly applicable to all interstate commerce, privacy protections under Section 5 must fit the mold of essentially all sectors of the economy and cannot speak to the specific challenges and issues posed by the unique broadband market that has historically been regulated by the FCC.

Although there is some disagreement on whether a comprehensive privacy law would be the appropriate solution to the many privacy concerns that consumers face,[65] the broadband internet industry is a prime example of the need at least for some sector-specific privacy rules. Because of their unique relationship with consumers and the comprehensive—and currently unavoidable—nature of their data collection, ISPs warrant dedicated rules to limit their collection and use of customer internet behavioral data for advertising and related purposes. Consumers Union strongly encourages the adoption of privacy and security rules governing broadband ISPs. Since the repeal of the Federal Communications Commission's (FCC) broadband privacy rules, consumers' online communications are afforded less privacy protection than traditional telephonic or paper communications. Therefore, it is vital that broadband privacy protections are reinstated. Broadband privacy protections are necessary because individuals depend on the internet, ISPs have a unique and all-encompassing view of consumer data through their online gatekeeper role, and consumers greatly value their privacy,[66] yet lack agency to effectuate their preferences due to a non-competitive ISP marketplace.[67]

---

[64] *Id*. at 28.

[65] *See*, *e.g.*, "Intense disagreements between Democrats and Republicans over the need for government regulation—on top of well-funded lobbying efforts by tech giants such as Facebook and Google—long have forestalled progress on even the simplest attempts to improve privacy online." Tony Romm, *The Trump Administration is Talking to Facebook and Google About Potential Rules for Online Privacy*, WASH. POST (July 27, 2018), https://www.washingtonpost.com/technology/2018/07/27/trump-administration-is-working-new-proposal-protect-online-privacy/?utm_term=.9f23670fe93c; *and*, *see*, John D. McKinnon & Marc Vartabedian, *Tech Firms, Embattled Over Privacy, Warm to Federal Regulation*, WALL ST. J. (Aug. 6, 2018), https://www.wsj.com/articles/tech-firms-embattled-over-privacy-warm-to-federal-regulation-1533547800.

[66] A recent survey from Consumer Reports found that 92 percent of Americans think companies should have to get permission before sharing or selling users' online data. *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER REPORTS (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/.

[67] Most consumers only have a choice of one or two high-speed broadband providers. Forty percent of all Americans are limited to one ISP. Liza Gonzalez, *Net Neutrality Repeal Fact Sheets*, INST. FOR LOCAL SELF-RELIANCE (Dec. 21,

Repeal of the FCC's Broadband Privacy Rules

In October 2016, the FCC passed rules to protect consumers' broadband privacy. These rules required ISPs to obtain their customers' affirmative consent before using and disclosing their web browsing history, application usage data, and other sensitive information for marketing purposes and with third parties. In addition, under the rules, ISPs were required to be transparent about their privacy practices in a simple and comprehensible way. The rules also created a breach notification regime that would have required ISPs to inform their customers when their information has been accessed by unauthorized parties and could cause harm.[68]

Despite consumers' clearly expressed desire for these protections,[69] in March 2017, the US Congress voted to repeal the rules with a resolution of disapproval under the Congressional Review Act (CRA)—thereby also preventing the FCC from ever passing a rule in "substantially the same form" in the future.[70]

The Unique Role of ISPs

An ISP has an intimate, all-encompassing window into its customers' behavior because they provide internet service that gives them access to a vast amount of data from and about their consumers. While it may be possible for some consumers to act to reduce their privacy risks once they are online, they have no choice but to use an ISP to access the internet and thus to subject all of their online data to unfettered access by the ISP. And consumers often have no choice over which ISP to use.[71] All of an individual's traffic flows over that internet connection, traffic which can convey very personal information such as personal banking details, presence at home, sexual preference, physical ailments, physical location, race or nationality, and religion.[72] Even when traffic is encrypted, ISPs still know the sites and services their customers use.

2017), https://ilsr.org/net-neutrality-repeal-fact-sheets-by-the-numbers-maps-and-data/. The majority of the US broadband market is controlled by two providers: Comcast and Charter. John Bergamayer, *We Need Title II Protections in the Uncompetitive Broadband Market*, PUB. KNOWLEDGE (Apr. 26, 2017), https://www.publicknowledge.org/news-blog/blogs/we-need-title-ii-protections-in-the-uncompetitive-broadband-market. The market for wireless internet service, which is already not very competitive particularly in rural areas, may even shrink from four to three available providers. *Id.* This lack of competition means that consumers cannot necessarily avoid one ISP's data policies simply by switching service providers. This trend of corporate consolidation seems unlikely to abate anytime soon, especially after the Supreme Court's recent decision in *Ohio v. American Express*. As consumers increasingly lack the ability to make meaningful choices or to protect their own interests, legislatures have an obligation to establish basic protections to safeguard fundamental interests and rights. Broadband privacy legislation would restore the traditional relationship between ISPs and their customers—and protect our online activities and communications from unwanted snooping.

[68] Historically, ISPs had not used subscriber data for advertising purposes, but in recent years many of the large ISPs began to build the capacity to monetize personal user data. Matt Keiser, *For Telecoms, The Adtech Opportunity is Massive*, EMARKETER (Jan. 18, 2017), https://www.emarketer.com/Article/Telecoms-Ad-Tech-Opportunity-Massive/1015052; *see* Anthony Ha, *Verizon Reportedly Closes in on a Yahoo Acquisition with a $250M Discount*, TECHCRUNCH (Feb. 15, 2017), https://beta.techcrunch.com/2017/02/15/verizon-yahoo-250-million/.

[69] Consumers' privacy concerns have translated into a desire for stronger laws to help them protect their privacy while online: two-thirds of Americans say that current laws are not good enough in protecting their privacy and the majority of consumers (64 percent) support more regulation of advertisers. Lee Raine, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, PEW RESEARCH CTR. (Mar. 27, 2018), http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/.

[70] 5 U.S.C. § 801(b)(2).

[71] *See supra* text accompanying note 67.

[72] *See What ISPs Can See*, UPTURN (Mar. 2016), https://www.teamupturn.com/reports/2016/what-isps-can-see.

Unfortunately, many consumers are unaware that their ISP collects and sells many kinds of sensitive and private information. User information that ISPs routinely collect and share with business partners includes: "geo-location" data, which can be used to determine precisely where you live and travel to, and when; details about your health and financial status; your web browsing and app usage history; and your social security number. ISPs can even delve into and extract information from the contents of your communications, including email, social media postings, and instant messages.

The potential misuses of personal information go well beyond aggressive product marketing: It gives virtually anyone willing to pay—identity thieves and other scam artists, employers, insurance and financial service providers, business and professional rivals, and even former romantic partners—the ability to assemble a detailed and highly personal dossier of your life. Essentially anything a consumer does or expresses on the internet that they would like to keep private, could all be examined and used to their disadvantage, including communications with doctors or lawyers, political activities, job inquiries, dating site history.

With such comprehensive data, ISPs can create intricately detailed profiles of their customers to sell for a variety of purposes, including targeted digital advertisements for products like payday loans or expensive and unnecessary medications. Consumers should have control over whether their ISP monetizes the data it collects in providing internet service. In addition, consumers clearly desire the protections the FCC rules would have provided.[73] For these reasons, we encourage the federal government to reinstate broadband privacy rules in order to protect consumers' privacy and security. In the absence of a reinstatement, we urge the federal government to avoid preemption of state and local efforts to protect their residents via broadband privacy rules and laws.

The Federal Trade Commission is now the only federal agency that has the power to police ISPs.[74] Although we appreciate the Commission's leadership on protecting consumer privacy under its Section 5 authority, the FTC is currently not a sufficient regulator for ISPs. The Commission needs the authority to require ISPs to be transparent about what personal information they collect and what they do with it, to require ISPs to ask for individuals' consent to use or share that information, and to prohibit "take it or leave it" privacy policies. We urge the FTC ask Congress for specific statutory authority to craft specific broadband privacy rules, or for a statute that broadly prohibits ISP surveillance of user behavior for advertising and related purposes without explicit consent.

---

[73] Recent research from Forrester shows that consumers in the US and Europe are increasingly concerned about how their data is being used online. Greg Sterling, *Survey: Chasm Exists Between Brands and Consumers on Data Privacy*, MARTECH (Apr. 6, 2018), https://martechtoday.com/survey-chasm-exists-between-brands-and-consumers-on-data-privacy-213646. This concern has resulted in individuals trusting fewer brands. *Id*. Additionally, 61 percent of US adults expressed concern about the sharing of their data or online behaviors between companies. *Id*. And an increasing number of consumers (33 percent) block ads when online and use browser do-not-track settings (25 percent). *Id*. Despite these tools, the majority of consumers (61 percent) would like to do more to protect their privacy. *Americans' Complicated Feelings*, *supra* note 69.

[74] *Setting the Record Straight on Broadband Privacy*, CTR. FOR DEMOCRACY & TECH. (June 19, 2017), https://cdt.org/files/2017/06/2017-06-19-Broadband-Privacy-Myths-Facts.pdf.

