December 21, 2018

Federal Trade Commission
Office of the Secretary
Constitution Center
400 7th Street SW
Washington, DC 20024

Re: Pre-Hearing Comments on Consumer Privacy for the Federal Trade Commission's Hearings on Competition and Consumer Protection in the 21st Century on February 12-13, 2019, FTC-2018-0098

Dear Sir or Madam:

Consumer Reports[1] writes to comment on the questions proposed for the February 12-13, 2019 hearing on consumer privacy hosted by the Federal Trade Commission (FTC or Commission).

General Questions

- What are the actual and potential benefits for consumers and to competition of information collection, sharing, aggregation, and use? To what extent do consumers today, or are consumers likely to, realize these benefits?

- What are the actual and potential risks for consumers and to competition of information collection, sharing, aggregation, and use? To what extent do consumers today, or are consumers likely to, realize these risks?

It is clear that consumers benefit from various commercial data processing activities; it would be impossible to enumerate all of those positive applications here. However, it is also important to recognize that all data collection activities also carry with it the potential for secondary misuse of that data to the consumer's detriment. Commission policy should recognize that as such consumers

[1] Consumer Reports is an expert, independent, nonprofit organization whose mission is to work for a fair, just, and safe marketplace for all consumers and to empower consumers to protect themselves. As the world's largest independent product-testing organization, it conducts its policy and mobilization work in the areas of privacy, telecommunications, financial services, food and product safety, and other areas. Using its dozens of labs, auto test center, and survey research department, the nonprofit organization rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 7 million members and publishes its magazine, website, and other publications.

may always have a legitimate reason to object to data collection practices.[2]

Consumers will always have a privacy *interest* in data collection, use, retention, or sharing because once private information is in the hands of another there is *always* a chance of some misuse. For example, data collected in the past could be publicly breached, accessed through mandatory legal process, or used for price discrimination to decrease a consumer's share of consumer surplus from any transaction.[3] From the perspective of the consumer, there is *necessarily* privacy risk when someone else has their data.

Consumers are already realizing the risks of data collection, storage, and use. One of the primary ways consumers have felt the effects of data collection and use is the resulting damage that follows when a company does not sufficiently protect consumer data and leaves data vulnerable to breach. It is clear from the never-ending spate of data breach incidents—many of which were preventable by basic security hygiene[4]—that a large number of companies are not sufficiently protecting the data under their control. And the failure to sufficiently protect the privacy and security of users injures consumers. This torrent of data breaches is concrete evidence that companies are not sufficiently internalizing risks of data exposure (even before the announcement of the Equifax data breach, a Pew poll in January of 2017 found that nearly two-thirds of Americans have experienced some sort of data theft[5]). And the harm from these data breaches are not only pervasive[6] but also

---

[2] "Consumers who don't want to be monitored all the time may be resistant to adopting new technologies; indeed, the Obama administration used this as an explicit commercial justification in calling for the enactment of comprehensive commercial privacy protections. More fundamentally, however, citizens who fear that they are being constantly observed may be less likely to speak and act freely if they believe that their actions are being surveilled. People will feel constrained from experimenting with new ideas or adopting controversial positions. In fact, this constant threat of surveillance was the fundamental conceit behind the development of the Panopticon prison: if inmates had to worry all the time that they were being observed, they would be less likely to engage in problematic behaviors." Justin Brookman & G.S. Hans, *Why Collection Matters: Surveillance as a De Facto Privacy Harm*, FUTURE OF PRIVACY FORUM BIG DATA & PRIVACY WORKSHOP PAPER COLLECTION (2013), https://fpf.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf.

[3] Justin Brookman & G.S. Hans, *Why Collection Matters: Surveillance as a De Facto Privacy Harm*, FUTURE OF PRIVACY FORUM BIG DATA & PRIVACY WORKSHOP PAPER COLLECTION (2013), https://fpf.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf.

[4] *90% of Data Breaches are Avoidable*, ONLINE TRUST ALLIANCE (Feb. 2, 2012), https://www.cybersecurityintelligence.com/blog/90-of-data-breaches-are-avoidable-1003.html ("Ninety one percent of data breaches that occurred from January to August of 2015 could have easily been prevented using simple and well-established security practices, such as applying software patches to a server, encrypting data or ensuring employees do not lose their laptops…"); *see, e.g.*, Meghan Kloth Rohlf, *Yahoo Data Breaches: A Lesson in What Not to Do*, LEXOLOGY (March 2, 2017), https://www.lexology.com/library/detail.aspx?g=cdf1c89f-75bf-4524-8e3e-6425529a7349 ("...in 2013, when the first data breach occurred, Yahoo was still using a discredited technology for data encryption known as MD5. The weaknesses of MD5 had been known by security experts and hackers for more than a decade and public warnings had been issued advising that MD5 was "unsuitable for future use.""); Lily Hay Newman, *Equifax Officially Has No Excuse*, WIRED (Sept. 14, 2017), https://www.wired.com/story/equifax-breach-no-excuse/ ("...Equifax has confirmed that attackers entered its system in mid-May through a web-application vulnerability that had a patch available in March").

[5] Kenneth Olmstead & Aaron Smith, *Americans and Cybersecurity*, PEW RESEARCH CTR. (Jan. 26, 2017), http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/.

[6] 86% of identity theft victims experienced the fraudulent use of existing account information. Erika Harrell, *Victims*

expensive (in 2016 alone, the Department of Justice found that the estimated cost of identity theft amounted to $15.4 billion).[7]

In addition, 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."

When dynamic pricing is 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[8] 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.[9] And 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.[10]

In addition, consumer information is routinely fed into algorithms that are used to make decisions about the consumer, often without the consumer's knowledge or control. In this situation, consumers are harmed not only in the collection of their information but also in the use of their information to make decisions about them that may be incorrect or inaccurate and also not open to redress or correction. Algorithms are routinely used to determine insurance rates,[11]

---

of Identity Theft, BUREAU OF JUSTICE STATISTICS (Sept. 27, 2015), https://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408.

[7] *Id*.

[8] 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.

[9] CONSUMER EXPERIENCE IN THE RETAIL RENAISSANCE, DELOITTE & SALESFORCE (2017), https://c1.sfdcstatic.com/content/dam/web/en_us/www/documents/e-books/learn/consumer-experience-in-the-retail-renaissance.pdf.

[10] 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.

