Comments of Consumer Reports
In Response to the
Federal Trade Commission
Advanced Notice of Proposed Rulemaking on
Commercial Surveillance and Data Security

By

Justin Brookman, Director of Technology Policy
Sumit Sharma, Senior Researcher, Technology Competition
Nandita Sampath, Policy Analyst

November 21, 2022

Consumer Reports[1] appreciates the opportunity to provide feedback on the Federal Trade Commission's Advanced Notice of Proposed Rulemaking on Commercial Surveillance and Security. We thank the Commission for initiating this proceeding and for its other efforts to rein in excessive commercial data practices.

Despite decades of FTC enforcement actions, consumer data today is routinely sold, shared, and monetized without meaningful disclosure or an opportunity to intervene, let alone consumer permission. Companies who possess consumer data do not take adequate measures to protect that data from outside attack. To address the failure to date of industry and policymakers to conform data practices to consumer preferences and expectations, we recommend the Commission promulgate a number of separate rules:

- **Data Minimization Rule**: Companies should be required to limit data collection, use, retention, and sharing to what is reasonably necessary to provide a service or conduct an activity that a consumer has requested, with limited additional permitted operational uses. This Rule should also include the principle of Non-Retaliation — that companies should not be allowed to discriminate or offer differential treatment to consumers who do not agree to unrelated data processing activities.
    - Alternatively, companies should be required to offer consumers the ability to opt out of most secondary uses and data sharing, including through universal opt-out mechanisms such as platform-level signals. These opt-out rights should also be subject to Non-Retaliation obligations — companies cannot discriminate against users who opt out of secondary data processing and sharing.

[1] Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers' interests, including their interest in securing effective privacy protections. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

- **Data Security Rule**: Companies should be required to implement and maintain reasonable security procedures and practices to safeguard personal information.
- **Nondiscrimination Rule**: Companies should be prohibited from discriminating against protected classes such as race, religion, gender identity, and sexuality in the provision of economic opportunities and public accommodations. This rule should be supplemented by rules specifically for automated data processing, such as a requirement for substantiation, explainability, and in some cases third-party auditing.
- **Access, Correction, Portability, and Deletion Rule**: Companies should offer consumers the right to access, correct, move, and delete their data with limited exceptions.
- **Transparency Rule**: Companies should provide standardized and simple instructions to users on how to take advantage of new legal rights, and large companies should be required to provide detailed information about data processing practices to provide for external accountability.

We describe these proposed Rules in detail below in the course of providing answers to the Commission's questions posed in the Advanced Notice of Proposed Rulemaking:

a. Harms to Consumers (To what extent do commercial surveillance practices or lax security measures harm consumers?)

This ANPR has alluded to only a fraction of the potential consumer harms arising from lax data security or commercial surveillance practices, including those concerning physical security, economic injury, psychological harm, reputational injury, and unwanted intrusion.

1. **Which practices do companies use to surveil consumers?**

The state of consumer tracking is complex, though well-documented — the FTC already has a robust record of surveillance practices from its yearly PrivacyCon workshops.[2] Online, websites install functionality from dozens of other companies onto their page (typically using invisible pixels), allowing those companies to track users both on that page as well as any others that embed the same company's functionality. As a result, large ad tech companies such as Google and Facebook have visibility into a large percentage — if not a majority — of all online web traffic.[3] Traditionally this tracking has been done through the use of cookies, though companies have resorted to other technologies to circumvent the limitations of cookies or to frustrate consumers' efforts to limit tracking.[4]

On mobile devices, companies have typically used mobile IDs generated by the mobile OS to replicate cookie technology, though Apple now requires consent from consumers before third parties are allowed access. As a result, as companies have sought to circumvent the limitations of cookies, many companies are looking for alternative solutions to track mobile app users.[5]

---

[2] *E.g.*, *PrivacyCon 2022*, Federal Trade Commission, (Nov. 1, 2022), https://www.ftc.gov/news-events/events/2022/11/privacycon-2022.

[3] Market Study Final Report, The role of data in digital advertising, Online platforms and digital advertising, United Kingdom Competition and Markets Authority, (Jul. 1, 2020), Appendix F, ¶ 43, https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study#final-report; Justin Brookman *et al*., *Cross-Device Tracking: Disclosures and Measurements*, Privacy Enhancing Technologies Symposium (PETS) 2017 (2):133–148, https://petsymposium.org/2017/papers/issue2/paper29-2017-2-source.pdf; Steven Englehardt and Arvind Narayanan, *Online Tracking: A 1-million-site Measurement and Analysis*, ACM CCS 2016, https://www.cs.princeton.edu/~arvindn/publications/OpenWPM_1_million_site_tracking_measurement.pdf .