3. The identification and measurement of market power and entry barriers, and the evaluation of collusive, exclusionary, or predatory conduct or conduct that violates the consumer protection statutes enforced by the FTC, in markets featuring "platform" businesses.

Antitrust

For Consumers Union's comments on antitrust and competition issues pertaining to this topic please see: *Comments of Consumers Union—Antitrust and Competition Issues*.

Consumer Protection

The emergence of giant, cross-service internet platforms such as Facebook, Google, and Twitter, present at least two novel consumer protection issues that the Federal Trade Commission (FTC) should address. First, platforms that offer disparate (and often not consumer-facing) services has led to increased *out-of-context data collection*: that is, collection and correlation of extensive consumer data profiles in surprising—and potentially objectionable—ways. Some of this is relatively transparent, though consumers may still object to the consolidation of data sets from different services. For example, over time Google has broken down its silos from its different products to create a more unified Google service as opposed to separate Gmail, Search, and YouTube products. Google offers some tools to keep these experiences separate, though users may not be aware of them, and when they do, they may be difficult to use. For example, Google offers a "Location History" control to limit Android's passive collection of persistent geolocation data; however, this control has no effect on geolocation data collected and associated with other products such as Search, Maps, and Weather.[1] This aggregation of data across services has become especially pervasive given extensive merger and acquisition activity in the technology sector. Some companies have sought to forestall concerns by making promises not to combine and use data across different products. For example, in the wake of its acquisition by Facebook, WhatsApp promised users that nothing would change from its policy of not using mobile phone numbers for advertising.[2] Nevertheless, in 2016, Facebook announced that it would begin using WhatsApp phone numbers for friend suggestions and ad targeting on Facebook.[3] Despite complaints from advocates, the FTC to date has taken no action.[4]

Still more concerning is the less visible—and more extensive—data collection enabled by

---

[1] Ryan Nakashima, *Google Tracks Your Movements, Like It or Not*, AP NEWS (Aug. 13, 2018), https://apnews.com/828aefab64d4411bac257a07c1af0ecb.
Facebook also collects geolocation in the background when consumers are not using the application. Janelle Nanos, *Every Step You Take*, BOSTON GLOBE (July 2018), https://apps.bostonglobe.com/business/graphics/2018/07/foot-traffic/.

[2] *Facebook*, WHATSAPP BLOG (Feb. 19, 2014), https://blog.whatsapp.com/499/Facebook; *Letter to Erin Egan, Facebook, and Anne Hoge, WhatsApp*, FED. TRADE COMM'N (Apr. 10, 2014), https://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf.

[3] *Looking Ahead for WhatsApp*, WHATSAPP BLOG (Aug. 25, 206), https://blog.whatsapp.com/10000627/Looking-ahead-for-WhatsApp.

[4] *WhatsApp Complaint*, ELEC. PRIVACY INFO. CTR. (Aug. 29, 2016), https://epic.org/privacy/ftc/whatsapp/EPIC-CDD-FTC-WhatsApp-Complaint-2016.pdf.

platforms acting as a service provider for other companies. For example, both Google and Facebook provide advertising, analytics, and social widgets to a massive number of other publishers' websites and applications. Various studies have shown that Facebook and Google track users on a tremendous number of third-party sites;[5] one survey from the FTC's Office of Technology Research and Investigation found that Google and Facebook were embedded on 87.5 percent and 69 percent of major websites.[6] Industry defenders used to call cross-site behavioral data collection "anonymous," meaning the data was not easily tied to real-name identity. That fact was relied upon by the FTC in closing its investigation into the DoubleClick acquisition of the data broker Abacus in 2002: the Commission declined to take action in part because "it appears that DoubleClick did not combine PII from Abacus Direct with clickstream data from client websites."[7] The separation between offline identity and behavioral data has fallen by the wayside in recent years: now both Google and Facebook (as well as others who have access to identity data) collect cross-site and -app data across multiple user devices tied to a user identity. This practice is not widely appreciated by consumers[8] and was the subject of bipartisan opprobrium during the recent Facebook-Cambridge Analytica hearings in the Senate and House of Representatives.[9]

In response, the Federal Trade Commission should:

- Encourage companies to be more transparent about actual data practices in privacy disclosures—instead of just vaguely asserting broad rights to collect and use data in a privacy policy. As discussed in more detail in response to Topic 1,[10] the Commission's guidance should recognize that privacy policies are not useful means of conveying information directly to consumers, but they can be studied and monitored by researchers, regulators, the press, and ratings services such as Consumer Reports. Detailed transparency is unlikely to be sufficient by itself to safeguard users' privacy but can introduce information and accountability to the marketplace.
- Aggressively enforce against companies that fail to live up to their privacy representations or offer tools that do not work as described, and continue to use the FTC's unfairness

---

[5] *E.g.,* Stephen Englehardt & Arvind Narayanan, *Online Tracking, A 1-Million-Site Measurement and Analysis*, OPENWPM (2016), http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf; Ibrahim Altaweel *et al., Web Privacy Census,* J. OF TECH. SCI. (2015), https://techscience.org/a/2015121502/.

[6] Justin Brookman, *et al*., *Cross-Device Tracking: Measurement and Disclosures*, 2 PROCEEDINGS ON PRIVACY ENHANCING TECH. 133-48 (2017), https://petsymposium.org/2017/papers/issue2/paper29-2017-2-source.pdf. Indeed, these numbers may be low as they do not account for server-to-server communications that are undetectable to end users.

[7] *Letter to Christine Varney, Re: DoubleClick, Inc*., FED. TRADE COMM'N (Jan. 22, 2001), https://www.ftc.gov/sites/default/files/documents/closing_letters/doubleclick-inc./doubleclick.pdf.

[8] "But, as it has become apparent in the past year, we don't really know who is seeing our data or how they're using it. Even the people whose business it is to know don't know. When it came out that the consulting firm Cambridge Analytica had harvested the personal information of more than fifty million Facebook users and offered it to clients, including the Trump campaign, the *Times*' lead consumer-technology writer published a column titled "I Downloaded the Information That Facebook Has on Me. Yikes." He was astonished at how much of his personal data Facebook had stored and the long list of companies it had been sold to. Somehow, he had never thought to look into this before." Louis Menand, *Why Do We Care So Much About Privacy?*, THE NEW YORKER (June 18, 2018), https://www.newyorker.com/magazine/2018/06/18/why-do-we-care-so-much-about-privacy.

[9] Natasha Singer, *What You Don't Know About How Facebook Uses Your Data*, N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html.

[10] For more on this issue, please see Consumers Union response to Topic 1: *The state of antitrust and consumer protection law and enforcement, and their development, since the Pitofsky hearings*.

authority under Section 5 to pursue out-of-context data collection engaged in without permission. The FTC has brought many important actions against privacy violations, but the Commission should continue to press the boundaries of its limited privacy authority to sufficiently deter practices that frustrate user autonomy and decision-making.

- Request Congress to grant the FTC new statutory authority to issue rules around out-of-context data collection. The burden to safeguard personal information should not fall entirely on consumers—large platforms today offer myriad settings with some degree of control, but they are difficult to manage, offer incomplete protections, and sometimes fail to work as advertised. New privacy law should dictate that data collection and sharing practices accord with reasonable expectations and preferences.

Another feature of large platforms that merits the FTC's attention is the fact that they can be manipulated and misused on an unprecedented scale, including for consumer fraud. While traditional product and information markets were more manually curated, online platforms allow millions (and in some cases, billions) of consumers to interact with others as well as businesses (both well-meaning and less-so) with limited intervention and overhead. Facebook, for example, employs relatively few people for a company its size (its market cap is over $500 billion, or approximately $21 million for each of its 25,000 employees); and only a small percentage are dedicated to eliminating malfeasance on the platform. These platforms are largely insulated from legal responsibility to police their services by Section 230 of the Communications Decency Act, which gives companies broad immunity for how others use their services.

Clearly, there are substantial benefits to both consumers and businesses in engaging on these types of platforms. However, there is also evidence that malicious actors can pervert the way these platforms function without sufficient redress from the platform operators. The 2016 election is but the starkest example of how foreign powers can simulate grassroots opinion on social media to further their own ends. YouTube's automated recommendation has been repeatedly gamed to promote vile and discredited conspiracy theories.[11] Vague promises that "artificial intelligence" may be able to address these problems at some point in the future are not entirely reassuring, as this technology is still potentially years away, not guaranteed to work, and may be compromised by the limitations and biases of the people who design it.[12] However, there have been some signs in recent months that many of the platforms are taking some more proactive measures to reduce

[11] "The algorithm has been found to be promoting conspiracy theories about the Las Vegas mass shooting and incentivizing, through recommendations, a thriving subculture that targets children with disturbing content...Google has responded to these controversies in a process akin to Whac-A-Mole: expanding the army of human moderators, removing offensive YouTube videos identified by journalists and de-monetising the channels that create them. But none of those moves has diminished a growing concern that something has gone profoundly awry with the artificial intelligence powering YouTube." Paul Lewis, '*Fiction is Outperforming Reality': How YouTube's Algorithm Distorts Truth*, THE GUARDIAN (Feb. 2, 2018), https://www.theguardian.com/technology/2018/feb/02/how-youtubes-algorithm-distorts-truth. Google recently announced a plan to combat this problem. Issie Lapowsky, *YouTube Debuts Plan to Promote and Fund 'Authoritative' News*, THE GUARDIAN (July 9, 2018), https://www.wired.com/story/youtube-debuts-plan-to-promote-fund-authoritative-news/.