[11] *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-

creditworthiness,[12] willingness to pay,[13] and employment prospects.[14] In addition, algorithmic tools are employed to: serve search engine results;[15] match children with schools;[16] detect employment,[17] healthcare, and Medicaid fraud[18] (sometimes erroneously[19]); and identify biometric markers.[20] Unfortunately, despite the notion that algorithms are neutral and objective arbiters, algorithms can exacerbate bias or have unexpected discriminatory effects, as numerous examples have demonstrated.[21]

Despite lacking effective privacy controls, consumers deeply care about their privacy and wish to limit the amount of data collected about them. Consumer Reports' 2015 survey showed that 88

---

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.

[12] *Understanding Credit Score Algorithms*, AMPLIFY (Dec. 8, 2017), https://www.goamplify.com/blog/improvecredit/understanding-credit-score-algorithms.aspx.

[13] *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/.

[14] 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.

[15] 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.

[16] 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/.

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

[18] 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.

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

[20] 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.

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

percent of individuals say it is important that they not have someone watch or listen to them without their permission.[22] A Mozilla study found that a third of people feel like they have no control of their information online;[23] 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."[24] The majority of consumers (74 percent) find it is "very important" to be in control over who can get information about them.[25] 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 about them.[26] 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."[27] 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.[28] These concerns are even prompting some Americans to limit their online activity.[29]

- The use of "big data" in automated decisionmaking has generated considerable discussion among privacy stakeholders. Do risks of information collection, sharing, aggregation, and use include risks related to potential biases in algorithms? Do they include risks related to use of information in risk scoring, differential pricing, and other individualized marketing practices? Should consideration of such risks depend on the accuracy of the underlying predictions? Do such risks differ when data is being collected and analyzed by a computer

---

[22] 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/.

[23] *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.

[24] 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/.

[25] *See Americans' Attitudes*, *supra* note 22.

[26] *Id*.

[27] 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/.

[28] 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.

[29] *Id*.

rather than a human?

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 Commission more authority and resources to create rules for the use of algorithms in light of insufficient applicable federal and state law.

Algorithms are routinely used to determine insurance rates,[30] creditworthiness,[31] willingness to pay,[32] and employment prospects.[33] In addition, algorithmic tools are employed to: serve search engine results;[34] match children with schools;[35] detect employment,[36] healthcare, and Medicaid fraud[37] (sometimes erroneously[38]); and identify biometric markers.[39] Unfortunately, despite the

---

[30] *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.
[31] *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*.
[32] *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/.
[33] 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.
[34] 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.
[35] 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/.
[36] *See*, *e.g.*, NORTH CAROLINA GOVERNMENT DATA ANALYTICS CENTER, NC IT, https://it.nc.gov/services/nc-gdac (last visited Aug. 17, 2018).
[37] 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.
[38] VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR, p. 5 (2018) [hereinafter AUTOMATING INEQUALITY].
[39] *How Fingerprint Scanners*, *supra* note 20; *Facial Recognition Technology*, *supra* note 20. *How Facial Recognition Algorithm Works*, *supra* note 20.

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.[40] 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).[41]

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,"[42] 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."[43]

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.[44] 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.[45] 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."[46]

---

[40] *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.

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

[42] NEW DISTRIBUTION CAPABILITY, IATA, https://www.iata.org/whatwedo/airline-distribution/ndc/Pages/default.aspx (last visited Aug. 17, 2018).

[43] *Advances in Airline Pricing, Revenue, Management, and Distribution: Implications for the Airline Industry*, PODS RESEARCH (Oct. 2017), https://www.atpco.net/sites/default/files/2017-10/ATPCO%20PODS%20Dynamic%20Pricing_2.pdf.

[44] 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/.

[45] *Id*.

[46] 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"*, CONSUMER REPORTS

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.[47]And consumers are also steered to bad deals or poorer products through the use of algorithms. Online retailers like Amazon[48] 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.[49]

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[50] 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.[51] And as we mentioned 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.[52]

Lack of Applicable Federal Law and the Need for Algorithmic Accountability

---

(Mar. 12, 2018), https://consumersunion.org/news/consumers-union-praises-senators-call-for-ftc-investigation-of-airline-dynamic-pricing/.

[47] 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.

[48] 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.

[49] *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.

[50] 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.

[51] *Consumer Experience in the Retail Renaissance*, DELOITTE & SALESFORCE (2017), https://c1.sfdcstatic.com/content/dam/web/en_us/www/documents/e-books/learn/consumer-experience-in-the-retail-renaissance.pdf.

[52] 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.

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, and other traits in the areas of housing,[53] employment,[54] and credit.[55] 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,[56] 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.[57]

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.

---

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

[54] 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.

[55] 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)

[56] 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.

[57] *How Algorithms Rule Our Working Lives*, *supra* note 40.

- Should privacy protections depend on the sensitivity of data? If so, what data is sensitive and why? What data is not sensitive and why not?

Consumer Reports advocates for a system of data classification that depends on context and reasonable expectations rather than a system that could work to deny some data less protection than others. Consumers' interests in their personal information are contextual and case- and individual-specific. As a result, it is challenging—and indeed inappropriate—for regulators to prescriptively identify and classify the sensitivity of data, especially since evolving techniques make it possible to extract more and better information from seemingly innocuous data. Section 5 of the Federal Trade Commission Act was conspicuously crafted to apply to a broad and evolving array of consumer protection concerns.[58] For these reasons, we encourage authorities like the FTC to focus on user expectations of how their data will be collected, stored, used, and shared rather than a third-party assessment of whether or not a user would say that information is sensitive. While the sensitivity of the data may be relevant for a few narrow inquiries, e.g., to ensure reasonable security and assessing penalties, for other data governance issues, like data minimization, transparency, access, and control, there is no need to distinguish between personal and non-personal data.

