



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

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's¹ 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.² The first is the online advertising industry which has been a significant focus for the Commission for nearly two decades.³ We describe how despite numerous calls for meaningful

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.

² *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>.

³ 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),

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.⁴ 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.⁵ In our view, the 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

<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/>.

⁴ 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>.

⁵ *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 U.S.C. §§801-808.

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,⁶ 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.⁷ Mozilla too has taken efforts to differentiate its Firefox web browser, by adopting policies to limit cross-site data collection.⁸ Services like DuckDuckGo have found some success in marketing themselves as the tracking-free alternative to larger companies that rely on data for advertising.⁹ 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.¹⁰ 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.¹¹

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 testing products under, the Digital Standard.¹² 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?¹³ While we are currently conducting case studies under the

⁶ 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.*

⁷ 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>.

⁸ 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>.

⁹ Apekshita Varshney, *Hey Google, DuckDuckGo Reached 25 Million Daily Searches*, TECHWEEK (June 4, 2018), <https://techweek.com/search-startup-duckduckgo-philadelphia/>.

¹⁰ *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>.

¹¹ 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/>

¹² 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.

¹³ *Id.*

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.¹⁴

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.¹⁵ 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.¹⁶ Over the next few years, 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.¹⁷ 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.

¹⁴ 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/>.

¹⁵ *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>.

¹⁶ Dawn Chmielecki, *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), <https://www.wsj.com/articles/SB10001424052970203960804577239774264364692>.

¹⁷ 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/>.

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...”¹⁸ Despite these concerns, the report also concluded that “current federal laws do not adequately safeguard Americans’ sensitive information.”¹⁹ 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.”²⁰ 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.”²¹ 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.²² In addition, as the examples detailed below demonstrate, there has been no clear examples of industry-wide plans to reform these data brokers’ practices.

¹⁸ *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/.

¹⁹ *Id.*

²⁰ DATA BROKERS, *supra* note 4, at 49.

²¹ 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.

²² *Reclaim Your Name*, FED. TRADE COMM’N (June 26, 2013), <https://loadtest.ftc.gov/public-statements/2013/06/reclaim-your-name>.

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).²³ For example, the FTC has taken action against the data broker Spokeo for its failure to comply with the FCRA.²⁴ The FCRA requires these companies to release the consumer's file to them upon request;²⁵ holds them to accuracy requirements;²⁶ and even places limits on with whom the information may be shared.²⁷ 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.²⁸

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."²⁹

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 barriers to consumer transparency. And the refusal by several major data broker companies to provide the Committee complete responses regarding data sources

²³ 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>.

²⁴ *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>.

²⁵ 15 U.S.C. § 1681g.

²⁶ 15 U.S.C. § 1681e.

²⁷ 15 U.S.C. § 1681b.

²⁸ S. 2155 (2018), available at <https://www.congress.gov/bill/115th-congress/senate-bill/2155>.

²⁹ CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY p.

152 (2016) [hereinafter WEAPONS OF MATH DESTRUCTION].

and customers only reinforces the aura of secrecy surrounding the industry.³⁰

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.³¹ 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.³² 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.³³ 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.³⁴ These assessments are not only privacy invasive, but also possibly incorrect.³⁵ 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.³⁶

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.³⁷ In 2011, the

³⁰ A REVIEW OF THE DATA BROKER INDUSTRY, *supra* note 21 at 36.

³¹ *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.

³² *People Searches & Data Brokers*, NAT'L NETWORK TO END DOMESTIC VIOLENCE (2013), <https://nnev.org/mdocs-posts/people-searches-data-brokers/>.

³³ *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>.

³⁴ *Id.*

³⁵ *Id.*

³⁶ *Id.*

³⁷ 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/.

hack of data broker Epsilon exposed the names and email addresses of millions of consumers who were then subjected to spam and targeted phishing attempts.³⁸ 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.³⁹

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.⁴⁰ (Adding insult to injury, many of these victims were "subsequently charged bank fees for emptying out their account or bouncing checks."⁴¹) 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.⁴² 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.⁴³

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.⁴⁴ 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.