[12] Sarah Jeong, *AI is an Excuse for Facebook to Keep Messing Up*, THE VERGE (Apr. 13, 2018), https://www.theverge.com/2018/4/13/17235042/facebook-mark-zuckerberg-ai-artificial-intelligence-excuse-congress-hearings. For more on the limitations of algorithms and artificial intelligence, see our comments in response to Topic 9: *The consumer welfare implications associated with the use of algorithmic decision tools, artificial intelligence, and predictive analytics*.

abuse on their services.[13]

While some of this behavior is obviously beyond the FTC's purview, it is clear that platforms enable extensive commercial fraud and malicious anti-consumer behavior as well as political attacks. Shoppers on Amazon—which processes half of all online sales[14]—face a massive fraudulent review ecosystem designed to simulate and obscure truthful information about millions of products, which Amazon has thus far been unable or unwilling to control.[15] Social media platforms are dogged by accounts promoting a wide variety of questionable products and services,[16] promoted through fake followers and fake engagement designed to exploit algorithms that reward such behavior.[17] Fraud in online programmatic advertising is estimated to approach 30% despite industry efforts to address it.[18] In many of these cases, not enough industry actors have sufficient incentives, let alone legal obligations, to try to reduce the scope of illegal activity on their platforms (further, they are in sole possession of the most relevant metrics in assessing the extent of misbehavior). In some cases, the companies benefit directly from the bad behavior; in others, they are judged by analysts based on the scope of their engagement, and as such may be loath to root out all the simulated traffic that distorts the information conveyed through these services. Ultimately, many of the costs of this misbehavior are borne by consumers in the form of higher prices or degraded services.

The FTC can do a number of things to help address these problems.

- Regularly update guidance on what sort of emerging online behaviors violate Section 5 of the FTC Act. The Commission has published solid guidance on native advertising and paid endorsements, but many tactics (such as purchasing followers to artificially amplify signals that may lead to more traffic) are not explicitly covered. The FTC should appoint a task force to keep its guidance up to date.
- More aggressively enforce against companies that abuse platforms to artificially amplify traffic or otherwise deceive consumers. The FTC has brought a number of important cases but clearly has not sufficiently deterred platform abuse.

---

[13] Anthony Ha, *Facebook will Allow You to See All the Active Ads from any Page*, TECHCRUNCH (June 28, 2018), https://techcrunch.com/2018/06/28/facebook-ad-transparency/; Craig Timberg & Elizabeth Dwoskin, T*witter is Sweeping Out Fake Accounts Like Never Before, Putting User Growth at Risk*, WASH. POST (July 6, 2018), https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/?utm_term=.bd9bbe4cf1d1.

[14] Ingrid London, *Amazon's Share of the US e-Commerce Market is Now 49%, or 5% of All Retail Spend*, TECHCRUNCH (July 13, 2018), https://techcrunch.com/2018/07/13/amazons-share-of-the-us-e-commerce-market-is-now-49-or-5-of-all-retail-spend/.

[15] Laura Stevens, *How Sellers Trick Amazon to Boost Sales*, WALL ST. J. (July 28, 2018), https://www.wsj.com/articles/how-sellers-trick-amazon-to-boost-sales-1532750493.

[16] Annie Singer & Joanna Laznicka, *Fake and Deceptive Use of Instagram: How to Spot False Influencers*, http://smartlinkup.com/fake-instagram-influencers/.

[17] Nicholas Confessore, *et al.*, *The Follower Factory*, N.Y. TIMES (Jan. 27, 2018), https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html; Michael H. Keller, *The Flourishing Business of Fake YouTube Views*, N.Y. TIMES (Aug. 11, 2018), https://www.nytimes.com/interactive/2018/08/11/technology/youtube-fake-view-sellers.html.

[18] Alexandra Bruell, *Fraudulent Web Traffic Continues to Plague Advertisers, Other Businesses*, WALL ST. J. (Mar. 28, 2018), https://www.wsj.com/articles/fraudulent-web-traffic-continues-to-plague-advertisers-other-businesses-1522234801.

- Explore ways to incentivize platforms to more aggressively police their platforms for deceptive, unfair, or otherwise illegal behavior.
- Explore ways to foster diversity of content and reduce the risk of algorithmic gaming. Potential solutions could interoperability, independent third-party algorithmic sorting, or more robust options for users to access social media feeds in chronological order, unmediated by algorithms.
- Explore how reducing fraudulent online content and other misbehavior could be a beneficial result of protecting competition and innovation in platforms, and whether that benefit could be a relevant consideration in antitrust investigations involving platforms.
-

4. The intersection between privacy, big data, and competition;

Antitrust

For Consumers Union's comments on antitrust and competition issues pertaining to this topic please see: *Comments of Consumers Union—Antitrust and Competition Issues*.

Consumer Protection

Consumers Union strongly supports the enactment of comprehensive privacy and security legislation as the commercial and societal benefits significantly outweigh any costs. First, for security, the Federal Trade Commission (FTC) has already used Section 5 of the FTC Act extensively to punish unreasonable data and cyber security practices. Legal accountability is important, because companies who fail to safeguard their products and services do not bear the direct risks from resulting security incidents; a company may anticipate that it could one day bear some loss to goodwill or reputation, though that risk is discounted by its occurrence in the (possibly distant) future, and attribution for data breaches is notoriously difficult. And this assumes perfectly rational company decision-making, whereas in reality companies tend to underestimate the potential losses posed by tail-risk events, and are often overly incentivized for focus on short-term revenues. Security law should require companies to internalize the potential harm to the ecosystem in their product planning and development, though no system need strive for *perfect* security—instead, companies should take reasonable and appropriate measures that take into account potential threat models, sensitivity of information, and also the cost of particular security measures.

With regard to privacy, legislation should seek to empower individuals to make choices about the collection and use of their personal information, and to align business practices with reasonable consumer expectations. Today many data practices are completely intransparent to consumers, leaving them generally frustrated but ultimately incapable of making informed choices.[1] Many consumers may willingly accept advertising-support products, but far fewer understand or agree to cross-service data tracking;[2] due to lack of information, companies are able to free-ride on consumers' data without accountability. Privacy disclosures are currently not designed to convey meaningful information either to ordinary consumers or even sophisticated privacy analysts. At the very least, companies should be required to provide more precise information to the market, whether through consumer-facing disclosures or in detailed policies more suited to regulators,

[1] A Mozilla study found that a third of people feel like they have no control of their information online. *Hackers, Trackers, and Snoops: Our Privacy Survey Results*, MOZILLA (Mar. 9, 2017), https://medium.com/mozilla-internet-citizen/hackers-trackers-and-snoops-our-privacy-survey-results-1bfa0a728bd5. And although the majority of consumers (74%) find it is "very important" to be in control of who can get information about them. Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security, and Surveillance*, PEW RESEARCH CTR. (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/. A Pew research poll found that 91 percent of adults "'agree' or 'strongly agree' that consumers have lost control over how personal information is collected and used by companies." Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RESEARCH CTR. (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

[2] Chris Kahn & David Ingram, *Americans Less Likely to Trust Facebook than Rivals on Personal Data, Reuters/Ispsos 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; Joseph Turow, *et al*., *Americans Reject Tailored Advertising and Three Activities that Enable It*, SSRN (Sept. 29, 2009), https://ssrn.com/abstract=1478214..

press, and analysts. Consumers should be able to obtain access to the information that companies have about them in a structured format to promote accountability and competition. Privacy law should also provide some limitations or choices around the secondary use or retention of data, though even advocates disagree on when outright prohibitions, or either opt-in or opt-out choices, are appropriate. All have their limitations: prohibitions may be too blunt, opt-in requirements can be gamed through the use of coercive dark patterns by companies with few competitors,[3] and opt-out choices are difficult to scale. However, given the rapid advance of technology, the alternative of doing nothing is still worse: companies increasingly possess the capacity to collect, store, and process every piece of data about us. Certainly it cannot be the case that consumers must passively submit to boundary-less surveillance simply in order to facilitate a never-ending flow of relevant offers.

Contrary to industry talking points, privacy regulation will benefit *consumers*, not Google and Facebook, which have lobbied aggressively against any expansion of privacy law both in the United States and Europe.[4] Indeed, Google and Facebook are *already* over-powerful and outsized monopolies absent new privacy rules. Similar arguments about the balance of benefits between consumers and those companies were advanced against the Commission's call for a Do Not Track (DNT) browser control;[5] again, however, both fought hard to stop industry adherence to that standard. As a result, Google and Facebook (and the vast majority of the ad tech industry) ignore users' DNT instructions on the web to this day.