[4] Press Release, Digital Advertising Company Settles FTC Charges It Deceptively Tracked Consumers Both Online and Through Their Mobile Devices, Federal Trade Commission, (Dec. 20, 2016), https://www.ftc.gov/news-events/news/press-releases/2016/12/digital-advertising-company-settles-ftc-charges-it-deceptively-tracked-consumers-both-online-through; Press Release, Online Advertiser Settles FTC Charges ScanScout Deceptively Used Flash Cookies to Track Consumers Online, Federal Trade Commission, (Nov. 8, 2011), https://www.ftc.gov/news-events/news/press-releases/2011/11/online-advertiser-settles-ftc-charges-scanscout-deceptively-used-flash-cookies-track-consumers.

[5] Ionut Ciobotaru, *4 alternatives to cookies and device IDs for marketers*, VentureBeat, (May 30, 2021),, https://venturebeat.com/marketing/4-alternatives-to-cookies-and-device-ids-for-marketers/.

Offline behavior can be correlated with other offline and online activities by matching identifiers, such as phone number, email addresses or even credit card numbers.[6] Over the years a robust data broker industry has developed around the buying and selling of personal data.[7] California law requires companies to register as a data broker each year with the state; the California data broker registry currently lists over 500 different companies.[8]

In the physical world, cameras are becoming both cheaper and more sophisticated. Improving facial-[9] and gait-recognition[10] technologies give companies the ability to identify consumers in public spaces, potentially without their awareness let alone their consent. Similarly, our phones are constantly broadcasting identifiers to the world that could be combined with real-name identifiers and used to track us as we go about our lives.[11] Companies and researchers are constantly developing novel methods to track users in unexpected ways, including activating smartphone microphones[12] or accessing smart power meters[13] to try to identify television shows that are being watched at home.

As data collection, storage, and processing techniques continue to evolve, every aspect of our personal lives will be technologically observable and interpretable — quite possibly

---

[6] Burt Helm, *Credit card companies are tracking shoppers like never before: Inside the next phase of surveillance capitalism*, Fast Company, (May 12, 2020), https://www.fastcompany.com/90490923/credit-card-companies-are-tracking-shoppers-like-never-before-inside-the-next-phase-of-surveillance-capitalism.

[7] Federal Trade Commission Report, *Data Brokers: A Call for Transparency and Accountability*, (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[8] *Data Broker Registry*, State of California Department of Justice, https://oag.ca.gov/data-brokers. This figure does not count an additional nearly 100 incomplete registrations from companies who have not yet paid their annual registration fee.

[9] Thorin Klosowski, *Facial Recognition Is Everywhere. Here's What We Can Do About It.*, New York Times, (Jul. 15, 2020), https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/.

[10] Darek Shanahan, *Gait Recognition: Using Deep Learning to Collect Better Data*, EXER, (Mar. 9, 2022), https://www.exer.ai/posts/gait-recognition-using-deep-learning-to-collect-better-data.

[11] Press Release, *Retail Tracking Firm Settles FTC Charges it Misled Consumers About Opt Out Choices*, Federal Trade Commission, (Apr. 23, 2015), https://www.ftc.gov/news-events/news/press-releases/2015/04/retail-tracking-firm-settles-ftc-charges-it-misled-consumers-about-opt-out-choices.

[12] Press Release, *FTC Issues Warning Letters to App Developers Using 'Silverpush' Code*, Federal Trade Commission, (Mar. 17, 2016), https://www.ftc.gov/news-events/news/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpush-code.

[13] Elinor Mills, *Researchers find smart meters could reveal favorite TV shows*, CNET, (Jan. 4, 2012), https://www.cnet.com/news/privacy/researchers-find-smart-meters-could-reveal-favorite-tv-shows/.

including our very thoughts and memories.[14] Legal and policy limitations will be needed to preserve zones of privacy where people can live their lives without constant observation and judgment.