³⁸ Brian Krebs, *Feds Indict Three in 2011 Epsilon Hack*, KREBSONSECURITY (Mar. 6, 2015), <https://krebsonsecurity.com/2015/03/feds-indict-three-in-2011-epsilon-hack/>.

³⁹ 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>.

⁴⁰ *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>.

⁴¹ WEAPONS OF MATH DESTRUCTION, *supra* note 29 at 82.

⁴² *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>.

⁴³ 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>.

⁴⁴ *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>.

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.⁴⁵ And Vermont recently 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.⁴⁶ 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.⁴⁷ 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.⁴⁸ 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.⁴⁹ 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.⁵⁰ Facebook has even patented an algorithm for using social media metrics and data to assess creditworthiness.⁵¹

⁴⁵ AB-375, CALIF. STATE LEGISLATURE, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 (last visited July 30, 2018).

⁴⁶ ACT 171: DATA BROKER REGISTRY ACT, VT. LEGISLATURE (May 2018), *available at* <https://legislature.vermont.gov/bill/status/2018/H.764>.

⁴⁷ 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.

⁴⁸ 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>.

⁴⁹ *Id.*

⁵⁰ 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>.

⁵¹ 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/>.

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.⁵² Most of the reports included multiple errors, including information that belonged to other people.⁵³ The participants also found it difficult to obtain the data.⁵⁴ 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 of the data they had collected about the consumer.⁵⁵ 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.⁵⁶

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,⁵⁷ 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.⁵⁸ 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."⁵⁹ 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.⁶⁰ When it comes to less-understood "health scores,"⁶¹ 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

⁵² BIG DATA, *supra* note 48, at 15.

⁵³ *Id.* at 18.

⁵⁴ *Id.* at 16-17.

⁵⁵ *Id.* at 18.

⁵⁶ *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>.

⁵⁷ MYFICO, WHAT'S IN MY FICO SCORES, <http://www.myfico.com/credit-education/whats-in-your-credit-score/>.

⁵⁸ 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.

⁵⁹ 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>.

⁶⁰ WEAPONS OF MATH DESTRUCTION, *supra* note 29 at 142-43.

⁶¹ The public is just beginning to understand "health scores," which was recently described in: *Health Insurers are Vacuuming Up Details About You*, *supra* note 33.

be used; although consumers have the right to correct some types of health information,⁶² 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,⁶³ particularly with regard to accuracy and transparency of information,⁶⁴ and the Equal Credit Opportunity Act with regard to disparate impact.⁶⁵ 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,⁶⁶ the broadband internet

⁶² 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.

⁶³ BIG DATA, *supra* note 48, at 33.

⁶⁴ *Id.* at 23-24.

⁶⁵ *Id.* at 28.

⁶⁶ *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->

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,⁶⁷ yet lack agency to effectuate their preferences due to a non-competitive ISP marketplace.⁶⁸

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.⁶⁹

embattled-over-privacy-warm-to-federal-regulation-1533547800.

⁶⁷ 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/>.

⁶⁸ 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, 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.

⁶⁹ 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/>.

Despite consumers' clearly expressed desire for these protections,⁷⁰ 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.⁷¹

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.⁷² 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.⁷³ Even when traffic is encrypted, ISPs still know the sites and services their customers use.

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.

⁷⁰ 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/>.

⁷¹ 5 U.S.C. § 801(b)(2).

⁷² See *supra* text accompanying note 68.

⁷³ See *What ISPs Can See*, UPTURN (Mar. 2016), <https://www.teamupturn.com/reports/2016/what-isps-can-see>.

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.⁷⁴ 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.⁷⁵ 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.

Respectfully submitted,

Justin Brookman
Director, Consumer Privacy
& Technology Policy

Katie McInnis
Policy Counsel

Consumers Union
1101 17th Street, NW
Suite 500

⁷⁴ 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 70.

⁷⁵ *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>.

Washington, DC 20036