Certainly, if a company's business model is predicated entirely on bad privacy practices, then privacy legislation will especially impact them, and will appropriately disadvantage them more compared to companies like Google and Facebook. Both companies have problematic practices that should be addressed by privacy rules, but both also have core products that can be monetized effectively without compromising user privacy. However, because those companies' business models are also heavily reliant on the use of personal information, privacy law does impact them directly—and more than most companies. The Commission has already brought actions against both companies for privacy violations, though due to weaknesses in the law and the limitations in its own authority, its actions have not sufficiently deterred their abuses.

To be clear, effective privacy law should not simply mandate expensive processes and compliance programs. Some companies have sought to frame privacy regulation in terms of *accountability*—

---

[3] DECEIVED BY DESIGN: HOW TECH COMPANIES USE DARK PATTERNS TO DISCOURAGE US FROM EXERCISING OUR RIGHTS TO PRIVACY, NORWEGIAN CONSUMERS COUNCIL (June 27, 2018), *available at* https://www.forbrukerradet.no/side/facebook-and-google-manipulate-users-into-sharing-personal-data/; *and*, *see*, Allen St. John, *CR Researchers Find Facebook Privacy Settings Maximize Data Collection*, CONSUMER REPORTS (June 27, 2018), https://www.consumerreports.org/privacy/cr-researchers-find-facebook-privacy-settings-maximize-data-collection/; *CU Letter to FTC on Norwegian Consumer Council Report "Deceived by Design" and CU Research on Facebook and Google Sign-Up*, CONSUMERS UNION (June 27, 2018), https://consumersunion.org/research/letter-to-ftc-norwegian-consumer-council-report-deceived-by-design/.

[4] Sam Schechner & Nick Kostov, *Google and Facebook Likely to Benefit from Europe's Privacy Crackdown*, WALL ST. J. (Apr. 23, 2018), https://www.wsj.com/articles/how-europes-new-privacy-rules-favor-google-and-facebook-1524536324; Daisuke Wakabayashi & Adam Satariano, *How Facebook and Google Could Benefit from the G.D.P.R., Europe's New Privacy Law*, N.Y. TIMES (Apr. 23, 2018), https://www.nytimes.com/2018/04/23/technology/privacy-regulation-facebook-google.html.

[5] *FTC Testifies on Do Not Track Legislation*, FED. TRADE COMM'N (Dec. 2, 2010), https://www.ftc.gov/news-events/press-releases/2010/12/ftc-testifies-do-not-track-legislation.

a form of self-regulation prioritizing the development of internal policies and procedures over actual substantive rights and protections. A privacy regime that pairs high levels of process with weak substantive rules may in fact unduly favor large companies while doing little to actually preserve users' privacy. Fundamentally, privacy law should accord behaviors with the consumer's reasonable expectations; if a small business is not engaged in dubious data practices, it should not have to alter its practices as much as a larger player like Google or Facebook when complying with new privacy protections.

The continued erosion of privacy also adds to the existing imbalance of information and power between consumers and businesses. Data collection affords companies greater insight and leverage for negotiating individualized prices, allowing companies to extract relatively more of the consumer surplus out of any given transaction. Increased corporate concentration tied with unconstrained data collection and sharing is likely to lead to greater first-order price discrimination, leading to worse results for consumers and greater inequality. As such, consumers have a rational interest in limiting data collection separate from any demonstration of objective "injury."

More broadly, privacy and competition are linked because it is considerably harder for individuals to make privacy-conscious choices when there are, in fact, no choices. While legal protections around privacy and security should be strengthened, there is also a role for improved marketplace solution. As discussed in more detail in our response to Topic 1, privacy policies and disclosures do not typically convey meaningful information to consumers upon which they can make reasoned choices. As such, Consumer Reports has started testing a range of products and services for elements such as privacy and security as part of our Digital Standard work.[6] We recently published our first set of ratings under this project as part of a broader assessment of personal peer-to-peer payment applications.[7] Increased market pressure due to improved transparency can help hold companies accountable for bad practices and bend corporate behaviors in a more positive direction for consumers. However, in the increasing number of markets insulated from sufficient competition, increased transparency can only have a more limited effect. For that reason, there is a rationale for stronger privacy rules for industries in concentrated sectors, such as internet service providers.[8] More broadly, the Commission should reinvigorate its commitment under competition law to ensure that markets provide sufficient *consumer choices* in order to function effectively.

[6] The Digital Standard (theDigitalStandard.org) was launched on March 6, 2017 and is the result of a collaboration with our cybersecurity partners, Disconnect, Ranking Digital Rights, and the Cyber Independent Testing Lab. The Standard is designed to hold companies accountable and equip Consumer Reports and other organizations to test and rate products for how responsibly they handle our private data. This is a collaborative and open source effort. The Standard is designed to empower consumers to make informed choices about the connected products, apps, and services consumers use everyday.

[7] Tobie Stanger, *Why Apple Pay is the Highest-Rated Peer-to-Peer Payment Service*, CONSUMER REPORTS (Aug. 6, 2018), https://www.consumerreports.org/digital-payments/mobile-p2p-payment-services-review/.

[8] For more on this subject, please see Consumers Union's response to Topic 2: *Competition and consumer protection issues in communication, information, and media technology networks.*

5. The Commission's remedial authority to deter unfair and deceptive conduct in privacy and data security matters;

Consumer Protection

Consumers Union is pleased to be able to submit comments on the issue of the Commission's remedial authority to deter unfair and deceptive conduct in privacy and data security matters in preparation for the Competition and Consumer Protection in the 21st Century Hearings.

The Federal Trade Commission (FTC) currently lacks sufficient remedial tools to fulfill its consumer protection mandate and to deter illegal conduct, and we strongly support additional powers—most notably civil penalty authority—to augment its current authority. Today, when a company commits an actionable privacy or security violation under Section 5 of the FTC Act, the Commission does not have the ability to obtain penalties from the company. Nor in most cases is restitution an appropriate remedy, as privacy harms or security risks are difficult to quantify and, while possibly substantial in aggregate, may be relatively small in any individual case. The FTC has ordered the disgorgement of ill-gotten gains in some cases,[9] and should expand its use of that authority in lieu of the ability to obtain penalties. However, even in those cases, a company must only cede what it gained directly from its bad behavior, which hardly serves as a sufficient deterrent to others given the relatively small chance of an FTC action. Certainly, the costs of defending an FTC action, the incumbent loss of customer goodwill, and the cost of implementing a compliance program are non-negligible, but in all they are still insufficient to deter rational actors from engaging in unlawful anti-consumer behaviors: the uncertain application of Section 5 in privacy and security matters, along with the relative unlikelihood of enforcement, are hardly outweighed by the weak consequences if they are caught.

The Federal Trade Commission should be granted civil penalty authority for all Section 5 consumer protection matters, and granted comparable authority in any new privacy and security statute. The way that penalties are assessed for violations of trade regulations is, the appropriate model for other FTC penalties. Penalties should be assessed per violation—or per person affected—not based on the number of days on which a violation has occurred, as has been proposed in some legislation. The latter would lead to obviously perverse results—a company could deliberately share or publish to the world all its customer records just for one day, with disastrous results. Nor should the FTC's penalty authority be subject to a hard, monetary cap, as has also been proposed in some legislation. The appropriate penalty for a small business is obviously very different than it should be for a giant company such as Google or Facebook; a cap would only favor the largest companies and most harmful violations, and thus weaken a law's deterrent and retributive effect as to them. Instead, the penalty amount should be reasonably tied to factors such as the nature of the violation, the types of data compromised, the willfulness of the behavior, and the size of a company, as well as its ability to pay.

[9] *Uber Agrees to Pay $20 Million to Settle FTC Charges that it Recruited Prospective Drivers with Exaggerated Earnings Claims*, FED. TRADE COMM'N (Jan. 19, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/uber-agrees-pay-20-million-settle-ftc-charges-it-recruited. Additionally, we reject the assertion of Commissioner Ohlhausen that disgorgement should be tethered to the amount of consumer harm in any particular case. Rather, the purpose of disgorgement is to deprive a wrongdoer of the fruits of his illegal behavior, not to reward such behavior unless harm can be meaningfully assessed and measured in any particular instance.

As we explain in response to Topics 1-4, Section 5 is not sufficient to ensure the privacy for American consumers deserve and expect.[10] While the Commission's interpretation of Section 5 to mandate reasonable security practices sets an appropriate baseline standard, dedicated security legislation would be beneficial for consumers and industry. As companies have challenged (unfortunately, with some success) the FTC's interpretation of Section 5 and enforcement remedies in court, it would be beneficial to articulate a reasonable security mandate in a dedicated statute. Moreover, as some have criticized the FTC reasonableness standard as not offering sufficient notice to businesses about appropriate security practices and procedures,[11] the FTC should propose a dedicated statute to give the Commission rulemaking authority to offer greater clarity and certainty over time as to what reasonable security entails.

Finally, we reiterate our comments in response to Topic 11 that the Federal Trade Commission needs dramatically more resources to achieve its consumer protection mission and should include these resources in its next budget request. The Commission currently has too few people to bring sufficient cases to effectively deter illegal conduct, and as noted in response to Topic 3, modern internet platforms that host more and more online commerce and advertising do not themselves have sufficient incentives to police their platforms for bad conduct. In addition to Congress dedicating substantially greater funds to augment the FTC's capacity, any new privacy and security statute should also empower state attorneys general to bring enforcement actions in order to supplement the Commission's own work on behalf of consumers.

