DEMAND PROGRESS
EDUCATION FUND

Introduction

We are pleased that the Federal Trade Commission has invited comments on privacy and online surveillance. For decades, Big Tech companies have operated in a largely self-regulatory environment, which has failed both consumers and the larger economy - resulting in harms to competition, privacy, and democracy. Because these harms have become so pervasive, we recommend that the agency adopt a strong comprehensive framework for consumer privacy protection, with additional sectoral rules that apply to specific industries, types of information, and consumer categories.

We recommend that the FTC adopt comprehensive rules governing the handling of most Personally Identifiable Information (PII) based on Fair Information Practice Principles (FIPPs). A general foundational framework with additional sectoral rules is preferable to sectoral rules alone because sectoral approaches are more likely to become outdated and unworkable as industry and technology advance, but a flexible comprehensive framework could be adapted over time to meet the new challenges posed by advancing economic models and technologies, while also providing regulated actors the most reliable forward-looking guidance that could be reasonably expected.

Some have raised concerns that enforcement of stricter privacy rules could disproportionately increase compliance burdens on smaller firms — or firms that don't yet exist — thus increasing costs, creating barriers to entry, entrenching incumbents, and reducing competition. We neither endorse this concern, nor dismiss it out of hand. If determined that such impacts could manifest, then the FTC could tailor rules so as to ensure that any such effects are minimized, for instance by increasing the stringency of rules (and any penalties for noncompliance) as companies scale — accumulating more users and the potential to extract and exploit more of their data. This would help to balance competition interests and consumer privacy interests. However, we urge the FTC not to set thresholds for privacy protections based on volume of information held or sold by market actors unless it is prepared to set those thresholds at levels that would apply to the vast majority or potentially all market participants, given that huge amounts of extremely sensitive data are trivial for an actor of any size to acquire; and to enforce such rules forcefully and swiftly, given that a small smattering of data holders could completely and quickly undermine even the best-crafted protections.

Treatment of Non-Sensitive PII

For most collection and handling of PII, we recommend a comprehensive foundational framework that is based on Fair Information Practice Principles (FIPPs), a venerable, yet still relevant, set of principles governing data collection, use, and sharing. Under this framework, the collection and treatment of most Personally Identifiable Information (PII) would be governed by the FIPPs, with special restrictions for particularly harmful uses of PII, for sensitive PII (SPII), and for data collection and use by market dominant firms.

The FTC has authority to designate all non-FIPPs-compliant handling of PII as an unfair trade practice. For FTC enforcement purposes, a practice is unfair if it:

- causes or is likely to cause substantial injury to consumers;
- cannot be reasonably avoided by consumers;
- and is not outweighed by countervailing benefits to consumers or to competition.

While definitions of harms have, historically, focused strictly on tangible physical or economic harms, that definition is too narrow to provide effective protection in the digital age. In a recent paper on "Privacy Harms," Professors Danielle Keats Citron and Daniel Solove detail the myriad of harms that consumers face when information about them is collected, stored, used, and shared across the web, often without their consent or even their knowledge.[1] Professors Keats Citron and Solove group privacy harms into several categories: physical harms, economic harms, reputational harms, relationship harms, discriminatory harms, autonomy harms, and psychological harms.[2] The improper use, collection, or disclosure of PII can lead to one or more of these harms occurring. For instance, release of PII like a home address can result in an assault (physical harm) and/or stalking (psychological and often physical harm), as well as fear and anxiety (psychological harm). The release of sensitive health information could cause embarrassment (psychological harm), reputational harm, and discriminatory harm.

Perhaps the least obvious but most relevant privacy harm is the autonomy harm. This category includes uses of data that facilitate:

> (1) coercion—the impairment on people's freedom to act or choose;
> (2) manipulation—the undue influence over people's behavior or decision-making;

---

[1]Danielle Keats Citron and Daniel Solove, *Privacy Harms,* 102 B.U.L. Rev. _ (2022), available at: https://scholarship.law.gwu.edu/faculty_publications/1534/

[2] Id. at 33-60.

(3) failure to inform—the failure to provide people with sufficient information to make decisions about how their data is being used;
(4) thwarted expectations—engaging in activities that undermine people's choices;
(5) lack of control—the inability to make meaningful choices about one's data or prevent the potential future misuse of it;
(6) chilling effects—inhibiting people from engaging in lawful activities.[3]

These harms are endemic in the online environment, in large part due to economic incentives driven by particular uses of information — surveillance advertising being the most pervasive. The entire purpose of a large percentage of online data collection is to manipulate — to get users to purchase items that they otherwise would not purchase, to influence users' political decisions, to capture users' attention in order to serve them even more advertisements. These harms have been well-documented in the paper Privacy Harms,[4] in Accountable Tech's recent Petition for Rulemaking to Ban Surveillance Advertising,[5] and in our own comment on that rulemaking.[6] As Professors Keats Citron and Solove note, "[t]he FTC has recognized that trade practices that prevent consumers from "effectively making their own decisions" are ones that cause substantial injury."[7] Discrimination harms are also widespread and well-documented.[8] And the chilling effects of being surveilled online grow ever greater as law enforcement agencies buy access to PII in private databases.[9]

Professors Keats Citron and Solove also detail how privacy harms aggregate exponentially.[10] While it may be merely annoying to receive one piece of spam email as the result of your email address being shared without your consent, an avalanche of such emails can render inbox dangerous, inoperable, or both. This is the same principle which resulted in the Do Not Call Registry. A single unwanted phone call is a mild irritation, a barrage of repeated telemarketing calls is profoundly detrimental to one's attention, mental health, and productivity. As noted in Privacy Harms, the FTC has

---

[3] Id. at 45.
[4] Id.
[5] Accountable Tech, Petition for Rulemaking to Prohibit Surveillance Advertising, Dec. 3, 2021, available at: https://www.ftc.gov/system/files/attachments/other-applications-petitions-requests/r207005_-_petition_for_rule_to_prohibit_surveillance_advertising_0.pdf
[6] Demand Progress Education Fund, Re: Petition for Rulemaking to Prohibit Surveillance Advertising, Jan. 26,2022, available at: https://www.regulations.gov/comment/FTC-2021-0070-0015
[7] Citron and Solove, *supra* note 1 at 48.
[8] *Id.* at 55
[9] Laura Hecht Felella, *Federal Agencies are Secretly Buying Consumer Data,* Brennan Center, Apr. 16, 2021, available at: https://www.brennancenter.org/our-work/analysis-opinion/federal-agencies-are-secretly-buying-consumer-data
[10] Citron and Solove, *supra* note 1 at 19.

recognized the aggregation of small harms, stating that “An injury may be sufficiently substantial . . . if it does a small harm to a large number of people, or if it raises a significant risk of concrete harm.”[11]

Many online surveillance practices are not only profoundly harmful, as detailed above, but also unavoidable by consumers — fulfilling the second prong of the unfairness definition. Many of the largest tech companies have been cited by the FTC for privacy violations which, prior to the FTC’s investigations, were entirely obscured from consumers — the Facebook/Cambridge Analytica scandal being perhaps the most prominent example.[12] But the obfuscation around online data acquisition, sharing, and usage is typical. Consumers usually only find out about what is happening with their data after there has been a breach, an agency or law enforcement investigation, an investigative news piece, or a class action lawsuit. This lack of transparency effectively negates user control and makes the harms created by data collection, sharing, and use unavoidable.