2. Which measures do companies use to protect consumer data?

Since bringing its first enforcement actions under its unfairness authority in 2005, the FTC has been clear to companies that they are required to use reasonable data security measures to protect consumer data from outside attack.[15] Moreover, in addition to their own consumer protection statutes, more than half the states have dedicated cybersecurity laws, though they vary significantly in scope and prescriptiveness.[16]

Nevertheless, due to limited enforcement and limited consequences for companies subject to enforcement actions, many companies today fail to take reasonable measures to safeguard personal information. This is especially true when it comes to *security updates*. While desktop operating systems such as Windows and iOS are generally supported for years, other connected devices receive little if any security support. In 2018, the Federal Trade Commission published the results of its Section 6(b) study into security updates provided to mobile phones.[17] The report demonstrated that most manufacturers provided security updates for their phones for less than two years — some expensive flagship phones received no security updates at all and were vulnerable to attack from the moment they were purchased.[18] Some manufacturers could not even provide data about how long phones were supported as they did not keep records documenting whether and when security updates were deployed.

---

[14] Grace van Deelen, *Researchers Report Decoding Thoughts from fMRI Data*, TheScientist, (Oct. 20, 2022), https://www.the-scientist.com/news-opinion/researchers-report-decoding-thoughts-from-fmri-data-70661.
[15] Press Release, *BJ's Wholesale Club Settles FTC Charges*, Federal Trade Commission, (Jun. 16, 2005), https://www.ftc.gov/news-events/news/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges.
[16] Data Security Laws | Private Sector, National Council of State Legislatures, (May 29. 2019), https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.
[17] Press Release, *FTC Recommends Steps to Improve Mobile Device Security Update Practices*, Federal Trade Commission, (Feb. 2018), https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-recommends-steps-improve-mobile-device-security-update-practices.
[18] Report, *Mobile Security Updates: Understanding the Issues*, Federal Trade Commission, (Feb. 2018), https://www.ftc.gov/system/files/documents/reports/mobile-security-updates-understanding-issues/mobile_security_updates_understanding_the_issues_publication_final.pdf.

The state of Internet of Things security is even more chaotic. As summarized by a recent Atlantic Council report:

> The current IoT ecosystem is rife with insecurity. Companies routinely design and develop IoT products with poor cybersecurity practices, including weak default passwords, weak encryption, limited security update mechanisms, and minimal data security processes on devices themselves. Governments, consumers, and other companies then purchase these products and deploy them, often without adequately evaluating or understanding the cybersecurity risk they are assuming. For example, while the US government has worked to develop IoT security considerations for products purchased for federal use, private companies routinely buy and deploy insecure IoT products because there is no mandatory IoT security baseline in the United States.[19] [citations omitted]

As companies increasingly build connectivity and smart features into their products, they are increasingly dependent upon the manufacturer for continued security and cloud processing support. While the FTC has taken a handful of actions against companies who do not support devices for the reasonable lifespan of the product,[20] there are few norms or consistent practices across the industry.[21]

3. **Which of these measures or practices are prevalent? Are some practices more prevalent in some sectors than in others?**

If the Commission defines the loss of consumer utility derived from unwanted surveillance as a substantial injury (see *infra* Question 4), then demonstrating prevalence is a trivial exercise. There is no shortage of papers and investigations detailing the myriad ways that consumer data is sold and shared, online and off (*see supra* Question 1). Many of these papers

---

[19] Patrick Mitchell *et al.*, *Security in the billions: Toward a multinational strategy to better secure the IoT ecosystem*, Atlantic Council, (Sep. 26, 2022), https://www.atlanticcouncil.org/in-depth-research-reports/report/security-in-the-billions/.
[20] Closing Letter, *Nest Labs, Inc.*, Federal Trade Commission, (Jul. 7, 2016), https://www.ftc.gov/system/files/documents/closing_letters/nid/160707nestrevolvletter.pdf.
[21] Xu Zou, *IoT devices are hard to patch: Here's why—and how to deal with security*, TechBeacon, https://techbeacon.com/security/iot-devices-are-hard-patch-heres-why-how-deal-security.

were presented at PrivacyCons hosted by the Federal Trade Commission;[22] indeed, much of the research has been generated by the Federal Trade Commission itself.[23] The record easily justifies the enactment of a Data Minimization Rule to address widespread secondary collection, sharing, use, and retention of personal data.

Similarly, despite the FTC's data security enforcement record since 2005, poor data security practices in the industry are rampant (*see supra*, Question 2 for more details). For several years, identity theft has been the single biggest source of complaints to the Federal Trade Commission from the public; last year, the Commission received 2.8 million complaints from consumers representing $5.9 billion dollars in losses, with a median loss of $500.[24] The record here or prevalent violations justifies the promulgation of a Security Rule.