Furthermore, consumer surveys demonstrate a concern with who has information about them at all, no matter the kind of data being tracked. The majority of consumers (74 percent) find it is "very important" to be in control of who can get information about them.[59] 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 about them.[60] Indeed, this is not a new sentiment for consumers: a Pew research poll in 2014 found that 91% of adults "'agree' or 'strongly agree' that consumers have lost control over how personal information is collected and used by companies."[61] Consumers desire the ability to limit access to their information, but lack the means to protect themselves and their privacy given the paucity of effective tools at their disposal. Indeed, the response to the Cambridge Analytica incident shows that consumers care about who has access to their data, even if it is information they will willingly share with a trusted party: 74 percent of Facebook users adjusted their privacy settings, taken a break from the platform for several weeks or more, or deleted the Facebook app from their phone "following revelations that the former consulting firm Cambridge Analytica had collected data on tens of millions of Facebook users without their knowledge."[62]

---

[58] *Petitioner's brief*, FEDERAL TRADE COMMISSION V. WYNDHAM WORLDWIDE CORP., 799 F.3d 236 (3rd Cir. 2015) ("Although Congress did not foresee modern electronic commerce when it enacted the relevant provisions of the FTC Act, it understood that threats to consumer welfare would evolve rapidly as the worlds of business and technology. It thus wrote Section 5 in open-ended terms, granting the FTC broad authority to pursue unfair practices across a broad range of economic contexts.").

[59] *See Americans' Attitudes*, supra note 22.

[60] *Id*.

[61] *Public Perceptions*, *supra* note 27.

[62] Andrew Perrin, *Americans are Changing their Relationship with Facebook*, PEW RESEARCH CTR. (Sept. 5, 2018), http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/.

- Should privacy protection depend on, or allow for, consumer variation in privacy preferences? Why or why not? What are the appropriate tradeoffs to consider? If desired, how should this flexibility be implemented?

Privacy protections should certainly allow for consumer variation in privacy preferences. However, default protections should accord to reasonable consumer expectations in order to lessen overall consumer frustration. Consumer expectations are already not being respected in some areas of the market, leading to poor outcomes.[63] For instance, consumer dissatisfaction with available controls have led to decreased confidence in social media companies and decreased use of these products.[64] Companies should provide options that allow consumers to access trade-offs for sharing more data with the service provider. The individual should be empowered to assess the trade-offs and their own privacy preferences. People are increasingly taking privacy considerations[65] into account when making market choices. A desire for occasional seclusion and some control over personal information are core human values, and sometimes consumers might want to demand some assurances from companies they interact with about how their information is going to be treated. However, others might think those personal choices are unnecessary—they might argue that personalized advertising is completely benign, that total surveillance is both inevitable and desirable,[66] and that consumers should have no reason to try and limit data collected about them.

But each consumer should have the ability to make the privacy decision that is best for them; individuals should be free to value considerations such as their own privacy however they want. In economics, this idea is called *utility*—the degree of subjective satisfaction that an individual derives from certain choices. Privacy law should—at the very least—encourage greater transparency about privacy practices so consumers can make their own determinations about the value of their privacy. If companies violate these privacy promises that are contained in transparent disclosures, regulators should not engage in a cost-benefit analysis to determine if the consumer was really harmed by the transfer of their personal information; rather, the issue should be assessed as deception. Consumer protections to should not be tethered to subjective assessments of privacy *risk* and *harm*. Rather, the Commission should look to consumer expectations in order to assess whether the company's actions contravened consumer expectations and privacy controls. In addition, since consumers are navigating an increasingly non-competitive marketplace and thus lack the choices necessary to fully express their privacy preferences. Since consumers lack effective alternatives and choices, they depend on groups like the FTC proscribing generally

---

[63] According to a recent report by the American Customer Satisfaction Index (ACSI), consumers now trust health insurers and airline companies more than they trust social media companies. *E-Business Report, 2018*, AMERICAN CUSTOMER SATISFACTION INDEX (June 24, 2018), https://www.theacsi.org/news-and-resources/customer-satisfaction-reports/reports-2018/acsi-e-business-report-2018/

[64] *Americans are Changing their Relationship with Facebook*, *supra* note 62.

[65] *Americans' Attitudes*, *supra* note 22.

[66] *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*, EXEC. OFFICE OF THE PRESIDENT (May 2016), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.

objectionable data practices in order to protect consumers.

- Market-based injuries can be objectively measured—for example, credit card fraud and medical identity theft often impact consumers' finances in a directly measurable way. Alternatively, a "non-market" injury, such as the embarrassment that comes from a breach of sensitive health information, cannot be objectively measured because there is no functioning market for it. Many significant privacy violations involve both market and non-market actors, sources, and harms. Should the Commission's privacy enforcement and policy work be limited to market-based harms? Why or why not?

The Commission's unfairness enforcement for privacy cases should not be limited to instances of financial harm.[67] And indeed, such financial harms can be hard to assess since it is difficult to trace harm back to one breach or another. However, consumers can experience a wide range of harms as a result of companies subverting consumer choice or overreaching into the personal information about consumers. As we noted above, Section 5 of the Federal Trade Commission Act was conspicuously crafted to apply to a broad and evolving array of consumer protection concerns. For these reasons, we encourage an expansive definition of what could constitute an injury to consumers that includes market and non-market harms.

The Commission has acted to protect consumers against harms that involve non-market harms in the past, especially in the arena of harms caused by unwarranted intrusion.[68] 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.[69] In robocall cases, machine-generated telephone solicitations are invading consumer's homes and privacy.[70] And in a series of cases involving *Aaron's* rent-to-own computers, the companies enabled spyware on the rentals that monitored computers in their homes.[71] These types of practices are all harmful and highly invasive, and should be viewed as actionable injury under the FTC Act, despite the fact that many of the harms contained within these cases are not necessarily market-based harms.

---

[67] Moreover, "harm" is not an element to be proven in the Commission's deception cases; providing misinformation to the marketplace about the terms of a transaction is sufficient rationale to justify Commission intervention on behalf of consumers.

[68] In her September 2017 speech, then-Acting Chairman Maureen Ohlhausen identified five types of consumer informational injury: deception injury or subverting consumer 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.

[69] *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.

[70] Maureen Mahoney, *Fed Up with Robocalls? Here's What You Can Do Right Now*, CONSUMER REPORTS (July 21, 2017), http://consumersunion.org/campaign-updates/fed-up-with-robocalls-heres-what-you-can-do-right-now/.