[10] Recent research from Forrester shows that consumers are increasingly concerned about how their data is being used online. Greg Sterling, *Survey: Chasm Exists Between Brands and Consumers on Data Privacy*, MARTECH (Apr. 6, 2018), https://martechtoday.com/survey-chasm-exists-between-brands-and-consumers-on-data-privacy-213646. This concern has resulted in individuals trusting fewer brands. *Id*. Additionally, 61 percent of US adults expressed concern about the sharing of their data or online behaviors between companies. *Id*. And an increasing number of consumers (33 percent) block ads when online and use browser do-not-track settings (25 percent). *Id*. Despite these tools, the majority of consumers (61 percent) would like to do more to protect their privacy. Lee Raine, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, PEW RESEARCH CTR. (Mar. 27, 2018), http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/.
Consumers' privacy concerns have translated into a desire for stronger laws to help them protect their privacy while online: two-thirds of Americans say that current laws are not good enough in protecting their privacy and the majority of consumers (64 percent) support more regulation of advertisers. *Id*.

[11] Gerard Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data Security Requirements*, 20 GEO. MASON L. REV. 673-720 (May 9, 2013), *available at* https://ssrn.com/abstract=2263037.

6. Evaluating the competitive effects of corporate acquisitions and mergers;

For Consumers Union's comments on antitrust and competition issues pertaining to this topic please see: *Comments of Consumers Union—Antitrust and Competition Issues*.

7. Evidence and analysis of monopsony power, including but not limited to, in labor markets;

For Consumers Union's comments on antitrust and competition issues pertaining to this topic please see: *Comments of Consumers Union—Antitrust and Competition Issues*.

8. The role of intellectual property and competition policy in promoting innovation;

For Consumers Union's comments on antitrust and competition issues pertaining to this topic please see: *Comments of Consumers Union—Antitrust and Competition Issues*.

9. The consumer welfare implications associated with the use of algorithmic decision tools, artificial intelligence, and predictive analytics;

Antitrust

For Consumers Union's comments on antitrust and competition issues pertaining to this topic please see: *Comments of Consumers Union—Antitrust and Competition Issues*.

Consumer Protection

Algorithmic decision tools and predictive analytics are being used to make decisions about consumers without sufficient transparency, testing, or accountability. While there is great potential in these emerging technologies, consumers need greater protections for the use of these tools. Accordingly, Congress should give the Federal Trade Commission (FTC) more authority and resources to create rules for the use of algorithms in light of insufficient applicable federal and state law. Finally, we propose principles for the use of algorithmic decision-making tools.

Algorithmic Decision Tools and Predictive Analytics

Algorithms are routinely used to determine insurance rates,[1] creditworthiness,[2] willingness to pay,[3] and employment prospects.[4] In addition, algorithmic tools are employed to: serve search engine

[1] *See*, *generally*, Rachel Goodman, *Big Data Could Set Insurance Premiums, Minorities Could Pay the Price*, ACLU (July 19, 2018), https://www.aclu.org/blog/racial-justice/race-and-economic-justice/big-data-could-set-insurance-premiums-minorities-could.
Health insurance: *Lifestyle Choices Could Raise Your Health Insurance Rates*, PBS NEWS HOUR (July 21, 2018), https://www.pbs.org/newshour/show/lifestyle-choices-could-raise-your-health-insurance-rates; Marshall Allen, *Health Insurers are Vacuuming Up Details about You—and It Could Raise Your Rates*, PROPUBLICA (July 18, 2018), https://www.scientificamerican.com/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates/.
Car insurance: *Auto Insurers Charging Higher Rates in Some Minority Neighborhoods*, CONSUMER REPORTS (Apr. 4, 2017), https://www.consumerreports.org/media-room/press-releases/2017/04/propublica_and_consumer_reports_auto_insurers_charging_higher_rates_in_some_minority_neighborhoods11/; Enrique Dans, *Why It's Time to Rethink Car Insurance*, FORBES (July 24, 2018), https://www.forbes.com/sites/enriquedans/2018/07/24/why-its-time-to-rethink-car-insurance/#51b7fca91037.

[2] *Understanding Credit Score Algorithms*, AMPLIFY (Dec. 8, 2017), https://www.goamplify.com/blog/improvecredit/understanding-credit-score-algorithms.aspx. For more on this topic, please see Consumers Union's response to Topic 2: *Competition and consumer protection issues in communication, information, and media technology networks*.

[3] *See*, *e.g.*, Nicholas Diakopoulos, *How Uber Surge Pricing Really Works*, WASH. POST (Apr. 17, 2015), https://www.washingtonpost.com/news/wonk/wp/2015/04/17/how-uber-surge-pricing-really-works/?utm_term=.b7ecadd3dc6b; *How Uber's Surge Pricing Algorithm Works*, CORNELL UNIV. (Mar. 17, 2016), https://blogs.cornell.edu/info4220/2016/03/17/how-ubers-surge-pricing-algorithm-works/.

[4] Alexia Elejalde-Ruiz, *The End of the Resume? Hiring is in the Midst of a Technological Revolution with Algorithms, Chatbots*, CHICAGO TRIBUNE (July 19, 2018), http://www.chicagotribune.com/business/ct-biz-artificial-intelligence-hiring-20180719-story.html.

results;[5] match children with schools;[6] detect employment,[7] healthcare, and Medicaid fraud[8] (sometimes erroneously[9]); and identify biometric markers.[10] Unfortunately, despite the notion that algorithms are neutral and objective arbiters, algorithms can exacerbate bias or have unexpected discriminatory effects. The discriminatory effects stem from historical data sets, lack of rigorous testing, and from the imperfect and inherently biased people who create them.[11] For instance, Latanya Sweeney's research found that Google searches for stereotypically African American names were more likely to generate ads suggestive of an arrest than a search for stereotypically white names (regardless of whether the company placing the ad reveals an arrest record associated with the name).[12]

Use of Algorithms in Employment

The biases of "neutral" algorithms are especially apparent in online job recruitment and dynamic pricing. Algorithms are heavily used in the employment sector to filter job applicants and present ads to desired applicant pools. Companies have turned to algorithms to help neutralize biased hiring practices and to help prevent costly employee churn. Unilever, Walmart, and Goldman Sachs, for example, have all turned to algorithms to recruit and sort job applicants.[13] Currently, the majority (72 percent) of all resumes are sorted by algorithms and never seen by human eyes.[14] The substitution of computers for humans in the hiring process has resulted in an employment system where "applicants who are skilled in sprinkling buzz phrases and keywords throughout their resume are often favored in hiring."[15] Job-matching algorithms that assess the likelihood of

---

[5] Dave Davies, *How Search Engine Algorithms Work: Everything You Need to Know*, SEO (May 10, 2018), https://www.searchenginejournal.com/how-search-algorithms-work/252301/; *and*, *see*, Latanya Sweeney, *Discrimination in Online Ad Delivery*, SSRN (Jan. 28, 2013, *available at* https://ssrn.com/abstract=2208240.

[6] Alvin Roth, *Why New York City's High School Admissions Process Only Works Most of the Time*, CHALKBEAT (July 2, 2015), https://www.chalkbeat.org/posts/ny/2015/07/02/why-new-york-citys-high-school-admissions-process-only-works-most-of-the-time/.

[7] *See*, *e.g.*, NORTH CAROLINA GOVERNMENT DATA ANALYTICS CENTER, NC IT, https://it.nc.gov/services/nc-gdac (last visited Aug. 17, 2018).

[8] Natasha Singer, *Bringing Big Data to Fight Against Benefits Fraud*, N.Y. TIMES (Feb. 20, 2015), https://www.nytimes.com/2015/02/22/technology/bringing-big-data-to-the-fight-against-benefits-fraud.html.

[9] VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR, p. 5 (2018) [hereinafter AUTOMATING INEQUALITY].

[10] Robert Triggs, *How Fingerprint Scanners Work: Optical, Capacitive, and Ultrasonic Variants Explained*, ANDROID AUTHORITY (Feb. 9, 2018), https://www.androidauthority.com/how-fingerprint-scanners-work-670934/; Rod McCullom, *Facial Recognition Technology is Both Biased and Understudied*, UNDARK (May 17, 2017), https://undark.org/article/facial-recognition-technology-biased-understudied/; *How Facial Recognition Algorithm Works*, BECOMING HUMAN (Oct. 16, 2017), https://becominghuman.ai/how-facial-recognition-algorithm-works-1c0809309fbb.

[11] *See* Cathy O'Neil, *How Algorithms Rule Our Working Lives*, THE GUARDIAN (Sept. 1, 2016), https://www.theguardian.com/science/2016/sep/01/how-algorithms-rule-our-working-lives.

[12] *Discrimination in Online Ad Delivery*, *supra* note 5.

[13] Wanda Thibodeaux, *Unilever is Ditching Resumes in Favor of Algorithm-Based Sorting*, INC. (June 28, 2017), https://www.inc.com/wanda-thibodeaux/unilever-is-ditching-resumes-in-favor-of-algorithm-based-sortingunilever-is-di.html.