We defer to other privacy and civil rights organizations to develop the record of prevalence to justify a Nondiscrimination Rule.

We are unaware of any thorough investigation into the state of companies' access, correction, portability, and deletion practices. However, it is worth noting that laws affording these rights exist only in five states, and for the most part those laws are not even in effect yet. Moreover, Consumer Reports research has documented the practical difficulties in exercising privacy rights under the California Consumer Privacy Act, indicating that additional rules are needed in order to make rights accessible to consumers.[25]

---

[22] *E.g.*, *PrivacyCon 2022*, Federal Trade Commission, (Nov. 1, 2022), https://www.ftc.gov/news-events/events/2022/11/privacycon-2022

[23] Justin Brookman *et al.*, *Cross-Device Tracking: Disclosures and Measurements*, Privacy Enhancing Technologies Symposium (PETS) 2017 (2):133–148, https://petsymposium.org/2017/papers/issue2/paper29-2017-2-source.pdf; Federal Trade Commission Report, *Data Brokers: A Call for Transparency and Accountability*, (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[24] Federal Trade Commission, *New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021*, (Feb. 22, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0.

[25] *See* Attachment 3, Maureen Mahoney, *California Consumer Privacy Act: Are Consumers' Digital Rights Protected?*, Consumer Reports, (Oct.1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2021/05/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf2.pdf. *See also* Maureen Mahoney, Ginny Fahs, and Don Marti, *The State of Authorized Agent Opt Outs Under the California Consumer Privacy Act*, (Feb. 21, 2021), https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_AuthorizedAgentCCPA_022021_VF_.pdf

For discussion of the justification for a Transparency Rule, see Questions 84-85.

4. **How, if at all, do these commercial surveillance practices harm consumers or increase the risk of harm to consumers?**

Rather than focus entirely on specific injuries tied to the collection and use of data, the FTC should recognize that unwanted observation, through excessive data collection and use, is harmful in and of itself. Intrusion upon seclusion has long been recognized as a privacy tort, and consumers will always have a legitimate interest in constraining unnecessary processing of their data.

Consumers have no shortage of reasons to object to the collection and retention of their personal information *per se* even if a company has no immediate plans to do anything with that data. Some of those reasons include:[26]

- **Data breach**: The data could be breached and accessed by outside attackers, or inadvertently exposed to the world.
- **Internal misuse**: Bad actors within the company could access and misuse the data for their own purposes.[27]
- **Loss of economic power and future unwanted secondary use**: Even if the company today has no present plans to use the data, the company could change its mind in the future (privacy policies often reserve broad rights to use personal information for any number of reasons). Such usage could range from the merely annoying (say, retargeted advertising) to price discrimination to selling the information to data brokers who could then use the information to deny consumers credit or employment. Differential pricing is a special concern, as companies with more data about an individual will have a better sense of how

[26] These categories are derived from a paper for the Future of Privacy Forum and the Stanford Center for Internet & Society's "Big Data and Privacy: Making Ends Meet" workshop. For further elaboration on these categories, *see* Justin Brookman and G.S. Hans, *Why Collection Matters: Surveillance as a De Facto Privacy Harm*, (Sep. 30, 2013), https://cdt.org/wp-content/uploads/2018/08/September-2013-Brookman-Hans-Why-Collection-Matters.pdf .

[27] Adrian Chen, *GCreep: Google Engineer Stalked Teens, Spied on Chats*, Gawker (Sep. 14, 2010) http://gawker.com/5637234/gcreep-googleengineer-stalked-teens-spied-on-chats.

much that person is willing to pay for a particular product. This in turn will empower the company to set personal prices closest to that equilibrium point, allowing the company to take relatively more of the consumer surplus from any transaction. This type of first-degree price discrimination is all the more of a concern to consumers as increasing corporate concentration means that consumers have fewer market alternatives.

- **Government access**: Consumers may be legitimately concerned about illegitimate government access to their personal information. TikTok, for example, has been dogged by fears of Chinese government access[28] — fears that appear to be justified.[29] Moreover, in the wake of the *Dobbs* Supreme Court decision, many Americans worry that fertility and health information generated and stored by tech companies may be accessed by states that criminalize abortion access.[30]
- **Chilling effect**: Finally, all these concerns together —along with others, and even with an irrational or inchoately realized dislike of being observed — has a chilling effect on public participation and free expression. 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.[31] The United States was founded on a tradition of anonymous speech. In order to remain a vibrant and innovative society, citizens need room for the expression of controversial — and occasionally wrong — ideas without worry that the ideas will be attributable to them in perpetuity. In a world where increasingly every action is monitored, stored, and analyzed, people have a substantial interest in finding some way to preserve a zone of personal privacy that cannot be observed by others.