Notably, the third prong of this standard does not favor countervailing benefits to companies or profits. It applies only to benefits that accrue to consumers or competition. Much of the backbone of the internet economy relies upon privacy-violating practices that harm consumers and benefit only a company’s bottom line. The benefits of online data collection and sharing are situationally dependent, but for the huge swath of data collection and sharing that support surveillance advertising, the benefits are minor and speculative at best, and most consumers don’t actually see much benefit to themselves.[13] Moreover, the data economy harms competition by exacerbating consolidation and monopolistic practices by Big Tech companies. As Big Tech companies grow larger, they are able to collect more data, which is then used to surveil and manipulate consumers, which gains the company greater profits and yet more dominance.

Based on the harms, the unavoidable nature of those harms, and the lack of countervailing benefits, the FTC can make a clear case that the current online data market is unfair to consumers. We recommend that the agency put in place a comprehensive set of rules, based on Fair Information Practice Principles (FIPPS) that will govern online data collection and handling of non-sensitive PII.

---

[11] Id. at 20.
[12] Federal Trade Commission, *Cambridge Analytica, LLC, In the Matter of*, Dec. 18, 2019, available at: https://www.ftc.gov/legal-library/browse/cases-proceedings/182-3107-cambridge-analytica-llc-matter
[13] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, Nov. 15, 2019, available at: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Comprehensive Rules Regarding Treatment of PII

FIPPs were first laid out in July 1973, when an advisory committee of the U.S. Department of Health, Education and Welfare (HEW) drafted a report, "Records, Computers and the Rights of Citizens: report of the Secretary's Advisory Committee on Automated Personal Data Systems," which set forth foundational ideas for safeguarding privacy.[14] Though the report is nearly fifty years old, the principles set forth in it are still relevant today. They create a framework which is flexible enough to adapt to new technologies and economic forces, while still embodying meaningful rights and protections.

The foundational principles in the HEW report are:

- There must be no personal-data record-keeping systems whose very existence is secret.

- There must be a way for an individual to find out what information about them is in a record and how it is used.

- There must be a way for an individual to prevent information about them obtained for one purpose from being used or made available for other purposes without consent.

- There must be a way for an individual to correct or amend a record of identifiable information about themself.

- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.[15]

The report specified that "[t]hese principles should govern the conduct of all personal-data record-keeping systems. Deviations from them should be permitted only if it is clear that some significant interest of the individual data subject will be served or if some paramount societal interest can be clearly demonstrated; no deviation should be permitted except as specifically provided by law."[16]

---

[14] Pam Dixon, *A Brief Introduction to Fair Information Practices*, World Privacy Forum, available at: https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/
[15] *Id.*
[16] *Id.*

FIPPs are widely respected and have been adopted by governments around the world, including the U.S. government. In the U.S. government, FIPPs are embodied in the Privacy Act of 1974, which governs the collection, storage, use, and sharing of PII by federal agencies.[17] The statute requires agencies that collect PII to publish public notices of that collection, including the purpose of the collection, details about what information will be collected, how the information will be used and stored, and under what circumstances it can be shared.[18] Additionally, the Privacy Act gives individuals a right of access to information collected about them and the right to correct erroneous information.[19] It also includes a private right of action through which individuals can vindicate their own privacy rights in court.[20]

FIPPs are also the basis of the California Consumer Privacy Act[21] and the California Privacy Rights Act,[22] which give consumers the right to know what information is being collected about them, the right to set limitations on the use of SPII, the right to correct inaccurate data, and the right to limit the sharing of their data.

Internationally, the FIPPs are also embodied in the Organisation for Economic Coordination and Development's "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"[23] and in the European Union's General Data Protection Regulation (GDPR).[24]

While the FTC has, historically, promoted FIPPs,[25] it has not routinely enforced these principles. Until the state of California's recent legislation, FIPPs have not been applied to private industry here in the U.S. Yet their application to private industry by the state of California and by the European Union demonstrate that this is, indeed, a workable

---

[17] The Privacy Act, 5 U.S.C. 552a, available at: https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf

[18] *Id.*

[19] *Id.*

[20] *Id.*

[21] The California Consumer Privacy Act of 2018, Cal. Civ. Code, §§1798.100-199

[22] *Id.*

[23] Organisation for Economic Coordination and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* available at: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[24] General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[25] See e.g. Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress, May 2000, available at: https://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report

strategy. They are flexible enough to evolve along with industry and technology, yet they provide meaningful rights and protections.

Some of the FIPPs were imperfectly embedded in the FTC's "Notice and Choice" model, but without sufficient enforcement, consistency, or penalties to make them actually meaningful. The Notice and Choice model was based on the idea that in order to provide adequate consumer privacy protection, companies need only notify users of data collection and handling practices then secure the users consent.[26] This model failed to embody most of the FIPPs - including data minimization and use limitations, user access and right to correction, or data protection requirements. Additionally, the Notice and Choice model assumed that all consent was meaningful — even if the disclosure of data handling practices was in obscure legal language, was hidden in an interminably long terms of service document, or was obtained in exchange for an essential service.[27] Study after study has reinforced the meaninglessness of consent under the Notice and Choice model.[28]

The Notice and Choice model relies on enforcement for deceptive practices, which means that companies only face consequences if they make representations about data handling that are untrue. The requirement of deceptiveness greatly reduces the FTC's potential for enforcement, because the range of corporate actions which can be found to be deceptive is too narrow — far narrower than the range of actions that could be found to be unfair — and that requirement is compounded by the density, length, and obscurity of disclosures that also cover swaths of other terms and conditions. Reliance on deceptiveness further does not take into account that certain data uses and data handling practices are, by default, unfair to consumers. There are many harmful practices that companies can engage in with user data which, even if fully and honestly disclosed, are still unfair. Enforcement exclusively for deceptiveness is not meaningful regulation, and it has effectively created an internet economy where unfettered collection, sharing, and use of PII have become the default model. So long as a company accurately discloses to the customer what data it is collecting and how that

---

[26] Statement of Federal Trade Commission Commissioner Rebecca Slaughter, Wait But Why? Rethinking Assumptions About Surveillance Advertising IAPP Privacy Security Risk Closing Keynote 2021, Oct. 22, 2021, available at: https://www.ftc.gov/system/files/documents/public_statements/1597998/iapp_psr_2021_102221_final2.pdf

[27] Id.

[28] Obar, Jonathan A. and Oeldorf-Hirsch, Anne. "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services." TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy, Apr. 2, 2016, https://ssrn.com/abstract=2757465; Smith, Aaron. "What Internet Users Know About Technology and the Web." Pew Research Center Internet & Technology, Nov. 25, 2014, https://www.pewinternet.org/2014/11/25/web-iq/.

data is being used, and so long as the customer consents (even implied consent), the company can do pretty much whatever it wants with the data.