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

In addition, just as effective digital security is a community effort,[72] effective privacy protection depends on group coordination.[73] Individual control and empowerment over data is not sufficient to control for the perversion of consumer choice and control that results from an individual sharing details about another. In addition, the need for community protection of privacy is especially true in the area of big data where highly accurate conclusions can be drawn about one person based on the data of many other similar people. As Joshua A. T. Fairchild and Christoph Engel argue in their article *Privacy as a Public Good*:

> Individual empowerment is not enough because an individual's disclosure of information about herself impacts many other people. One source of risk is immediate and palpable—information about one person is also information about others.[74] If a machine learning algorithm knows where someone is at a given time, it can predict where a spouse or friend is as well. Another source of risk is remote and concealed, but potentially even more dangerous. Big data companies collect large amounts of information about everyone.[75] They then mine this data for patterns.[76] A single cue may facilitate an inference regarding information an individual has chosen not to reveal, or perhaps even something she did not know about herself. For instance, imagine paying higher insurance premiums because a sibling has cancer, or because a parent posts something about his heart disease, or a relative self-identifies as suffering from a particular mental illness.[77]Alternatively, imagine not receiving a job offer because an algorithm has identified that the distance an employee lives from work strongly correlates with higher turnover.[78,79]

---

[72] One great example of this is the necessity for connected devices to be secure in order to avoid a DDoS attack like Marai botnet attack in 2016. Nick Statt, *How an Army of Vulnerable Gadgets Took Down the Web Today*, THE Verge (Oct. 21, 2016), http://www.theverge.com/2016/10/21/13362354/dyn-dns-ddos-attack-cause-outage-status-explained.

[73] *See* Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1927 (2013) ("Privacy rights protect individuals, but to understand privacy simply as an individual right is a mistake. The ability to have, maintain, and manage privacy depends heavily on the attributes of one's social, material, and informational environment.").

[74] *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1939 (2013) ("Big Data is notable not just because of the amount of personal information that can be processed, but because of the ways data in one area can be linked to other areas and produce new inferences and findings.").

[75] *See* Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 I/S: J.L. & POL'Y FOR INFO. SOC'Y 425, 431 (2011) ("[T]he biggest dangers associated with online behavioral advertising might come from the possible secondary use of the profiles and analytics constructed to enable targeted advertising.").

[76] *See* Richards, *supra* note 74, at 1939 ("Big Data is fundamentally networked. Its value comes from the patterns that can be derived by making connections between pieces of data, about an individual, about individuals in relation to others, about groups of people, or simply about the structure of information itself."); Jordan Ellenberg, *What's Even Creepier than Target Guessing that You're Pregnant?*, SLATE (June 9, 2014), http://www.slate.com/blogs/how_not_to_be_wrong/2014/06/09/big_data_what_s_even_creepier_than_target_guessing_that_you_re_pregnant.html [http://perma.cc/E68S-UP4C].

[77] *See* MacCarthy, *supra* note 75, at 450 ("If a data collector knows the independent variable in that circumstance, it can use the regularity to infer the presence of the dependent variable, even when the people involved have not revealed the presence of that characteristic and it cannot be found in public records.").

[78] *See id*. at 450–51 (discussing how big data impacts eligibility decisions).

[79] Joshua A. T. Fairchild & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L. J. 385 (2015), *available at* https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3824&context=dlj.

Furthermore, the need for privacy to be protected at the community level is especially pressing due to the tendency of consumers to trade away their friends' privacy for a short-term benefit.[80] The Cambridge Analytica scandal also demonstrates how privacy protections can depend on the actions of others: an app installed by 300,000 people let the firm access their friends' data too, thus increasing the number of people's information that was shared to more than 50 million people.[81] For the foregoing reasons, the FTC should not constrain their enforcement powers to a narrow conception of financial harms, as that method would overlook the many other ways consumers' privacy is invaded to consumers' detriment.

- In general, privacy interventions could be implemented at many different points in the process of collecting, processing, and using data. For example, certain collections could be banned, certain uses could be opt-in only, or certain types of processing could trigger disclosure requirements. Where should interventions be focused? What interventions are appropriate?

Consumer Reports supports the use of minimization of the data collected from the consumer in the first instance as a primary driver of giving consumers back context and control and place force collection to occur in context. Data minimization, done correctly, would redistribute the onus of good data practices onto the company and off of the consumer. Consumers are already overwhelmed with the number of decisions they are asked to make. Consumers should be empowered to use products without fear that the service or product will mine and collect more data than the consumer would reasonably expect. Ever-present pop-up dialogs and byzantine user controls do not serve users well; instead, consumers should be entitled to expect that data collection and sharing will be limited to the context of their interactions with any given company.

Specifically, a business that collects a consumer's personal information should limit its collection and sharing of personal information with third parties to *what is reasonably necessary to provide a service or conduct an activity that a consumer has requested*. Additional data collection or sharing should only happen with a user's clear and informed permission. Such a principle could have narrow exceptions—such as allowing collection or sharing as is reasonably necessary for security or fraud prevention. Additionally, some related, operational processing of already-collected data should be allowed without bothering the user for permission—such as first-party analytics, research, and marketing.[82] However, if a company wants to engage in out-of-context

[80] An experiment by Susan Athey, Christian Catalini, and Catherine Tucker found that people who profess concern about privacy will provide emails of their friends in exchange for some pizza. Susan Athey, *et al.*, *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk*, STANFORD (Feb. 13, 2017), https://athey.people.stanford.edu/sites/g/files/sbiybj5686/f/digital_privacy_paradox_02_13_17.pdf.

[81] Laura Hautala, *Facebook Privacy Settings Make You Work to Stop the Data Sharing*, CNET (Mar. 22, 2018), https://www.cnet.com/news/how-to-stop-sharing-facebook-data-after-cambridge-analytica-mess/.

[82] However, due to the breadth of the security/fraud exception and the potential for this exception swallowing the rule, data collected or retained solely for security or fraud prevention should not be used for related operational purposes.

data collection or sharing, it should make a clear and compelling case to the consumer and only proceed with permission. An opt-out approach is inconsistent with consumer demands and expectations.

- Should policymakers and other stakeholders attempt to improve accountability for privacy issues within organizations? Why or why not? If so, how? Should privacy risk assessments be mandated for certain companies? Should minimum standards in privacy protections be required?

- How can firms that interface directly with consumers foster accountability of third parties to whom they transfer consumer data?

Consumer-facing companies should identify contractors and recipients of user data as much as reasonably practicable in order to foster accountability. However, if this higher standard cannot be met, companies need to identify the categories of contractors and recipients of data. Whether or not the companies disclose such information, they still have a duty to exercise reasonable care in selecting and monitoring the third parties to which they transfer consumer data.

- What are the effects, if any, on competition and innovation from privacy interventions, including from policies such as data minimization, privacy by design, and other principles that the Commission has recommended?