---

[28] Jack Sommers, *Nearly half of Americans fear TikTok would give their data to the Chinese government*, Business Insider, (Jul. 15, 2021), https://www.businessinsider.com/nearly-half-of-americans-fear-tiktok-would-give-china-data-2021-7.
[29] Christianna Silva and Elizabeth de Luna, *It looks like China does have access to U.S. TikTok user data*, Mashable, (Nov. 3, 2022), https://mashable.com/article/tiktok-china-access-data-in-us.
[30] Naomi Nix and Elizabeth Dwoskin, *Search warrants for abortion data leave tech companies few options*, Washington Post, (Aug. 12, 2022), https://www.washingtonpost.com/technology/2022/08/12/nebraska-abortion-case-facebook/.
[31] Michel Foucault, *Discipline and Punish: The Birth of the Prison* (1977).

And, in fact, more consumers do feel this way about data collection — a Pew Research Center study showed that *81 percent* of Americans believe that the potential risks of companies collecting data about them outweigh the benefits.[32] This loss of utility from commercial data collection is a substantial injury that the FTC can and should constrain using its Section 5 and Section 18 authorities. Indeed, given the near constant furor over commercial privacy issues over the past decade and more, it would be difficult to argue that privacy concerns are not a significant issue for the vast majority of Americans.

Alternatively, the FTC may decide that there is a stronger case for substantial injury only where consumers have affirmatively objected to data processing (where it would be difficult to argue that a consumer experiences a loss of utility when their deliberate choice is ignored). In that case, the FTC should mandate compliance with global opt-out controls and mechanisms so that consumers are able to meaningfully exercise opt-out rights at scale (*see infra* Questions 80-82). The FTC has previous precedent for the proposition that evading platform-level privacy settings such as the Global Privacy Control is unfair and deceptive. For example, the FTC's recent Zoom settlement held that circumventing platform privacy protections is inherently harmful.[33]

Finally, the current surveillance marketing ecosystem has led to industry consolidation and concentration in the advertising marketplace, leading to giant middlemen such as Google and Facebook extracting more and more of the relative value from advertising transactions. For more details, *see infra* Question 11.

5. **Are there some harms that consumers may not easily discern or identify? Which are they?**

---

[32] Brooke Auxier *et al.*, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[33] Complaint, *In the Matter of Zoom Video Communications, Inc.*, Comm'n File No. 1923167 (Nov. 9, 2020) at ¶ 34-53, https://www.ftc.gov/system/files/documents/cases/1923167zoomcomplaint.pdf.

Yes, but we again urge the Commission not to adopt a reductive view of privacy harms — instead, the FTC should recognize that unwanted data collection and processing inherently imposes significant injury on consumers requiring policy intervention. Certainly, it is difficult for consumers or even sophisticated researchers to track all the unwanted data processing that is happening due to inadequate transparency requirements, company obfuscation, and a lack of visibility into backend data processing and server-to-server data sharing. For more information on the opacity of tracking mechanisms, *see infra* Question 86.

6. **Are there some harms that consumers may not easily quantify or measure? Which are they?**

Yes, but we again urge the Commission not to adopt a reductive view of privacy harms — instead, the FTC should recognize that unwanted data collection and processing inherently imposes significant injury on consumers requiring policy intervention. For more information on the opacity of tracking mechanisms, *see infra* Question 86.

7. **How should the Commission identify and evaluate these commercial surveillance harms or potential harms? On which evidence or measures should the Commission rely to substantiate its claims of harm or risk of harm?**

See response to Question 4 *supra.*

8. **Which areas or kinds of harm, if any, has the Commission failed to address through its enforcement actions?**

The Federal Trade Commission has brought scores of important enforcement actions on privacy, security, and discrimination since forming the Division of Privacy and Identity Protection twenty years ago. Nevertheless, these actions by themselves have been insufficient to deter industry from engaging in the types of practices that are the subject of this proceeding. On privacy, the majority of the FTC's cases have been brought under the Commission's deception authority — as a result, while companies have become more careful to avoid affirmative misstatements in privacy policies and elsewhere, the core data behaviors have often gone

uncontested.[34] The FTC has fitfully used its unfairness authority to challenge data behaviors directly, but there have been too few cases to clearly draw bright lines and proscribe invasive practices. For example, the FTC has argued that television viewing[35] and geolocation[36] are "sensitive" meriting heightened protections and affirmative consent; however, it has not made the same case for web browsing, app usage and shopping — which can be at least as personal and revealing. The FTC should use this proceeding to clarify that *all* personal data merits strong protections, and that data processing should be narrowly limited to what is functionally necessary to deliver the services consumers request..