Thus the Notice and Choice model, while based on some FIPPs ideas, is not a fair representation of the FIPPs more generally. In order for the FTC to engage in meaningful regulation and enforcement in this area, it must instead issue enforceable rules regarding data governance which would embody the FIPPs — including not only notice, but also access, correction, minimization, and protection. Violations of these rules must be, by default, an unfair practice.

Such rules would include the following provisions for all PII, based on FIPPs:

1.) **Transparency: Individuals have the right to know:**
   - i.) **What information is being collected about them**
   - ii.) **How that information is being used**
   - iii.) **Whom that information can be shared with (and how those third parties will also share that information)**
   - iv.) **Where that information is being stored**
   - v.) **What protections are in place to ensure that information is not unintentionally disclosed**
   - vi.) **If a dataset is being used to make a decision regarding them, which dataset is being used, who holds that dataset (with contact information for the entity possessing the dataset)**

The agency should promulgate specific regulations specifying what companies must do to fulfill this requirement. But at a minimum, this information must be clearly visible, presented in writing (along with an audio version for the visually impaired), and drafted in a way that is easily understandable by a layperson. For apps, this would mean text that is presented when the app is used for the first time, along with updated text whenever changes are made. For websites, this would mean a clearly visible link on the homepage that brings the user to a page summarizing this information in an easily readable format. This information must not be buried in larger terms of service, must not be cloaked in legalese, and must be updated routinely as circumstances change. Failure to abide by these requirements would be a per se unfair practice.

Importantly, the final requirement should apply not only to internet companies, but to any company that relies on commercial datasets of PII to make decisions. The idea that potentially life changing decisions are being made about individuals based on secret datasets is, by default, unfair; this unfairness is the basis of the Fair Credit Reporting Act and it is the basis of the “Failure to Inform” harm described by Professors Keats

Citron and Solove in their paper on privacy harms.[29] This would expand the requirements of the Fair Credit Reporting Act to any decision-maker that is relying on a commercial dataset to make a decision about whether to offer a benefit, product, or service. The individual who is the subject of a decision ought to have a right to know what dataset was the basis of the decision and, as addressed below, an opportunity to correct inaccuracies in that dataset.

2.) Data Minimization and Use Limitations

- **a.) Companies shall only collect the PII necessary to provide the service requested by the user. All secondary uses are prohibited, with limited exceptions for:**
  - **i.) Data security,**
  - **ii.) Analytics, and**
  - **iii.) Product improvement**
- **b.) Alternatively, if the agency is unable or unwilling to prohibit most secondary uses, it could prohibit specific secondary data uses, such as behavioral advertising or the use of sensitive data; or**
- **c.) Mandate a right to opt out of secondary data use, including through global opt-out controls and databases.**

a.) Prohibition on All Secondary Uses

In the opinion of most privacy advocates the first approach - prohibiting most secondary uses of PII, is preferable. The Electronic Privacy Information Center (EPIC) and Consumer Reports have published an extensive report titled “How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking”, explaining why a general prohibition on secondary uses is the most effective approach.[30] We are supportive of the framework presented by EPIC and Consumer Reports and their legal reasoning regarding the FTC’s authority to enforce data minimization rules. In short, a prohibition of secondary uses provides the greatest level of privacy protection for consumers. This approach takes into account the broad universe of harms that come from the mere handling of PII — that unwanted collection, viewing, and processing of personal data itself is an intrusion into a person’s privacy and, thus, inherently harmful. As noted in “How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking,” the FTC has recognized similar harms in the past:

---

[29] Citron and Solove, *supra* note 1 at 48.

[30] Electronic Privacy Information Center and Consumer Reports, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking,* Jan. 26, 2022, available at: https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf

> The FTC has adopted such a framework in the past: for example, in its 2017 settlement with Vizio, the FTC alleged that collecting and disclosing television viewing data without user permission was likely to cause those users substantial injury. While the FTC emphasized that such viewing data is inherently "sensitive," it is not clear that television viewing behavior is inherently more personal than any other activity. It would be difficult to argue that purchases or web browsing, for example, is any less revealing and sensitive than information about television programming viewed. More to the point, so much of the information collected is as revealing and sensitive as our intellectual habits (like television viewing) including even seemingly prosaic information like our purchase of alcohol swabs because our everyday purchases and interactions often reveals our health conditions (for instance, Type 1 diabetics use alcohol swabs), sexual orientation, gender, close relationships, and other intimate information.[31]

b.) Prohibition on Some Particularly Harmful Secondary Uses

Alternatively, the agency could take an approach that prohibits certain uses of PII, starting with the uses that we have highlighted below — especially surveillance advertising and selling data to law enforcement. For the reasons discussed in EPIC and Consumer Reports' report, we agree that this would be less protective than prohibiting all secondary uses, but it would provide significantly more protection than the final option - global opt-outs and opt-out databases. This regulatory regime would rely on the idea that certain uses are so harmful, and with so little countervailing benefit to consumers, that they ought to be prohibited outright as unfair trade practices. We would suggest, at a minimum, the below list of prohibited uses.

i.) Surveillance Advertising

Few information uses are more harmful or less beneficial than surveillance advertising. For the purposes of these comments, we accept Consumer Federation of America's definition of surveillance advertising: "Surveillance advertising, also known as targeted advertising or behavioral advertising, is the practice of showing individual consumers different advertisements based on inferences about their interests, demographics, and other characteristics drawn from tracking their activities over time and space."[32] As noted earlier, the FTC's definition of unfairness depends on whether a practice harms consumers, is reasonably avoidable, and has a countervailing benefit to consumers. Surveillance advertising is profoundly harmful, touching on several of the privacy harms

---

[31] *Id.*

[32] Consumer Federation of America, *Factsheet: Surveillance Advertising: What is it?*, Aug. 26, 2021, available at: https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-what-is-it/

discussed above — it is designed to be manipulative, it is often discriminatory, it offers consumers little or no control, and it results in consumers having the pervasive sense of being watched online, which creates a chilling effect. Surveillance advertising is likely the most pernicious example in the data economy of both the Genie-out-of-the-bottle and Pandora's Box problems: once these dossiers on consumers are held by one unscrupulous actor, it is unlikely any affected consumer can reasonably mitigate further harm, whether that be the sale of a detailed consumer profiles to stalkers, who have already used this kind of information to threaten and kill,[33] or to malign foreign governments, which is currently so trivially easy for them to do in secret it is almost certainly already occurring.[34]

Moreover, surveillance advertising as a business model ensures that the most dominant Big Tech firms will continue to dominate the online landscape for the foreseeable future. It is on this basis that we, and many others, have previously called for the FTC to ban surveillance advertising,[35] defined as "1) an information or communication platform collecting personal data and 2) targeting advertisements at users, based on that personal data, as they traverse the internet, including other digital platforms."[36]

As we discussed in our comments on FTC's request for comments on Accountable Tech's Petition to Ban Surveillance Advertising, surveillance advertising presents several unique problems, while offering little actual benefit to consumers.