Competition and innovation do not depend on unregulated data collection and use. Some of the biggest actors on the internet established their market dominance through methods other than poor privacy practices: Google is funded primarily through first-party contextual advertising (search ads); Facebook grew based on first-party ads (as the privacy-friendly alternative to MySpace); and Amazon and Apple established themselves as sellers of products. None of these business models are inconsistent with data collection practices that are tethered to reasonable expectations. Contrary to claims from the ad industry and others, dialing back the level of consumer tracking will not prevent companies from profiting from their web presence.

Furthermore, the notion that privacy interventions, a.k.a. privacy protections, will work to entrench Google and Facebook is belied by the fact that Google and Facebook have consistently lobbied aggressively against nearly all proposed privacy legislation in both the United States and Europe.[83]

This approach to consumer data dovetails with Professor Jack M. Balkin's concept of "information fiduciaries" in which the company must be loyal to the consumer's interests and show a duty of care to the data collected. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, FACULTY SCHOLARSHIP SERIES 5154 (2016), https://digitalcommons.law.yale.edu/fss_papers/5154.

[83] And have been the target of investigations by the EU already following the implementation of the GDPR. Catalin Cimpanu, *Facebook Sued Hours After Announcing Security Breach*, ZDNET (Oct. 1, 2018), https://www.zdnet.com/article/facebook-sued-hours-after-announcing-security-breach/; Charlie Osborne, *Facebook Faces £500,000 fine in UK over Cambridge Analytica Scandal*, ZDNET (July 11, 2018),

In the past similar arguments were used to caution against the adoption of Do Not Track; 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' do-not-track 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, and should, especially impact them, and will probably 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.

Finally, an effective privacy law should not simply mandate processes and compliance programs. Fundamentally, privacy law should accord behaviors with consumer's reasonable expectations; if a small business is not engaged in dubious data practices, it should not be impacted by new privacy protections as much as a larger player like Google or Facebook.

- Do firms incur opportunity costs as a result of increased investments in privacy tools? If so, what are the tradeoffs between functionality, innovation, and security and privacy protections at the design level?

All considerations involved trade-offs. But while companies are incentivized to take functionality and innovation into consideration, they are not likewise incentivized to prioritize privacy and security (and they can free-ride on consumers' inability to make privacy- and security-conscious choices). Therefore, policy should encourage companies to consider those other utility-enhancing elements as well. And although a company may face a small opportunity cost for developing a privacy tool rather than innovating in another sector, the costs of *not* providing consumers with effective privacy tools, while also collecting data about those consumers, are much greater.

For instance, in 2016 the rideshare app Uber released an update that allowed the app to track users' locations for at least five minutes after their Uber ride had actually ended (if not constantly) without giving consumers nuanced controls to limit this tracking.[84] After sustained public outcry, the company finally eliminated the feature in an update in mid-2017.[85] And this issue and others have

---

https://www.zdnet.com/article/uk-watchdog-to-give-facebook-500000-fine-over-data-scandal/; Tom Jowitt, *Google Faces Multiple GDPR Complaints over Location Tracking*, SILICON (Nov. 28, 2018), https://www.silicon.co.uk/e-regulation/surveillance/google-gdpr-complaints-location-tracking-239291?inf_by=5c1bf106671db85d3e8b5613.
In addition, Facebook's many privacy mishaps have led to investigations from state Attorneys General. Rhett Jones, *DC Attorney General Hits Facebook with Major Cambridge Analytica Lawsuit*, GIZMODO (Dec. 19, 2018), https://gizmodo.com/dc-attorney-general-hits-facebook-with-major-cambridge-1831206719.

[84] Andrew J. Hawkins, *Uber Wants to Track Your Location Even When You're Not Using the App*, THE VERGE (Nov. 30, 2016), https://www.theverge.com/2016/11/30/13763714/uber-location-data-tracking-app-privacy-ios-android.

[85] Dustin Volz, *Uber to End Post-Trip Tracking of Riders as Part of Privacy Push*, REUTERS (Aug. 29, 2017), https://www.reuters.com/article/us-uber-privacy/uber-to-end-post-trip-tracking-of-riders-as-part-of-privacy-push-idUSKCN1B90EN.

led to a decline in the number of Uber users.[86] Facebook is a another prime example of the consequences companies can incur for the failing to provide their users effective privacy controls or tools. Facebook has faced, and is facing, sustained public condemnation of their products and services as a result of their numerous issues[87] in protecting consumer privacy and data. Backlash[88] over these issues led to a dramatic decrease in use of the social media platform in 2018.[89] Indeed, Facebook has received criticism for delays in deploying privacy tools or for bugs in the privacy tools they did provide. For example, Facebook has continued to delay the release of their Clear History feature, that was first promised to consumers in May 2018, until "spring of 2019."[90] And in June 2018, while assessing the design and language used in Facebook's privacy controls that nudge people toward sharing the maximum amount of data with the company,[91] researchers at Consumer Reports found a bug in the Ad Preferences settings that could possibly confuse consumers.[92] This bug was later fixed by Facebook after Consumer Reports brought it to their attention,[93] but the bug and dark patterns utilized by Facebook worked to undermine their repeatedly promised reforms that would "put people more in control of their privacy."[94]

---

[86] Rani Molla, *Uber's Market Share has Taken a Big Hit*, Recode (Aug. 31, 2017), https://www.recode.net/2017/8/31/16227670/uber-lyft-market-share-deleteuber-decline-users.