[14] *How Algorithms Rule Our Working Lives*, *supra* note 11; *and*, *see*, CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY, p. 152 (2016) [hereinafter WEAPONS OF MATH DESTRUCTION].

[15] Shiva Bhaskar, *Algorithms, Big Data and Accountability*, MEDIUM (Sept. 30, 2016), https://medium.com/@shivagbhaskar/algorithms-big-data-and-accountability-8924bf9e2b24.

employee retention and success can also be biased against those who are poor.[16] Xerox discovered that a now-defunct program they used for evaluating applicants likelihood of quitting relied heavily on how far away an individual lived from the job site. [17]

Although companies have sometimes turned to algorithms to realize the goal of making hiring more neutral, in practice these algorithms can *increase* bias. For instance, in 2015, researchers at Carnegie Mellon found that women were less likely to be shown ads for high-paying positions.[18] Researchers have also shown that young women were less likely to be presented with an employment ad in a STEM field than young men due to an algorithm that optimized the cost-effectiveness of the ad placement. Ironically, since young women are a more prized demographic, the supposedly gender-neutral algorithm actually favored displaying a STEM employment ad to men.[19] In addition, some personality tests used in the hiring process have been alleged to violate the Americans with Disabilities Act of 1990.[20]

Unfortunately, prejudice and bias are unlikely to be completely eliminated from employee recruitment, regardless of whether an algorithm or human resources personnel conducted the selection and hiring process.[21] However, human resource departments and companies using algorithms to find and select candidates should be encouraged to routinely evaluate the algorithms they use.[22]

Dynamic Pricing

Online retailers use algorithms to create dynamic, individual prices, also known as first-degree price discrimination, on the basis of consumers' assessed willingness to pay. Since 2000, Consumers Union has investigated the murky pricing practices by airlines and travel companies online, and reporting on what Consumer Reports has termed "disturbing evidence of bias" in how airfares are presented to the public. In recent years some of these marketing schemes have come to light, particularly after the International Air Transport Association—the global airline industry's leading trade organization—unveiled "New Distribution Capacity,"[23] a detailed program to enhance "product differentiation." And a recent study commissioned by an aviation company reported that airlines are developing "dynamic availability of fare products" that "could be adjusted for specific customers or in specific situations."[24]

---

[16] *How Algorithms Rule Our Working Lives*, *supra* note 11.
[17] *Algorithms, Big Data and Accountability*, *supra* note 15.
[18] Samuel Gibbs, *Women Less Likely to be Shown Ads for High-Paid Jobs on Google, Study Shows,* THE GUARDIAN (July 8, 2015), https://www.theguardian.com/technology/2015/jul/08/women-less-likely-ads-high-paid-jobs-google-study.
[19] Anja Lambrecht & Catherine E. Tucker, *Algorithmic Bias? An Empirical Study into Apparent Gender-Based Discrimination in the Display of STEM Career Ads*, SSRN (Mar. 9, 2018), https://ssrn.com/abstract=2852260.
[20] *How Algorithms Rule Our Working Lives*, *supra* note 11.
[21] Gideon Mann & Cathy O'Neil, *Hiring Algorithms are Not Neutral*, HARV. BUS. REV. (Dec. 9, 2016), https://hbr.org/2016/12/hiring-algorithms-are-not-neutral.
[22] Human resource departments could help assess their company's hiring algorithms by carrying out randomized spot-checks on machine resume decisions and then put them through an extensive human review in order to uncover potential biases. In addition, HR employees could conduct manual reviews of the correlations that the machine learns and eliminate those that appear biased. *Id.*
[23] NEW DISTRIBUTION CAPABILITY, IATA, https://www.iata.org/whatwedo/airline-distribution/ndc/Pages/default.aspx (last visited Aug. 17, 2018).
[24] *Advances in Airline Pricing, Revenue, Management, and Distribution: Implications for the Airline Industry*, PODS

In October 2016, Consumer Reports published an extensive study of nine leading travel sites and compared identical itineraries, in real time, using both "scrubbed" browsers cleared of all "cookies" and browsers used for extensive web searches.[25] Among 372 searches, CR found 42 pairs of different prices on separate browsers for the same sites retrieved simultaneously. Industry representatives dismissed these disparities as technological glitches; but CR has found similar evidence of dynamic pricing in previous years.[26] Accordingly, Consumers Union supports Senator Chuck Schumer's call for the FTC to investigate the airline industry amid questions about the use of "dynamic pricing," and the use of consumers' personal online data to set the price of airfares, which Schumer termed "a sad state of affairs that just might violate consumer protections."[27]

These practices are not restricted to the travel and airline industry. In 2012, an investigation by the Wall Street Journal found that Staples would quote a cheaper price to a consumer who lived near a competitor store.[28]And consumers are also steered to bad deals or poorer products through the use of algorithms. Online retailers like Amazon[29] have used algorithms to push consumers towards their own products, and those of companies that pay for its services, even when there were substantially cheaper offers for the same products available from other vendors on the site. This tactic is very effective: most Amazon shoppers end up adding the item that is highlighted to their cart.[30]

Dynamic pricing can lead to a loss of consumer power. When combined with excessive data collection practices and corporate consolidation, companies today have a greater ability to extract a relatively larger amount of consumer surplus for any given transaction. For instance, Uber and Lyft have been alleged to use data about individual users such as their phone's current battery charge[31] in order to assess how much the individual would be willing to pay for a ride. Indeed, these companies are not outliers in this practice. A recent report from Deloitte and Salesforce finds that 40 percent of brands that currently use artificial intelligence to personalize the consumer experience have used this technology to tailor prices and deals in real time.[32] And as we mentioned

---

RESEARCH (Oct. 2017), https://www.atpco.net/sites/default/files/2017-10/ATPCO%20PODS%20Dynamic%20Pricing_2.pdf.

[25] William J. McGee, *How to Get the Lowest Airfares*, CONSUMER REPORTS (Aug. 25, 2016), https://www.consumerreports.org/airline-travel/how-to-get-the-lowest-airfares/.

[26] *Id*.

[27] In the letter to the FTC, Senator Schumer cited recent news reports of airlines developing software that could track their potential customers' online browser histories and use that data to decide how much to charge them for a flight. *Consumers Union Praises Senator's Call for FTC Investigation go Airline "Dynamic Pricing"*, CONSUMERS UNION (Mar. 12, 2018), https://consumersunion.org/news/consumers-union-praises-senators-call-for-ftc-investigation-of-airline-dynamic-pricing/.

[28] Jennifer Valentino-DeVries, *et al*., *Websites Vary Prices, Deals Based on User's Information*, WALL ST. J. (Dec. 12, 2012), https://www.wsj.com/articles/SB10001424127887323777204578189391813881534.

[29] Julia Angwin & Surya Mattu, *Amazon Says It Puts Customers First. But Its Pricing Algorithm Doesn't*, PROPUBLICA (Sept. 20, 2016), https://www.propublica.org/article/amazon-says-it-puts-customers-first-but-its-pricing-algorithm-doesnt.

[30] *Id*.; *and*, *see*, BIG DATA AND DIFFERENTIAL PRICING, EXEC. OFFICE OF THE PRESIDENT (Feb. 2015), https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/docs/Big_Data_Report_Nonembargo_v2.pdf.

[31] Shankar Vedantam, *This is Your Brain on Uber*, NAT'L PUB RADIO (May 17, 2016), https://www.npr.org/templates/transcript/transcript.php?storyId=478266839.

[32] CONSUMER EXPERIENCE IN THE RETAIL RENAISSANCE, DELOITTE & SALESFORCE (2017),

above, these practices are obscured to the end user by design. As Maurice Stucke, Professor of Law at the University of Tennessee, notes, information about first-degree pricing practices typically "only comes out when there's a leak, when someone from the inside divulges it."

Consumers are also harmed through the use of differential pricing because companies can protect their market dominance through ensuring that consumers buy products or services sold by companies they have partnerships with.[33,34]

Consumer Awareness of Algorithms

Despite the fact that consumers are constantly seeing the results of algorithmic decision-making, in their feeds on social media platforms,[35] in their insurance premiums, and in the ads they are shown, consumers are largely unaware and unable to assess when an algorithm is at work. As Virginia Eubanks notes in her book, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*:

> But that's the thing about being targeted by an algorithm: you get a sense of a pattern in the digital noise, an electronic eye turned toward *you*, but you can't put your finger on exactly what's amiss. There is no requirement that you be notified when you are red-flagged. There is no sunshine law that compels companies to release the inner details of their digital fraud detection systems. With the notable exception of credit reporting, we have remarkably limited access to the equations, algorithms, and models that shape our life chances.[36]

Consumers are routinely the subject of algorithmic decisionmaking yet have no transparency as to their use or any recourse to challenge the decisions made about them. Algorithms warrant targeted enforcement and rulemaking precisely because of the opaque nature of their use, and because of the lack of current legal frameworks to assess and hold accountable algorithmic decision-making.