First, surveillance advertising sets up perverse incentives which encourage companies to collect vast amounts of data on users. The more data that is collected, the thinking goes, the more effective and targeted the ads may be and the more money the company can make from advertising revenue. This data is used to create comprehensive consumer profiles, which are then used to tailor not only advertising, but also newsfeeds, video and news content, and recommendations. The delivery of these products is often inherently discriminatory — serving up different products, services, deals, and recommendations based upon the user's inherent characteristics - sexual identity, gender, sexual orientation, and race.

---

[33] Robert O'Harrow Jr., *Online Firm Gave Victim's Data to Killer*, Chicago Tribune, Jan. 6, 2002, available at: https://www.chicagotribune.com/news/ct-xpm-2002-01-06-0201060305-story.html; Joseph Cox, *T-Mobile 'Put My Life in Danger' Says Woman Stalked With Black Market Location Data,* Vice News, Aug. 21, 2019, available at https://www.vice.com/en/article/8xwngb/t-mobile-put-my-life-in-danger-says-victim-of-black-market-location-data

[34] Justin Sherman, *The U.S. Needs Controls on Data Brokerage,* Tech Policy Press, June 24, 2022, available at: https://techpolicy.press/the-u-s-needs-controls-on-data-brokerage/

[35] Demand Progress Education Fund, *supra* note 6.

[36] Accountable Tech, *supra* note 6.

These vast troves of data are also often collected and shared without users' knowledge or meaningful consent. Companies engaging in surveillance advertising are notoriously secretive about the algorithms that govern the targeting of advertising and content and downright deceitful about the way that consumer data is used and shared — as evidenced by Facebook's Cambridge-Analytica scandal.[37] There is a rich history of internet companies (especially Big Tech) engaging in deceptive trade practices while collecting private user information for use in surveillance advertising. Many Big Tech companies that engage in surveillance advertising are frequent offenders, subject to multiple FTC complaints and settlements.[38] These bad privacy practices are the direct result of companies being incentivized to collect and share greater volumes of PII in order to facilitate more and more targeted advertising, supercharged by an absence of meaningful regulatory oversight.

Surveillance advertising harms not only individuals, but society at large. It has become increasingly obvious that surveillance advertising drives a harmful attention economy. Platforms are incentivized by surveillance advertising to hold consumers' attention for two reasons: 1) keeping users engaging with the platform allows the company to collect more information on the user, their interests, likes and dislikes, their location and habits and 2) keeping the user's eyes on ads for a longer period of time equals more ad revenue. Therefore, companies are incentivized to serve up the most "engaging" content.[39] This is often inaccurate, hateful, or extreme and polarizing content.[40] This extreme content then feeds larger patterns of political polarization, conspiracy theories, hate, and even violence.[41]

---

[37] Paolo Zialcita, *Facebook Pays $643,000 Fine For Role In Cambridge Analytica Scandal*, NPR News, Oct. 30, 2019, available at: https://www.npr.org/2019/10/30/774749376/facebook-pays-643-000-fine-for-role-in-cambridge-analytica-scandal

[38] See e.g Federal Trade Commission, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook,* July 24, 2019, available at: https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions; Federal Trade Commission, *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law,* Sept. 4, 2019, available at: https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations; Federal Trade Commission, *FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network,* Mar. 30, 2011, available at: https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz

[39] Humane Tech, *The Attention Economy*, https://www.humanetech.com/youth/the-attention-economy

[40] Paul Lewis, *Fiction is Outperforming Reality: How Youtube's Algorithm Distorts Truth,* The Guardian, Feb. 2, 2018, https://www.theguardian.com/technology/2018/feb/02/how-youtubes-algorithm-distorts-truth

[41] Brookings Institute, *How Tech Platforms Fuel U.S. Political Polarization and What Government Can Do About It,* Sept. 27, 2021, https://www.brookings.edu/blog/techtank/2021/09/27/how-tech-platforms-fuel-u-s-political-polarization-and-what-government-can-do-about-it/

A 2021 Brookings Institute report, based on a review of more than 50 social science studies and interviews with more than 40 academics, concluded that the algorithms of social media platforms that are driven by surveillance advertising "intensif[y] divisiveness and thus contribute[] to its corrosive effects."[42] Brookings' experts found that "social media companies do not seek to boost user engagement because they want to intensify polarization. They do so because the amount of time users spend on a platform liking, sharing, and retweeting is also the amount of time they spend looking at the paid advertising that makes the major platforms so lucrative."

Many other experts have come to similar conclusions[43] (including many of the experts featured in the popular 2021 documentary "The Social Dilemma"[44]): surveillance advertising incentivizes engagement-driven "attention economy" algorithms, which rely on extreme, hateful, and polarizing content to capture audience attention and derive greater revenue.

Additionally, surveillance advertising creates competition harms by allowing Big Tech Companies to engage in anticompetitive behavior and solidify their market dominance. Surveillance advertising by any company is pernicious, for all of the privacy-related reasons discussed above. But surveillance advertising by Big Tech companies in particular — which have become increasingly dominant in this space — poses serious threats to competition policy. Big Tech companies like Google and Apple have incomparably vast troves of user data, including communications, social connections, financial transactions, location information, search and browsing histories, biometrics, and even health data. These datasets are integrated across platforms to allow Big Tech companies to engage in unparallelled analysis and granular marketing that no other companies can compete with. As discussed in the House Judiciary Committee Subcommittee on Antitrust, Commercial, and Administrative Law Report on Investigation of Competition in Digital Markets, the digital advertising market "has become increasingly concentrated since the advent of programmatic trading. In 2017, Business Insider reported that Google and Facebook accounted for 99% of year-over-year growth in U.S. digital advertising revenue. Today, advertisers and publishers alike have few options when deciding how to buy and sell online ad space."[45]

The surveillance advertising revenue can then be used to offset/subsidize losses in other areas of business, which allows market dominant companies to further undercut

---

[42] Brookings Institute, *Fueling the Fire: How Social Media Intensifies U.S. Political Polarization - and What Can Be Done About It,* Sept. 2021, available at: https://bhr.stern.nyu.edu/polarization-report-page
[43] Katherine J. Wu, *Radical Ideas Spread Through Social Media. Are the Algorithms to Blame?*, PBS Nova, Mar. 28, 2019, https://www.pbs.org/wgbh/nova/article/radical-ideas-social-media-algorithms/
[44] Humane Tech, *The Social Dilemma,* https://www.humanetech.com/the-social-dilemma
[45] House Committee on the Judiciary Subcommittee on Antitrust, Commercial, and Administrative Law *Report on Investigation of Competition in Digital Markets* at 131 (internal citations omitted).

competitors in other spheres of operation. Already, many Big Tech companies are offering free products (for example, Google Maps and Facebook's social network) in exchange for data collection and related digital advertising. Additionally, ad revenue generated by financial data can also be used to acquire even more data, or more businesses that possess or create data, which can then be used for more acquisitions — a vicious anti-competitive cycle. Even now, the decade-plus of data troves and user adoption advantages make it nearly impossible for other companies to compete with Big Tech, not just in digital advertising, but in many online realms.[46]