[87] In reverse chronological order: Bree Fowler, *Facebook Bug Allowed Access to Millions of Private Photos*, CONSUMER REPORTS (Dec. 14, 2018), https://www.consumerreports.org/holiday-season/facebook-bug-allowed-access-to-millions-of-private-photos/; Zach Whittaker, *Facebook Bug Let Websites Read 'Likes' and Interests from a User's Profile*, TECHCRUNCH (Nov. 13, 2018), https://techcrunch.com/2018/11/13/facebook-bug-website-leak-likes-interests-profile/; Lily Hay Newman, *How Facebook Hackers Compromised 30 Million Accounts*, WIRED (Oct. 12, 2018), https://www.wired.com/story/how-facebook-hackers-compromised-30-million-accounts/; Josh Constine, *Facebook Mistakenly Deleted Some People's Live Videos*, TECHCRUNCH (Oct. 11, 2018), https://techcrunch.com/2018/10/11/facebook-deleted-live-videos/; Josh Constine, *Facebook Alerts 14M to Privacy Bug that Changed Status Composer to Public*, TECHCRUNCH (June 7, 2018), https://techcrunch.com/2018/06/07/facebook-status-privacy-bug/; *Revealed: 50 Million Facebook Profiles Harvest for Cambridge Analytica in Major Data Breach*, THE GUARDIAN (Mar. 17, 2018), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[88] In reverse chronological order: *See, e.g.*, Casey Newton, *Facebook Keeps Asking for Our Trust even as it Loses Control of Our Data*, THE VERGE (Oct. 13, 2018), https://www.theverge.com/2018/10/13/17971346/facebook-data-breach-portal-trust-credibility; Charlie Warzel, *Facebook Doesn't Deserve Your Information*, BUZZFEED NEWS (Oct. 12, 2018), https://www.buzzfeednews.com/article/charliewarzel/facebook-doesnt-deserve-your-information; Seth Fiegerman, *Congress Grilled Facebook's Mark Zuckerberg for Nearly 10 Hours. What's Next?*, CNN (Apr. 12, 2018), https://money.cnn.com/2018/04/12/technology/facebook-hearing-what-next/index.html; *Facebook Privacy Settings Make You Work to Stop the Data Sharing*, *supra* note 81.

[89] *Americans are Changing their Relationship with Facebook*, *supra* note 62.

[90] Jon Fingas, *Facebook's 'Clear History' Tool Won't Arrive Until Spring 2019*, ENGADGET (Dec. 17, 2018), https://www.engadget.com/2018/12/17/facebook-browsing-history-control-delayed/.

[91] *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy*, NORWEGIAN CONSUMER COUNCIL (June 27, 2019), https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

[92] 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/.

[93] Allen St. John, *Facebook Fixes Privacy Bug Spotted by Consumer Reports*, CONSUMER REPORTS (July 19, 2018), https://www.consumerreports.org/privacy/facebook-changes-settings-after-cr-investigation/.

[94] *It's Time to Make Our Privacy Tools Easier to Find*, FACEBOOK NEWSROOM (Mar. 28, 2018), https://newsroom.fb.com/news/2018/03/privacy-shortcuts/.

Facebook has also been the subject of public censure for their perversion of the few and imperfect privacy controls they do provide users. On December 18, 2018, the *New York Times* released an investigation detailing how the social media platform shared and provided access to private user information including private, direct messages, device identifiers, complete lists of users' friends, to companies like the Canadian Royal Bank, Amazon, Netflix, and Spotify without obtaining the consumers' consent for this sharing.[95] Although these revelations will be examined by regulators considering possible enforcement actions in the days and weeks to come, Facebook is already facing consequences as a result of these poor practices: "Facebook's stock price has fallen, and a group of shareholders has called for Mr. Zuckerberg to step aside as chairman. Shareholders also have filed a lawsuit alleging that executives failed to impose effective privacy safeguards. Angry users started a #DeleteFacebook movement."[96] By providing consumers with *effective* controls, companies can prevent the need to respond to scandals like Facebook's and conserve resources and time to instead devote to new projects and tools rather than responding to angry users.

However, with regards to a data protection law, any effective statute needs to pair substantive requirements with strong enforcement in order to sufficiently protect consumers. A law that favors process mandates over substantive controls is less likely to serve consumers. Further, the goal of such legislation should be to accord business practices with consumers' reasonable expectations without forcing consumers through a consent flow like those currently at use in Europe, which often confusingly conflate both contextual, first-party collection and usage with non-essential third-party sharing for advertising.

- If businesses offer consumers choices with respect to privacy protections, can consumers be provided the right balance of information, i.e., enough to inform the choice, but not so much that it overwhelms the decisionmaker? What is the best way to strike that balance and assess its efficacy?

The best way for companies to provide choices without overwhelming the consumer is to accord data collection, in the first instance, with consumer expectations. If a company wants to engage in additional, non-contextual data collection or sharing, it should obtain the consumer's permission to do so. This request should be relatively rare, as most consumers are unlikely to want unrelated data collection absent a compelling value proposition.

Furthermore, in order to strike the balance of effective consumer information without overwhelming the user, companies should avoid the use of user interfaces that deceive or manipulate users into acting in a way that benefits the company and not the individual. These dark patterns of design[97] can nudge users away from choosing the privacy-protective choices made

[95] Gabriel J.X. Dance, *et al.*, *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants*, N.Y. TIMES (Dec. 18, 2018), https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html?module=inline.
[96] *Id.*
[97] "To put it plainly, dark pattern design is deception and dishonesty by design…The technique, as it's deployed online

available to them. The Norwegian Consumer Council (NCC) published an in-depth report on the use of these dark patterns in June 2018, noting that big tech companies like Facebook and Google utilize tools like "privacy intrusive default settings, misleading wording, giving users an illusion of control, hiding away privacy-friendly choices, take-it-or-leave-it choices, and choice architectures where choosing the privacy friendly option requires more effort for the users" in order to nudge or compel certain actions by the user.[98] This is not the first time Facebook was the focus of criticism due to their use of dark patterns in design: in 2016 Facebook used a consent flow that made it appear that WhatsApp users' did not have the opportunity to opt-out by using a hard-to-spot alternative button (and a buried opt-out) in order to mask the privacy implications of linking a WhatsApp account with a Facebook account, which included sharing user data with Facebook for the purposes of ad targeting.[99] Dark patterns like the ones detailed in the NCC's report are also used by smaller and medium-sized online service providers or manufacturers in order to steer users through a consent flow in a way that is beneficial to the company.[100]

In addition, although lengthy disclosures at the initial point of interaction have not fostered sufficient consumer understanding, companies should still be required to provide these disclosures and be more transparent and explicit about their data collection and practices. While few consumers read privacy policies, detailed disclosures should be written for the groups that already read them: regulators, reporters, and consumer-protection organizations like Consumer Reports. All of these entities are engaged in monitoring privacy policies for policy, consumer protection, and investment purposes and should continue to do so, but with more explicit information at hand. Today's policies are often vaguely expansive, providing little reliable concrete information about companies' actual practices. A transparency mandate to provide more precise information could remedy that.

- To what extent do companies compete on privacy? How do they compete? To what extent are these competitive dynamics dictated or influenced by consumer preferences, regulatory requirements, or other factors?