Lack of Applicable Federal Law and the Need for Algorithmic Accountability

Algorithms are increasingly being used to make life-impacting decisions (especially in employment decisions and in the criminal justice system), but they lack requisite auditing and accountability for their use. The vast majority of algorithmic decision-making is currently unregulated, not subject to any federal law. The United States lacks any federal laws that speak directly to the issues that the use of algorithms by government entities or by private actors pose; however, there are sector-specific laws that ban discrimination on the basis of race, sex, religion,

---

https://c1.sfdcstatic.com/content/dam/web/en_us/www/documents/e-books/learn/consumer-experience-in-the-retail-renaissance.pdf.

[33] For more on competition issues, please see Consumers Union's comments pertaining to antitrust: *Comments of Consumers Union—Antitrust and Competition Issues*.

[34] Arwa Mahdawi, *Is Your Friend Getting a Cheaper Uber Fare Than You Are?*, THE GUARDIAN (Apr. 13, 2018), https://www.theguardian.com/commentisfree/2018/apr/13/uber-lyft-prices-personalized-data.

[35] *See*, *e.g.*, Ethan Rakin, *Facebook is Changing Its News Feed—Here's How it Works and What You Need to Know*, BUS. INSIDER (Aug. 16, 2018), https://www.businessinsider.sg/facebook-changing-news-feed-how-it-works-what-you-need-to-know/.

[36] AUTOMATING INEQUALITY, *supra* note 9 at 5.

and other traits in the areas of housing,[37] employment,[38] and credit.[39] Although New York city recently-passed a law that creates a task force designed to give recommendations to the state regarding use of algorithms by state agencies,[40] this task force lacks any additional power to hold algorithms accountable. It is scheduled to release its report in late 2019.

We also lack sufficient technical safeguards for the use of algorithmic decision-making tools. While researchers have discovered several discriminatory effects noted above, in fact few algorithms and other scoring systems have been scientifically assessed. The risks of using algorithms to make important decisions about individuals are exacerbated by the flawed assumption that algorithms are scientific and inherently neutral:

> Their popularity relies on the notion they are objective, but the algorithms that power the data economy are based on choices made by fallible human beings. And, while some of them were made with good intentions, the algorithms encode human prejudice, misunderstanding, and bias into automatic systems that increasingly manage our lives. Like gods, these mathematical models are opaque, their workings invisible to all but the highest priests in their domain: mathematicians and computer scientists. Their verdicts, even when wrong or harmful, are beyond dispute or appeal. And they tend to punish the poor and the oppressed in our society, while making the rich richer.[41]

Finally, consumers also lack any means to correct erroneous conclusions made by algorithms, or any recourse to object to the use of an untested and undisclosed algorithm to make inferences or decisions about them.

Guidelines for Algorithmic Decision-making Tools

For these reasons, we urge the FTC to give guidance directing companies and organizations that use algorithms to do regular assessments of the accuracy of the algorithmic decisions, and to inspect the source code in order to root out any inherent or sample-bias that has been embedded in the algorithm.

Algorithms are used widely, without any accountability or consumer knowledge and control over their use, to make important, and sometimes life-changing, decisions about individuals. In order for consumers to be sufficiently protected, the FTC needs, and should request, additional authority

---

[37] FAIR HOUSING ACT, 42 U.S.C. § 3604(a), (f).

[38] TITLE VII OF THE CIVIL RIGHTS ACT OF 1964, 42 U.S.C. § 2000e-2(a)-(b); AGE DISCRIMINATION IN EMPLOYMENT ACT, 29 U.S.C. § 623(a); 29 U.S.C. § 623(e); AMERICANS WITH DISABILITIES ACT, 42 U.S.C. § 12112(a); and GENETIC INFORMATION NONDISCRIMINATION ACT, 42 U.S.C. § 2000ff et seq.

[39] EQUAL CREDIT OPPORTUNITY ACT, 15 U.S.C. § 1691(a). The Fair Housing Act applies to the issuing of mortgage loans. 42 U.S.C. § 3605(a)

[40] The law creates a task force that provides recommendations on how information on agency automated decision systems may be shared with the public and how agencies may address instances where people are harmed by agency automated decision systems. *A Local Law in Relation to Automated Decision Systems Used by Agencies, Int. 1696*, N.Y CITY COUNCIL (2017), *available at* http://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3137815&GUID=437A6A6D-62E1-47E2-9C42-461253F9C6D0.

[41] *How Algorithms Rule Our Working Lives*, *supra* note 11.

and resources to assess the use of algorithms and to require companies to provide easy means for correction of consumer data that is used in the algorithm. The Commission's authority should also include the ability to create rules requiring audits of algorithms and mandating in some cases some right of redress and human intervention. In the meantime, the Commission should craft guidelines for the use of algorithms to help determine whether a particular algorithm produces decisions that are fair, accurate and representative. To that end, any guidance, at a minimum, should include the following principles:

- **The use of algorithms should be transparent to the end users.** When algorithms make decisions about consumers the individual should have notice that an algorithm was used. In many cases, such as in the sorting of posts in a social media feed or in the prioritization of search results, this will be obvious and no dedicated notice will be necessary; but in some non-intuitive settings, companies should let consumers know when some decision-making relies on algorithmic evaluation.
- **Algorithmic decision-making should be testable for errors and bias, while still preserving intellectual property rights.** Algorithms should be able to be tested by outside researchers and investigators.[42] Opaque algorithms that have the ability to affect a large number of people in life-changing ways should be subject to higher scrutiny.[43] Using this assessment, algorithms used in life-altering situations, such as the employment process and in the creation of FICO and similar scores,[44,45] warrant greater scrutiny.

  Currently, the US lags behind on algorithmic transparency compared to our European counterparts:[46] The European Union incorporated algorithmic transparency and accountability into their new data privacy law: any decision based "solely on automated processing" which includes "legal effects" or "similarly significantly affects" an individual, be subject to "suitable safeguards," including an opportunity to obtain an explanation of an algorithmic decision, and to challenge such decisions."[47] France's president, Emmanuel Macron, pledged that the country will make all algorithms used by its governments open to the public.[48] And in June, the United Kingdom called for public

[42] *See*, *e.g.*, Lauren Kirchner, *Federal Judge Unseals New York Crime Lab's Software for Analyzing DNA Evidence*, PROPUBLICA (Oct. 20, 2017), https://www.propublica.org/article/federal-judge-unseals-new-york-crime-labs-software-for-analyzing-dna-evidence.

[43] WEAPONS OF MATH DESTRUCTION, *supra* note 14.

[44] For more on FICO scores and the interaction between data brokers and credit scoring agencies, please see Consumers Union response to Topic 2: *Competition and consumer protection issues in communication, information, and media technology networks*.

[45] Algorithms are used in state and local agencies across the country, including Arkansas: "Algorithmic tools like the one Arkansas instituted in 2016 are everywhere from health care to law enforcement, altering the ways people affected can usually only glimpse, if they know they're being used at all. Even if the details of algorithms are accessible, which isn't always the case, they're often beyond the understanding of the people using them, raising questions about what transparency means in an automated age, and concerns about people's ability to contest decisions made by machines." Colin Lecher, *What Happens When an Algorithm Cuts Your Health Care*, THE VERGE (Mar. 21, 2018), https://www.theverge.com/2018/3/21/17144260/healthcare-medicaid-algorithm-arkansas-cerebral-palsy. The article describes similar algorithmic tools used in other states, including California, Colorado, and Idaho. *See*, *also*, *Why New York*, *supra* note 6; *and*, NORTH CAROLINA GOVERNMENT DATA, *supra* note 7.

[46] Julia Angwin, *Making Algorithms Accountable*, PROPUBLICA (Aug. 1, 2016), https://www.propublica.org/article/making-algorithms-accountable.

[47] Art. 22, GENERAL DATA PRIVACY REGULATION, https://gdpr-info.eu/art-22-gdpr/.

[48] Nicholas Thompson, *Emmanuel Macron Talks to Wired about France's AI Strategy*, WIRED (Mar. 31, 2018),

sector entities to be transparent and accountable about their data practices and to "carefully consider the social implications of the data and algorithms used."[49]

- **Algorithms should be designed with fairness and accuracy in mind.** Companies should not simply rely on outsiders to detect problems with their algorithms; instead, companies should be required to plan for and design to avoid adverse consequences at all stages of the development of algorithms. Algorithms based on current data sets should be examined closely at the design stage in order to weed out historic discriminatory attitudes.[50] Algorithms can "inherit the prejudices of prior decision makers…in other cases, data may simply reflect the biases that persist in society at large."[51] To correct for sample size disparity that would disproportionately favor the creators or the majority of the data-set population, the data sets used in the algorithmic tool should be thoroughly assessed to root out any unintended bias towards any group.[52] Since algorithms and all data-driven products "will always reflect the design choices of the humans who built them,"[53] companies should commit to the further diversification of their employees.[54]
- **The data set used for algorithmic decision-making should avoid the use of proxies.** Algorithms can only serve to address the question posed to it. When possible, algorithms should avoid the use of unnecessary proxies like zip codes or credit scores that may be used to make discriminatory decisions against individuals. This problem persists even when the creators are trying to correct for unexpectedly biased results: "Even in situations where data miners are extremely careful, they can still [e]ffect discriminatory results with models that, quite unintentionally, pick out proxy variables for protected classes."[55] For instance,

---

https://www.wired.com/story/emmanuel-macron-talks-to-wired-about-frances-ai-strategy/.