Surveillance advertising also fulfills the second prong of the FTC's unfairness definition, because it cannot be reasonably avoided by consumers. Surveillance advertising is pervasive across the internet. In 2021, digital advertising spending worldwide amounted to 521.02 billion U.S. dollars.[47] The average consumer is simply unable to avoid being tracked online or served surveillance advertising as the result of that tracking. According to a recent PEW survey, "[a] majority of Americans believe their online and offline activities are being tracked and monitored by companies and the government with some regularity. It is such a common condition of modern life that roughly six-in-ten U.S. adults say they do not think it is possible to go through daily life without having data collected about them by companies or the government."[48]

As discussed above, surveillance advertising offers no benefit to competition. Instead, it actively promotes continued consolidation and market dominance by monopolistic Big Tech companies. Additionally, there is little or no benefit to consumers — the third prong of the FTC's unfairness definition. Behavioral advertising involves the collection of vast troves of data, which most consumers object to. According to PEW's survey "large shares of U.S. adults are not convinced they benefit from this system of widespread data gathering. Some 81% of the public say that the potential risks they face because of data collection by companies outweigh the benefits, and 66% say the same about government data collection."[49]

Though it isn't relevant to the question of unfairness for the FTC's purposes, it bears noting that even for companies, the benefits of surveillance advertising are dubious. One recent study on the impacts of surveillance advertising on online publishers' revenue by researchers at the University of Minnesota, University of California, Irvine,

---

[46] Id. at 40-46
[47] Statista, *Digital Advertising Spending Worldwide from 2021 to 2026*, July 27, 2022, available at: https://www.statista.com/statistics/237974/online-advertising-spending-worldwide/
[48] Pew Research Center, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Nov. 15, 2019, available at: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/
[49] *Id.*

and Carnegie Mellon University suggested that publishers only get about 4% more revenue for an ad impression that has a cookie enabled than for one that doesn't.[50]

Because it is harmful to both consumers and competition, because it is unavoidable, and because it provides little benefit to consumers, surveillance advertising should be considered an unfair use of information and should be prohibited.

ii. Selling of PII to Law Enforcement Agencies

News reports have revealed that numerous federal law enforcement agencies are circumventing Fourth Amendment warrant requirements by purchasing data from commercial vendors. A recent report by the Brennan Center noted several such instances:

> "Federal agencies are using purchased data to target already vulnerable communities. For example, leaked documents revealed that at least two branches of DHS — Customs and Border Protection and Immigration and Customs Enforcement — bought cell phone location data. In addition, ICE has reportedly purchased utility data, as well as information from private license plate reader databases. The agencies tracked migrant groups and targeted individuals for immigration enforcement using this information.
>
> News reports also indicate that the FBI, Secret Service, and Department of Defense have acquired smartphone location data without a warrant. Defense contractors purchased location data from popular Muslim prayer and Qur'an apps and dating apps. Several members of Congress have made an official inquiry into how this data has been utilized. And cell phone data was allegedly used to track Black Lives Matter protesters over the summer. Though it is uncertain exactly how cell phone data informed the FBI's response to the protests, it is notable that the agency renegotiated its purchase contract with a data broker around the time of the demonstrations."[51]

The harms of this usage of information are obvious. The Fourth Amendment exists to protect individuals from unreasonable searches and seizures. Fourth Amendment jurisprudence has created warrant requirements with specific, limited carve-outs in order to prevent law enforcement from invading an individual's privacy without just cause and

---

[50] Keach Hagey, *Behavioral Ad Targeting Not Paying Off for Publishers, Study Suggests,* The Wall Steet Journal, May 29, 2019, available at: https://www.wsj.com/articles/behavioral-ad-targeting-not-paying-off-for-publishers-study-suggests-11559167195

[51] Hecht Felella, *supra* note 9.

without oversight. Allowing companies to sell data to law enforcement agencies with no warrant undermines those purposes - it creates a secret mechanism for law enforcement surveillance with no oversight, accountability, or practical limitation.

Allowing paid access to PII is directly contrary to the Supreme Court's recent ruling in Carpenter v. United States. In Carpenter, the Court considered whether or not a court order - a mechanism that requires less of an evidentiary showing than a warrant - was sufficient for law enforcement to access cell phone location data held by the wireless carrier. The Court held that accessing location data held by a third party wireless provider was a Fourth Amendment search that requires a warrant. The Court noted that location data was particularly sensitive from a privacy standpoint, holding that "[a] majority of the Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements. Allowing government access to cell-site records—which hold for many Americans the 'privacies of life, contravenes that expectation."[52]

Yet location data, according to many reports, is exactly what law enforcement agencies are purchasing. Allowing this use of data clearly harms individuals by invading their privacy and violating their Fourth Amendment rights.

This practice, too, is likely unavoidable for consumers. Companies collect information secretly, then law enforcement data purchases are made in secret, and that secrecy takes away consumers' ability to avoid this privacy violation. The proportion of this data that even results in a prosecution - in which such collections *might* be revealed - is likely tiny, foreclosing even that minimal amount of transparency about this collection.

And the practice of selling PII to law enforcement also has no benefit to the consumer whose data is being sold. Quite the contrary - this data may result in that person being criminally prosecuted. And though, again, it is only the consumer whose benefits are to be considered for "unfairness" purposes, it may be useful to note that the bulk of the information shared this way likely does not even contribute to a societal crime control benefit, since the vast majority of people whose data is being purchases are entirely innocent.

iii. Special Prohibitions for Market Dominant Firms

Because of their outsize dominance in the online economy, certain companies pose a unique threat and require specialized restrictions. Market dominant Big Tech companies already have a proven track record of aggressively anti-competitive actions. In fact the

---

[52] Carpenter v. United States, 138 S.Ct. 2206 (2018), available at: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf (internal citations and quotations omitted)

four largest tech companies - Amazon, Apple, Facebook/Meta, and Google - have already been the subject of an intensive investigation by the House Committee on the Judiciary's Subcommittee on Antitrust, Commercial and Administrative Law.[53] This investigation found that Amazon, Apple, Facebook, and Google routinely engaged in anticompetitive business practices. The Subcommittee's investigation revealed that Amazon had acquired competitors, preferenced its own products on its platform, and utilized seller data to secure its dominance. The Subcommittee found that Apple used control of its app store to create barriers to competition, had misappropriated competitively sensitive data from app developers, and had used dominance and control of the app store to raise prices. The Subcommittee found that Facebook, had engaged in the acquisition and neutralization of nascent competitive threats and had preferenced its own services. Lastly, the Subcommittee investigation revealed that Google was guilty of undermining vertical search providers, using dominance to steadily increase advertising fees, using anti competitive contracts to block competitors, and utilizing user data in anticompetitive ways to secure its dominance. The Subcommittee concluded that these four companies needed to be broken up and then heavily regulated - including prohibitions on acquisitions of competitors and potential competitors and prohibitions on self-preferencing.

As discussed above, in section 2(b)(i), allowing Big Tech companies to continue to acquire ever more data creates significant harms not just to consumers, but to competition. More data acquisition begets more dominance, which begets more data acquisition. Because of the unique threat they pose, evidenced by a comprehensive investigation by Congress, there should be special limits around Big Tech data acquisition, sharing, and uses. The FTC should also investigate and establish rules prohibiting Big Tech companies from engaging in anticompetitive practices that endanger users privacy and safety.