Unfortunately, the digital advertising ecosystem has become more complex in recent years, leaving

---

today, often feeds off and exploits the fact that content-overloaded consumers skim-read stuff they're presented with, especially if it looks dull and they're in the midst of trying to do something else — like sign up to a service, complete a purchase, get to something they actually want to look at, or find out what their friends have sent them.
Manipulative timing is a key element of dark pattern design. In other words *when* you see a notification can determine how you respond to it. Or if you even notice it. Interruptions generally pile on the cognitive overload — and deceptive design deploys them to make it harder for a web user to be fully in control of their faculties during a key moment of decision." Natasha Lomas, *WTF is Dark Pattern Design?*, TECHCRUNCH (July 1, 2018), https://techcrunch.com/2018/07/01/wtf-is-dark-pattern-design/.

[98] *Deceived by Design*, *supra* note 91.

[99] Natasha Lomas, *WhatsApp to Share User Data with Facebook for Ad Targeting—Here's How to Opt Out*, TECHCRUNCH (Aug. 25, 2018), https://techcrunch.com/2016/08/25/whatsapp-to-share-user-data-with-facebook-for-ad-targeting-heres-how-to-opt-out/; *WTF is Dark Pattern Design?*, *supra* note 97.

[100] *See*, *e.g.*, *Hall of Shame*, DARK PATTERNS, https://darkpatterns.org/hall-of-shame (last visited Dec. 18, 2018).

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. These practices made it difficult for consumers to exact control on who has access to detailed information about them.

However, in response to long-standing consumer concerns, some market actors have made significant changes to limit data collection on their platforms in order to compete in the marketplace on the basis of their privacy protections. 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.[101] Mozilla too has taken efforts to differentiate its Firefox web browser, by adopting policies to limit cross-site data collection.[102] Services like DuckDuckGo have found some success in marketing themselves as the tracking-free alternative to larger companies that rely on data for advertising.[103] 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.[104] 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.[105]

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.[106] 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

---

[101] 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.

[102] 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.

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

[104] *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.

[105] 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/.

[106] 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.

needed to make the product or service work correctly? And does the company explicitly disclose every way it uses the individual's data?[107] 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.[108]

However, this effort, and the ability of any third party to assess the privacy practices of a company, depends on transparency and specificity of language used in privacy policies that companies provide. Privacy disclosures are currently not designed to convey meaningful information either to ordinary consumers or even sophisticated privacy analysts. Therefore, we hope the FTC will 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. 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.

- Some academic studies have highlighted differences between consumers' stated preferences on privacy and their "revealed" preferences, as demonstrated by specific behaviors. What are the explanations for the differences?

Consumers' privacy concerns are contextual and subjective. As we noted in the section above devoted to answering the question regarding trade-offs, in some cases consumers would be willing to trade away the privacy of their information for a benefit. But overall consumers do not have the time or sufficient information to ensure their privacy preferences are being articulated and respected as they traverse the web.

---

[107] *Id*.

[108] 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/.

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.[109]

In addition, consumers lack robust tools that could effectuate their privacy preferences at scale.

- Given rapidly evolving technology and risks, can concrete, regulated technological requirements—such as data de-identification—help sustainably manage risks to consumers? When is data de-identified? Given the evolution of technology, is the definition of de-identified data from the FTC's 2012 Privacy Report workable? If not, are there alternatives?

While deidentification of consumer data is a valuable goal since it allows companies to extract value from consumer data while minimizing privacy and security impacts, there should be a higher standard of deidentification when such data is made public. Currently, the three-part test[110] does not control for situations in which the data is made public. The three-part test should include rules for situations in which the deidentified data is later made public and these rules should be strong enough to prevent re-identification in the future. For instance, the test could be expanded to require that there is no "reasonable foreseeability" that the data could be reidentified.

- What should the role of the Commission be in the privacy area? What would define successful Commission intervention? How can the Commission measure success?

The Federal Trade Commission should do the following in the area of privacy to ensure that consumers are protected:

- 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

[109] 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/.

[110] "...data is not 'reasonably linkable' to the extent that a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits to not try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data." *Protecting Consumer Privacy in an Era of Rapid Change*, FED. TRADE COMM'N (Mar. 2012), iv, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

privacy policy. 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 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.

Questions About Legal Frameworks

- What are existing and emerging legal frameworks for privacy protection? What are the benefits and drawbacks of each framework?

In any privacy law, data minimization should be a leading principle. Data minimization, done correctly, would redistribute the onus of good data practices onto the company and off of the consumer. Consumers are already overwhelmed with the number of decisions they are asked to make. Consumers should be empowered to use products without fear that the service or product will mine and collect more data than the consumer would reasonably expect. Ever-present pop-up dialogs and byzantine user controls do not serve users well; instead, consumers should be entitled to expect that data collection and sharing will be limited to the context of their interactions with any given company.

Specifically, a business that collects a consumer's personal information should limit its collection and sharing of personal information with third parties to *what is reasonably necessary to provide a service or conduct an activity that a consumer has requested*. Additional data collection or sharing should only happen with a user's clear and informed permission. Such a principle could have narrow exceptions—such as allowing collection or sharing as is reasonably necessary for security or fraud prevention. Additionally, some related, operational processing of already-collected data should be allowed without bothering the user for permission—such as first-party

analytics, research, and marketing.[111]

- What are the tradeoffs between ex ante regulatory and ex post enforcement approaches to privacy protection?

The most effective way to improve accountability within organizations is to provide for substantial external consequences for bad privacy practices. The threat of enforcement should incentivize companies to develop practices and procedures to best avoid legal liability. That said, a privacy law may reasonably mandate some degree of internal assessment in order to push companies to meaningfully assess their data practices. Importantly, however, these process requirements cannot substitute for strong substantive protections.

- The U.S. has a number of privacy laws that cover conduct by certain entities that collect certain types of information, such as information about consumers' finances or health. Various statutes address personal health data, financial information, children's information, contents of communications, drivers' license data, video viewing data, genetic data, education data, data collected by government agencies, customer proprietary network information, and information collected and used to make certain decisions about consumers. Are there gaps that need to be filled for certain kinds of entities, data, or conduct? Why or why not?