[49] *Data Ethics Framework*, UK DEP'T FOR DIGITAL, CULTURE, MEDIA & Sport (June 13, 2018), https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework.

[50] The use of algorithms in the criminal justice sector sufficiently demonstrates the perils of using existing data sets to evaluate problems in a new way. "Our analysis of Northpointe's tool, called COMPAS [...] found that black defendants were far more likely than white defendants to be incorrectly judged to be at a higher rate of recidivism, while white defendants were more likely than black defendants to be incorrectly flagged as low risk[…]even when controlling for prior crimes." Jeff Larson, *et al.*, *How We Analyzed the COMPAS Recidivism Algorithm*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm. The risk assessment used by Northpointe was based on data that included items that can be correlated with race, such as poverty, joblessness, and social marginalization. Judges have used these scores in their sentencing decisions, despite the exacerbation of bias that the algorithm created. This algorithm, that was used to decide many individuals' fates, was not rigorously tested before use: "As often happens with risk assessment tools, many jurisdictions have adopted Northpointe's software before rigorously testing whether it works." Julia Angwin & Jeff Larson, *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[51] Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact,* 104 CALIF. LAW REV. 671 (2016), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899

[52] Organizations can available tools to test whether algorithms already in use and algorithms in the design stage have a discriminatory effect. Researchers are actively developing tools they hope companies and government agencies could use to test whether their algorithms yield discriminatory results and to fix them when necessary. *See*, *e.g.*, *Utah Computer Scientists Discover How to Find Bias in Algorithms*, UNIV. OF UTAH (Aug. 14, 2015), https://unews.utah.edu/programming-and-prejudice/. Cathy O'Neil also created a company that audits algorithms to see how biased they are. *See* O'NEIL RISK CONSULTING & ALGORITHMIC AUDITING, http://www.oneilrisk.com/ (last visited Aug. 17, 2018).

[53] Nanette Byrnes, *Why We Should Expect Algorithms to be Biased*, MIT TECH. REV. (June 24, 2016), https://www.technologyreview.com/s/601775/why-we-should-expect-algorithms-to-be-biased/.

[54] *See*, *e.g.*, Nitasha Tiku, *Google's Diversity Stats are Still Very Dismal*, WIRED (June 14, 2018), https://www.wired.com/story/googles-employee-diversity-numbers-havent-really-improved/.

[55] *Big Data's Disparate Impact*, *supra* note 51; Karen Levy & danah boyd, *Networked Rights and Networked Harms*,

a joint collaboration between Consumer Reports and ProPublica demonstrated that car insurance companies were using an individual's zip code as a proxy for race and class in order to discriminatorily charge customers in minority-majority neighborhoods a higher price for car insurance.[56]

- **Algorithmic decision-making processes that could have significant consumer consequences should be explainable.** In some cases, algorithms are programmed to learn or evolve over time, such that a developer might not know why certain inputs lead to certain results. This could lead to unfair results if there is no meaningful accountability for how decisions are made. If an algorithm is (1) used for a significant purpose, like the determination of a credit score[57] and (2) cannot be sufficiently explained, then the process should not be used.

———————

Thank you for the opportunity to comment on the important emerging technologies of algorithms, predictive analytics, and artificial intelligence. We look forward to reading the comments submitted, to following the hearings, and to further opportunities to assist the Commission in this and its other endeavors to protect the 21st Century marketplace and ensure that it works for consumers.

paper presented at the INT'L COMMC'N ASSOC.'S DATA & DISCRIMINATION PRECONFERENCE (May 14, 2014), http://www.datasociety.net/initiatives/privacyand-harm-in-a-networked-society/.

[56] *Auto Insurers Charging Higher Rates*, *supra* note 1.

[57] BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION?, FED. TRADE COMM'N (Jan. 2016), *available at* https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf. For this reason, the Fair Credit Reporting Act requires explainability today for credit determinations. However, other important determinations not covered by FCRA may be completely unregulated.

10. The interpretation and harmonization of state and federal statutes and regulations that prohibit unfair and deceptive acts and practices; and

For Consumers Union's comments on antitrust and competition issues pertaining to this topic please see: *Comments of Consumers Union—Antitrust and Competition Issues*.

11. The agency's investigation, enforcement, and remedial processes.

Antitrust

For Consumers Union's comments on antitrust and competition issues pertaining to this topic please see: *Comments of Consumers Union—Antitrust and Competition Issues*.

Consumer Protection

The most important reform to improve the Commission's investigation and enforcement processes would be to dramatically expand staffing. The Federal Trade Commission (FTC) should urge Congress to provide resources to bring on more staff to address litigation needs, provide technical expertise, and enable more frequent and thorough investigations.

Although the economy has doubled in size since the Ronald Reagan administration, the FTC has fewer employees today than it did in at that time.[1] Moreover, especially on privacy and security, other agencies are increasingly abdicating their own responsibilities and deferring authority to the FTC. For example, the Federal Communications Commission supported the Congressional repeal of its broadband privacy rules in order to put the FTC—the "expert" on privacy and security—in charge of policing internet service provider (ISP) misbehavior.[2] Similarly, last year the National Highway Traffic and Safety Administration declined to address privacy in its policy framework for automated vehicles, placing responsibility entirely with the FTC.[3]

Additionally, several observers have called on the FTC to litigate more cases in order to develop more robust case law on privacy and security (rather than developing norms through negotiated consent decrees).[4] In order to engage in additional litigation to protect consumers, the Commission will need more considerably more attorneys in order to meaningfully contest the practices of deep-pocketed multinational companies. Otherwise, a dictate to take more cases to court will severely hamstring the agency and limit each division to a handful of active cases at any given time.

In addition to privacy and litigation staff, the Commission also needs to substantially expand its technical expertise. The FTC has made important strides in recent years between the establishment of the Chief Technologist position advising the Chairman and the creation of the Office of Technology Research and Investigation (OTECH). Nevertheless, more is needed. OTECH currently only has a handful of technologists to support all five bureaus of the Consumer Protection Bureau; the Bureau of Competition has no analogous office to assist it. Given widespread concerns

---

[1] *Oral Testimony of Commissioner Rebecca Slaughter*, BEFORE THE SUBCOMM. ON DIGITAL COMMERCE & CONSUMER PROT., HOUSE COMM. ON ENERGY & COMMERCE (July 18, 2018), https://democrats-energycommerce.house.gov/committee-activity/hearings/hearing-on-oversight-of-the-federal-trade-commission-subcommittee-on.

[2] Ajit Pai & Maureen Ohlhausen, *No, Republicans Didn't Just Strip Away Your Internet Privacy Rights*, WASH. POST (Apr. 4, 2017), https://www.washingtonpost.com/opinions/no-republicans-didnt-just-strip-away-your-internet-privacy-rights/2017/04/04/73e6d500-18ab-11e7-9887-1a5314b56a08_story.html?utm_term=.b30dabcd3fb5.

[3] Joe Jerome, *NHTSA Automated Vehicle Guidance Punts Privacy to the FTC and Congress*, CTR. FOR DEMOCRACY & TECH. (Sept. 22, 2017), https://cdt.org/blog/nhtsa-automated-vehicles-guidance-punts-privacy-to-the-ftc-and-congress/.

[4] *E.g.*, David Bahr, *You Down to Reform the FTC—Yea, You Know Me!*, R ST. INST. (Dec. 2, 2017), https://www.rstreet.org/2017/12/07/you-down-to-reform-the-ftc-yea-you-know-me.

about concentration and anti-competitive practices in the technology sector, the lack of access to technologists is troubling. The FTC should urge Congress for resources to bring more technologists into the agency, potentially with the aim of developing a full-fledged Bureau of Technology.

Finally, in order to fulfill its ever-expanding mission, the Commission should also request Congress to grant it general rulemaking authority under Section 5 to give it the full panoply of tools to address emerging consumer protection threats. Many FTC critics have argued that a reasonableness standard for data security does not give companies sufficient guidance on what practices are required.[5] Similarly, the 11th Circuit in *LabMd* recently held that an order to develop a "reasonably designed" security program was vague and unenforceable.[6] In order to offer more clarity and certainty to companies as to what the law requires, the FTC should have the ability—certainly at least on data security—to engage in Administrative Procedure Act[7] rulemaking.

Respectfully submitted,

Justin Brookman
Director, Consumer Privacy
& Technology Policy

Katie McInnis
Policy Counsel

Consumers Union
1101 17th Street, NW
Suite 500
Washington, DC 20036

[5] Brief for TechFreedom *et al*. as AMICUS CURIAE, FTC V. WYNDHAM WORLDWIDE CORP., 10 F. Supp. 3d 602 (D.N.J. 2014), aff'd, 799 F.3d 236 (3d Cir. 2015); Gerard Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data Security Requirements*, 20 GEO. MASON L. REV. 673-720 (May 9, 2013), *available at* https://ssrn.com/abstract=2263037.
[6] LABMD, INC. V. FED. TRADE COMM'N, 894 F.3d 1221 (11th Cir. 2018).
[7] *See* 5 U.S.C. §§ 500-504.