First, Big Tech companies should be prohibited from acquiring or developing payment systems. We have presented detailed comments on this topic to the Consumer Financial Protection Bureau.[54] Big Tech expansion into payment systems would have - and in some cases, is already having - a negative effect on competition, privacy, and small businesses. Big Tech companies, particularly Amazon, Apple, Facebook, and Google, have a history of anticompetitive behavior, unfair surveillance, poor data management practices, and invasions of privacy. Financial data is among the most

---

[53] House Committee on the Judiciary Subcommittee on Antitrust, Commercial, and Administrative Law, *Investigation of Competition in Digital Markets Majority Staff Report and Recommendations,* 2020, at 170-172, 206-208 (hereinafter Subcomm. Report)

[54] Demand Progress Education Fund, *Re: Docket No. CFPB-2021-0017 Request for Comment Regarding the CFPB's Inquiry Into Big Tech Payment Platforms,* Dec. 6, 2021, available at: https://s3.amazonaws.com/demandprogress/letters/Demand-Progress-Education-Fund-CFPB.pdf

sensitive of personal information.[55] Financial data includes purchasing history, which reveals a variety of personal preferences, as well as income and asset information. Purchase and transaction histories can reveal a variety of other sensitive information about individuals, including sexual preferences and identity, religious and political associations, and medical information. And some companies are also already collecting sensitive biometric data as part of their payment systems (for example, Amazon's One payment system).[56] Entrusting sensitive financial data to Big Tech companies would be unwise because these companies have a history of both purposefully disregarding user privacy (for instance, sharing sensitive information with third parties without user consent)[57] and negligently handling sensitive information in ways which have allowed for data breaches.[58]

Additionally, Big Tech companies should be prohibited from acquiring other companies primarily for the consumer data that the company holds. One academic study found that when Big Tech companies acquire apps, half of those acquired apps are discontinued, and the ones that remain often then request more data from users.[59] There are only two easily identifiable reasons why Big Tech companies would engage in these kinds of acquisitions: to eliminate competitors or to acquire the data held by the app (or perhaps both at the same time). These kinds of acquisitions are both anticompetitive and intrusive to users and should be prohibited.

Even if the FTC does not decide to prohibit all surveillance advertising, Big Tech companies should be prohibited from collecting data for use in surveillance advertising. As discussed in our prior comments to the agency on this topic, surveillance advertising by Big Tech companies creates harms to both consumers and competition.[60]

Separate but related to these issues are anticompetitive practices that endanger consumers' privacy and safety. An ongoing conflict between two of the largest tech companies, Apple and Google, demonstrates the need for FTC action to prevent

---

[55] United States Department of Commerce, *Office of Privacy and Open Government, Safeguarding Information,* available at: https://www.osec.doc.gov/opog/privacy/pii_bii.html
[56] Amazon One, available at: https://one.amazon.com/
[57] Will Evans, *Amazon's Dark Secret: It has Failed to Protect Your Data,* Reveal and Wired, Nov. 18, 2021, available at: https://www.wired.com/story/amazon-failed-to-protect-your-data-investigation/
[58] In May 2017, Amazon found that for two years, 24 million customers' names and American Express numbers were outside a "secure zone" for payment data. And there was no way to know whether the data had been accessed. Aaron Holmes, *533 Million Facebook Users' Phone Numbers and Personal Data Have Been Leaked Online,* Business Insider, Apr. 3, 2021, available at: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4
[59] Pauline Affeldt and Reinhold Kesler, *Competitors' Reactions to Big Tech Acquisitions: Evidence from Mobile Apps,* German Institute for Economic Research, Dec. 9, 2021, available at: https://www.diw.de/documents/publikationen/73/diw_01.c.831752.de/dp1987.pdf
[60] Demand Progress Education Fund*, supra* note 6.

companies, and in particular dominant tech companies, from exposing users to such unnecessary risks.

The conflict between Apple and Google revolves around the companies' failure to include in iOS and Android's default messaging apps mutual support for modern communications features — namely end-to-end encryption. The status quo, instead, involves sending texts between devices running different operating systems as Short Message Service (SMS) messages, which have been notoriously vulnerable for years.[61] Google has publicly called on Apple to support one option, Rich Communications Services, which would at least protect one-on-one messaging.[62] We take no position on which protocol is adopted — only that failure to support end-to-end encryption across multiple operating systems within default messaging apps creates unacceptable dangers for consumers.

Specifically, Apple and Google sending messages from one default messaging app to another as SMS or MMS messages, instead of adopting a mutually supported protocol that provides for end-to-end encryption, turns the communications into privacy and security vulnerabilities.[63] An individual consumer is severely impacted, for example, when bad actors exploit a vulnerability in SMS messages to compromise two-factor authentication codes, which in turn facilitates stealing money from bank accounts and unlawful access to people's accounts more generally.[64] Given the ubiquity of securing accounts like this, the secondary effects are virtually endless. As unsecured messages are accumulated for processing by telecommunications companies, the lack of end-to-end encryption support further coalesces into a wide-reaching vulnerability that is ripe for exploitation by malign.[65]

Failure to implement a mutually supported protocol that includes end-to-end encryption, is anticompetitive at its root. The primary consequence from a business perspective is

---

[61] Brian Krebs, *Can We Stop Pretending SMS Is Secure Now?*, Krebs on Security, March 16, 2021, available at: https://krebsonsecurity.com/2021/03/can-we-stop-pretending-sms-is-secure-now/

[62] Android, *It's Time for Apple to Fix Texting*, https://www.android.com/get-the-message/

[63] Rob Pegaroro, *Google Posts Yet Another Plea for Apple to Support RCS Messaging in iMessage,* PC Mag, Aug 9, 2022, available at: https://www.pcmag.com/news/google-posts-yet-another-plea-for-apple-to-support-rcs-messaging-in-imessage

[64] Joseph Cox, *Criminals Are Tapping into the Phone Network Backbone to Empty Bank Accounts,* Vice News, Jan. 31, 2019, available at: https://www.vice.com/en/article/mbzvxv/criminals-hackers-ss7-uk-banks-metro-bank

[65] Lorenzo Franceschi-Bicchierai, *Company That Routes Billions of Text Messages Quietly Says It Was Hacked*, Vice News, Oct. 4, 2021, available at: https://www.vice.com/en/article/z3xpm8/company-that-routes-billions-of-text-messages-quietly-says-it-was-hacked

walling in consumers.[66] Months ago, Tim Cook, Apple's Chief Executive Officer, responded to a question about adopting RCS by telling an audience-member to "buy your mom an iPhone."[67] Refusing to support a cross-platform protocol is even reported to drive stigmatization of non-iPhone users.[68] These are not compelling business interests or competitive actions in even the best of light, but certainly not when weighed against the unnecessary vulnerability of millions of communications.

It is difficult to identify any consumer benefit to the status quo. Conversely, a more modern protocol would permit higher quality media in messages, real-time feedback like typing indicators, and sender verification. But end-to-end encryption across default messaging apps is critical because it would significantly improve the security of countless messages, making all consumers less vulnerable to targeted attacks on their privacy while also making their information far more resilient to attacks on centralized communications infrastructure.