Although we do have some laws to protect some kinds of data in the US, those are imperfect and all the other data is unregulated. And companies are failing to effectively self-regulate their collection, storage, use, retention, and protection of consumer data. For example, the online advertising industry worked to implement some self-regulatory measures in order to avoid stricter regulations from the government. And in 2012, industry representatives committed to honoring Do Not Track instructions at a White House privacy event.[112] However, over the next few years, 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.[113] Today, seven years after Do Not Track settings were introduced into all the major browser vendors, few ad tracking companies meaningfully limit

---

[111] However, due to the breadth of the security/fraud exception and the potential for this exception swallowing the rule, data collected or retained solely for security or fraud prevention should not be used for related operational purposes.
This approach to consumer data dovetails with Professor Jack M. Balkin's concept of "information fiduciaries" in which the company must be loyal to the consumer's interests and show a duty of care to the data collected. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, FACULTY SCHOLARSHIP SERIES 5154 (2016), https://digitalcommons.law.yale.edu/fss_papers/5154.

[112] 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), https://www.wsj.com/articles/SB10001424052970203960804577239774264364692.

[113] 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/.

their collection, use, or retention of consumer data in response to consumers' Do Not Track instructions. Indeed, today when ad companies do allow users to access to tracking controls these options do not control for data collection practices but rather serve to put limits on the use of such data for things like ad practices.

Despite these failures, or perhaps because of them, consumers are aware of the clear gaps in our privacy laws and greatly desire stronger protections for their data. A January 2017 Consumer Reports survey found that 65 percent of Americans lack confidence that their personal information is private and secure.[114] And a few months later, a Consumer Reports survey found that this percentage had raised to 70 percent.[115] In addition, a March 2018 survey from Pew Research Center reported that although the 74 percent of individuals say that it is very important for them to be in control of who can get information about them, only nine percent of those surveyed believe that they have "a lot of control" over the information that is collected about them.[116]

In addition, a Consumer Reports survey found that 92 percent of Americans think companies should have to get permission before sharing or selling users' online data.[117] Clearly 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.[118]

In addition to consumers' desires for more and stronger general privacy protections, consumers also need privacy protections for the highly personal information they share with their internet service provider (ISP) in the course of using the service. Most Americans do not believe that having to give up their personal information to get basic communications service over broadband is a fair deal.[119] There are not enough rules at the local, state, or federal level regulating how ISPs can make use of their unfettered access to the personal data of their subscribers.[120] At the federal

---

[114] *As Trump Takes Office, What's Top of Consumers' Minds?*, CONSUMER REPORTS (Jan. 19, 2017), https://www.consumerreports.org/consumer-protection/as-trump-takes-office-what-is-top-of-consumers-minds/.

[115] *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/.

[116] Lee Rainie, *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/.

[117] *Consumers Less Confident*, *supra* note 115.

[118] *Americans' Complicated Feelings*, *supra* note 116.

[119] Joseph Turow, *et al.*, *The Tradeoff Fallacy*, UNIV. OF PA. (June 2015), *available at* https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.

[120] 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. (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

level, 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 Federal Communications Commission.

Although there is some disagreement on whether a comprehensive privacy law would be the appropriate solution to the many privacy concerns that consumers face,[121] 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,[122] yet lack agency to effectuate their preferences due to a

---

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, (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. *Americans' Complicated Feelings*, *supra* note 116.) 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. (5 U.S.C. § 801(b)(2).)

[121] *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.

[122] A recent survey from Consumer Reports found that 92 percent of Americans think companies should have to get

non-competitive ISP marketplace.[123]

- Other than explicit statutory exemptions, are there limitations to the FTC's authority to protect consumers' privacy? If so, should they be removed? Why or why not? Should more limitations be implemented? Why or why not?

- If the U.S. were to enact federal privacy legislation, what should such legislation look like? Should it be based on Fair Information Practice Principles? How might a comprehensive law based on Fair Information Practice Principles account for differences in uses of data and sensitivity of data?

Consumer Reports continues to support broader legislation that would provide increased protections for consumer data security and privacy.[124] 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.[125]

Unfortunately, legal protections at the federal level are currently getting weaker.[126] 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[127] will give consumers control

---

permission before sharing or selling users' online data. *Consumers Less Confident*, *supra* note 115.

[123] 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.

[124] 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/.

[125] Consumer Reports, *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/.

[126] 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.

[127] 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),

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,[128] states seem poised to set more comprehensive standards for security and data privacy. While Consumer Reports 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.

- Does the need for federal privacy legislation depend on the efficacy of emerging legal frameworks at the state level? How much time is needed to assess their effect?

A federal law should be complementary to any action at the state level to protect the privacy and digital security of their residents. As we noted above, a federal privacy law should not preempt stronger state laws. States have always been our "laboratories of democracy"[129] and should be permitted to create stronger laws to protect their consumers from new and emerging threats. However, Americans across the country need and desire a federal data privacy law that gives them control over their privacy and digital lives now. Such an important consumer protection should not be delayed in order wait for states to pass laws and implement new policies. Congress should respond to the series of serious data privacy and security breaches over the last two years and act to protect their constituents. In addition, we urge Congress to provide full funding and resources, along with rulemaking authority, to the Commission in order to ensure consumers are proactively protected from such harms.

- Short of a comprehensive law, are there other more specific laws that should be enacted? Should the FTC have additional tools, such as the authority to seek civil penalties?

We encourage states to continue to protect their citizens by passing new laws that expand safeguards for consumers. Consumer Reports supports the expansion of tools under the FTC's disposal, including rulemaking authority and civil penalties.

The Commission 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

---

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).

[128] *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.

[129] U.S. Justice Louis Brandeis in NEW STATE ICE CO. V. LIEBMANN, 285 U.S. 262 (1932).

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,[130] 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.

- How should First Amendment norms be weighed against privacy values when developing a legal framework?

Collection restrictions should be broad, and not purpose-specific, in order to avoid discriminating against certain kinds of activities.[131] The First Amendment argues for a collection limitation (i.e., data minimization) rather than a use restriction because once another individual knows information about a person, they have an interest in having the freedom of speech in voicing this knowledge. However, if an individual does not have such information, the First Amendment is less implicated.

---

[130] *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.

[131] *See*, *e.g.*, SORRELL V. IMS HEALTH, INC., 564 U.S. 552 (2011).

Therefore, the First Amendment encourages a limitation on collection.

Thank you for the opportunity to comment in advance of the February 12-13, 2019 Consumer Privacy hearing. If you have any questions, please feel free to contact us at 202.462.6262.

Sincerely,

Katie McInnis
Policy Counsel
Consumer Reports
1101 17th Street NW, Suite 500
Washington, DC 20036