To reiterate, we do not endorse any particular protocol; rather, we are sounding the alarm that anticompetitive posturing is endangering the privacy and security of an untold number of communications among millions of people. The FTC should make clear that it will not tolerate negative impacts on consumer privacy or security that attend anticompetitive practices like these. At a minimum, the FTC should investigate the privacy and security consequences of this ongoing conflict between Apple and Google that is apparently (and explicitly) rooted in anticompetitive interests.

iv. Other Prohibited Uses

The above prohibitions are in no way an exhaustive list. As EPIC laid out in its report on data minimization, there are a variety of other prohibitions that have been suggested, including

- Discriminatory use of data that deprives consumers of opportunities based on protected characteristics (see infra Section V.B ("Civil Rights"))
- Tracking users across different devices

---

[66] Abner Li, *Apple: 'Moving iMessage to Android Will Hurt Us More Than Help Us'*, 9to5Google, Apr. 8, 2021, https://9to5google.com/2021/04/08/apple-imessage-android/

[67] Emma Roth and Richard Lawler, *Tim Cook Says 'Buy Your Mom an iPhone' If You Want to End Green Bubbles*, Sept. 16, 2022, available at: https://www.theverge.com/2022/9/7/23342243/tim-cook-apple-rcs-imessage-android-iphone-compatibility

[68] Tim Higgins, *Why Apple's iMessage Is Winning: Teens Dread the Green Text Bubble*, The Wall Street Journal, Jan. 8, 2022, available at: https://www.wsj.com/articles/why-apples-imessage-is-winning-teens-dread-the-green-text-bubble-11641618009

- Personalization based on sensitive attributes
- Facial recognition and other biometric identification
- Collection and use of intimate information — about the human body, health, innermost thoughts and searches, sex, sexuality, and gender, and close relationships, and
- Disclosure of personal information of minors (or children under the age of 13).[69]

We agree with this list and are supportive of other suggestions from privacy, civil rights, children's advocacy, and corporate accountability organizations.

c. Global Opt-out and Database

We do not believe that the third option - providing a global opt-out with an opt-out database - would be as effective. This is in large part because companies often create coercive requirements that consumers accept data collection as a predicate for receiving an unrelated service. Relying on an opt-out model will only result in more companies telling consumers that they can either choose to opt-in or they cannot use the product. Additionally, the transfer and sharing of PII is often outwardly invisible, so it would be difficult for consumers - or regulators - to know whether or not companies are honoring the consumer's opt-out preferences. Reliance on opt-out databases would also not address the perniciousness of surveillance advertising (and other similarly harmful uses of data) and the negative impacts it has on both privacy and competition. In order to create meaningful regulations, at a minimum certain very harmful practices must be prohibited, and ideally, all secondary uses (with narrow exceptions) should be.

3.) Access and Correction

a.) Users shall have the right to request a copy (electronically or physically, based on the user's preference) of all data that the company has collected about them

i.) Companies shall provide this data in a reasonable amount of time

ii.) Companies shall provide clear instructions for access on their websites

b.) Users shall have the right to correct inaccuracies in the data about them

i.) Companies shall make a decision about correction requests within a reasonable amount of time

[69] Electronic Privacy Information Center and Consumer Reports, *supra* note 30.

ii.) Companies shall provide clear instructions for correction on their websites

iii.) Companies shall create an internal review mechanism for users whose requests for correction were denied

The idea that consumers would have the right to access the data that is collected about them, and a right to correct inaccuracies, is not revolutionary. It is, in fact, the backbone of the Federal Privacy Act, which grants all citizens and lawful residents the right to access the data a government agency holds about them and the right to correct inaccuracies in that data. The European General Data Protection Directive (GDPR) also gives access[70] and correction rights.[71] California's privacy statutes also grant rights of access and correction.[72]

Given that information collected online can be the basis for employment, housing, or other life-changing decisions, consumers must be able to view datasets about them and correct potential inaccuracies there. In order to make access and correction rights meaningful, companies must have obvious routes through which consumers can make access and correction requests, they must provide information free of charge, they must provide and correct information in a timely manner, they must provide information in a user-friendly format, and there must be a mechanism for review of correction decisions to ensure accountability. The GDPR lays out many useful examples of such requirements. The GDPR requires that companies "[m]ake available to consumers two or more designated methods for submitting requests for information …or requests for deletion or correction … including, at a minimum, a toll-free telephone number."[73] It also requires that information be provided in a user-friendly format and free of charge and it sets a general deadline of 45 days responding to a request for access or correction.

Over time, implementation of access and correction rights would likely result in less data collection overall because more data collection would make compliance more onerous, and because the sheer amount of data collected, if laid out to consumers, would likely result in pressure to lessen data collection.

We recommend that the FTC create an easy mechanism for consumers to report non-compliance with access and correction requirements to the agency. Failure to satisfy these requirements would be considered an unfair practice.

---

[70] GDPR, *supra* note 24, at Article 15.
[71] GDPR, *supra* note 24, at Article 16.
[72] California Privacy Rights Act, *supra* note 21.
[73] *Id.*

4.) Security

- **a.) Companies shall properly secure all PII to industry standards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure**
- **b.) If PII is improperly accessed, used, shared, or breached, companies shall notify users and the FTC within a reasonable amount of time**

The FTC already enforces against financial institutions who fail to properly secure information under the Safeguards Rule, but the agency should expand that enforcement to all internet companies who collect and store PII. The security requirements of the Safeguards Rule are:

1.) Implement and periodically review access controls.
2.) Know what you have and where you have it.
3.) Encrypt customer information on your system and when it's in transit.
4.) Assess your apps.
5.) Implement multi-factor authentication for anyone accessing customer information on your system.
6.) Dispose of customer information securely.
7.) Anticipate and evaluate changes to your information system or network.
8.) Maintain a log of authorized users' activity and keep an eye out for unauthorized access.

Similarly, the GDPR's security rules mandate, as appropriate, the following measures: "the pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."[74]

In particular, we want to call attention to the importance of encryption. FTC rules should make it an unfair practice to fail to use encryption for both website traffic and the storage of PII. Encryption is important because it can protect data in transit and in storage by scrambling the data and preventing it from being easily usable by any individual who intercepts it. Encryption protects consumer data against improper access by hackers and government actors. "The benefits of robust encryption are clear. Examples in daily life include enabling secure electronic banking and financial transactions, confidential private communications, and the secure exchange of sensitive

[74] GDPR, *supra* note 24, at Article 32.

information, such as healthcare data."[75] Encryption of data in transit is already an industry standard security practice, with more than 80% of websites using encryption.[76] It is inexpensive, with certificate authority services offered free from some organizations.[77]

Similarly, many cloud storage providers also provide encryption, including Microsoft OneDrive and Dropbox. Requiring internet companies that store PII to encrypt it would help to protect against data breaches, which have continued to rise year over year, especially for the manufacturing and utilities, healthcare and financial industries.[78] According to Identity Theft Resource Center research, the total number of data breaches through September 30, 2021 had already exceeded the total number of events in 2020 by 17%, with 1,291 data breaches in 2021 compared to 1,108 breaches in 2020.[79] Requiring all internet companies to employ encryption for traffic and stored data would not be onerous, and it would create important protection for consumer data.

Similarly, failing to inform consumers of data breaches in a timely manner should be considered an unfair practice. The GDPR and many state statutes already require data breach notifications. In California, for instance, requires "a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[80] The earlier companies notify consumers of a data breach, the more effective that breach notification is. Earlier notification allows consumers to take action to mitigate potential harms, including freezing or locking their credit, checking their credit reports for unauthorized transactions, and purchasing identity theft protection tools. For this reason, the FTC should set deadlines for notification. The GDPR provides a useful example, requiring notification to a government data protection officer within 72 hours[81] and individuals without undue delay.[82] A similar 72 hour deadline for notifying

---

[75] Namrata Maheshwari, *10 Facts to Counter Encryption Myths,* Access Now, Aug. 2021, available at:https://www.accessnow.org/cms/assets/uploads/2021/08/Encryption-Myths-Facts-Report.pdf (at 3).
[76] Nicole Casal Moore, *How Let's Encrypt Doubled the Internet's Percentage of Secure Websites in Four Years,* University of Michigan Michigan News, Nov. 13, 2019, available at: https://news.umich.edu/how-lets-encrypt-doubled-the-internets-percentage-of-secure-websites-in-four-years/#:~:text=The%20percentage%20of%20websites%20protected,in%202016%20to%2080%25%20today.
[77]
[78] Maria Henriquez, *The Top Data Breachs of 2021*, Security Magazine, Dec. 9, 2021, available at: https://www.securitymagazine.com/articles/96667-the-top-data-breaches-of-2021
[79] *Id*.
[80] Cal. Civ. Code 1798.82 and 1798.29.
[81] GDPR, *supra* note 24, at Article 33.
[82] GDPR, *supra* note 24, at Article 34.

authorities applies in the United States to breaches affecting critical infrastructure.[83] We recommend that the FTC set firm deadlines for notification to the FTC - within 72 hours - and for notification to the individuals affected - within 30 days. This will allow consumers to take action to protect themselves from the harms of identity theft.

5.) Enforcement and Redress

- **a.) The FTC shall enforce monetary penalties for primary violations, not just for secondary violations of settlements**
- **b.) The FTC shall set up a clear, user-friendly process for users to submit complaints regarding violations of these rules**

We urge the FTC to issue monetary fines that are commensurate with the violator's revenue and to issue monetary penalties in response to the initial violation, as opposed to waiting until after the company has violated a prior settlement with the FTC.

15 U.S.C. § 45(m)(1)(A) clearly establishes the FTC's authority to issue monetary penalties "against any person, partnership, or corporation which violates any rule under this subchapter respecting unfair or deceptive acts or practices." These penalties are most impactful if they are issued as an initial response to a privacy violation, instead of later in response to settlement violation, as the FTC has often done historically. If the agency issues clear rules, as we have suggested in these comments, that should be sufficient to give companies notice of potentially unfair or deceptive trade practices, which would allow the agency to issue fines in response to a violation.

In order for monetary penalties to be meaningful, they need to be proportionate. The Big Tech companies that are frequent privacy violators make tens or even hundreds of billions of dollars of revenue annually. In order to actually deter bad actions, the penalty has to be large enough to actually impact the company's revenue. The agency's record-breaking 2019 settlement with Facebook for $5 billion is a good starting point, but still amounted to less than 15% of the company's revenue in 2019.[84]

As part of these requirements, the FTC should set up an easy, user-friendly process for submission of complaints regarding violations of the agency's rules. In order to ensure maximum engagement by all members of the population, this process should include options for online submissions, email submissions, submissions by mail, and

---

[83] Ropes and Gray, *Expansive Federal Breach Reporting Requirement Becomes Law,* March 22, 2022, available at: https://www.ropesgray.com/en/newsroom/alerts/2022/March/Expansive-Federal-Breach-Reporting-Requirement-Becomes-Law

[84] Statista, *Meta's Annual Revenue from 2009-2021,* https://www.statista.com/statistics/268604/annual-revenue-of-facebook/

submissions by phone. The submissions process and any tools that are a part of it should be developed with input from a variety of diverse stakeholder communities. The FTC should not simply rely on publications in the Federal Register; the agency should instead participate in active outreach to communities in order to maximize engagement.

Special Rules for Sensitive PII

Sensitive PII presents even greater risks and challenges than regular PII. The United States Department of Homeland Security (DHS) has defined Sensitive PII as "Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual."[85] DHS encourages agency officials to consider the context of the information. Some pieces of information – Social Security numbers, identity document numbers (passports, drivers licenses, etc.), biometric identifiers, and financial account numbers, for example – are inherently sensitive, especially as it pertains to identity theft. Other pieces of information – like personal contact information, mother's maiden name, or date of birth – can be sensitive depending on the context. DHS has recognized that Sensitive PII is deserving of particularly high levels of protection – including stricter access controls, stricter collection limitations, and stronger security measures.

The FTC should begin by defining, for its own purposes, what is Sensitive PII. We would encourage the agency to include, at a minimum, the categories of information the DHS has listed, but also to explicitly include medical/health information, information about protected class identities (sex, gender identity, sexual orientation, race, ethnicity, religion, and political affiliation/beliefs), financial information (including not only account numbers, but also purchases, buying patterns, and financial history), and genetic information and other biometric identifiers. Any information about children should also be considered inherently Sensitive PII – as is the basis for the Children's Online Privacy Protection Act.

Collection and use of Sensitive PII should be governed by stricter rules than regular PII. Even if the agency does not decide to adopt the general ban on secondary uses of PII that we would advocate for, the agency should at least ban all secondary uses of Sensitive PII. Additionally, there should be a strict prohibition on the sharing of Sensitive PII, the use of Sensitive PII for any targeted advertising, and it should be as easy as possible for the consumer to rescind a company's right to retain the Sensitive PII at any

[85] U.S Department of Homeland Security, *DHS Policy Directive 047-01-007 Handbook for Safeguarding Sensitive Personally Identifiable Information*, available at: https://www.dhs.gov/sites/default/files/publications/dhs%20policy%20directive%20047-01-007%20handbook%20for%20safeguarding%20sensitive%20PII%2012-4-2017.pdf

time (ideally with one, prominently displayed button). Any breach of Sensitive PII should be a per se unfair practice, subject to stricter monetary penalties than an ordinary breach.

Conclusion

For the reasons discussed above, the FTC should issue comprehensive privacy rules that embody the FIPPS, including rules that require transparency about data collection and use, minimization of data collection, specific use prohibitions, access and correction rights, security requirements, and monetary penalties. Additional rules should be created around particularly harmful practices and particularly sensitive information.

Sincerely,

Ginger Quintero-McCall
Legal Director
Demand Progress Education Fund
ginger@demandprogress.org

Sean Vitka
Senior Policy Counsel
Demand Progress

David Segal
Executive Director
Demand Progress Education Fund