On data security, despite bringing dozens of cases against companies for insecure practices, many companies fail to take even rudimentary steps to safeguard consumer data (*see supra* Question 2). The FTC's inability to obtain civil penalties or disgorgement of ill-gotten gains combined with the FTC's limited resources and inability to bring a critical mass of cases means that companies are insufficiently incentivized to invest the appropriate level of resources on security. To the contrary, in the current environment, it is rational for companies to underspend on cybersecurity despite the risks to consumers.

9. Has the Commission adequately addressed indirect pecuniary harms, including potential physical harms, psychological harms, reputational injuries, and unwanted intrusions?

For the reasons described in response to Questions 1-4, 8, and 86, the FTC has not adequately addressed indirect pecuniary harms stemming from privacy and security violations.

---

[34] *E.g.*, Press Release, *Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser*, Federal Trade Commission, (Aug. 9, 2012), https://www.ftc.gov/news-events/news/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented-privacy-assurances-users-apples. In this case, the FTC predicated its against Google on a misleading FAQ instead of the underlying practice of circumventing the Safari web browser's privacy controls to place cookies.

[35] Press Release, *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*, Federal Trade Commission, (Feb. 6, 2017), https://www.ftc.gov/news-events/news/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it-collected-viewing-histories-11-million.

[36] Press Release, *FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations*, Federal Trade Commission, (Aug. 29, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other.

10. Which kinds of data should be subject to a potential trade regulation rule? Should it be limited to, for example, personally identifiable data, sensitive data, data about protected categories and their proxies, data that is linkable to a device, or non-aggregated data? Or should a potential rule be agnostic about kinds of data?

The Commission should apply its rule to all data that is reasonably linkable to a person, household, or consumer device. The FTC has recognized for years that limiting personal data to data linked to real-name is outdated;[37] pseudonymous — even hashed data[38] — can often be trivially traced back to real individuals and can otherwise be used to charge different prices, discriminate based on protected characteristics, or otherwise change the user's experience. Thus, the FTC's Rules on Data Minimization, Security, Nondiscrimination, and Transparency should apply to any data reasonably associated with a person, household, or consumer device.[39]

The Commission's Access, Correction, Portability, and Deletion Rule presents its own privacy challenges — mandating access and control over personal data creates an opportunity for bad actors to try to illegitimately exercise the rights of others. As such, this Rule should apply to a narrower set of data — data that is reasonably authenticated to an individual or personal device. Companies should also be required to authenticate requests from consumers to take advantage of these rights.[40]

In general, the FTC does not need to provide special protections for certain sensitive categories of data — instead all data should be subject to rules such as the Data Minimization Rule. It may be reasonable to require heightened and prominent notice to consumers when a company is required to process sensitive data in direct service of a consumer request. However,

---

[37] Lindsey Tonsager, *FTC's Jessica Rich Argues IP Addresses and Other Persistent Identifiers Are "Personally Identifiable"*, Inside Privacy, (Apr. 29, 2016), https://www.insideprivacy.com/united-states/ftcs-jessica-rich-argues-ip-addresses-and-other-persistent-identifiers-are-personally-identifiable/.

[38] Ed Felten, *Does Hashing Make Data "Anonymous"?*, Federal Trade Commission, (Apr. 22, 2012), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2012/04/does-hashing-make-data-anonymous.

[39] We would support a clarification in the Rules that they are not intended to apply to data associated with industrial devices or other categories of devices that are not typically associated with consumers.

[40] See Attachment 2, Consumer Reports, Model State Privacy Act, (Feb. 2021), §§2-105, 2-110, 2-115, 2-120, https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf.

such notice would simply be limited to ensuring that consumers understand when sensitive data is operationally necessary; companies will still be fundamentally constrained to only use this data to respond to a consumer request or for one of a narrow set of permitted business purposes.

While recognizing that even sophisticated and well-intentioned deidentification and aggregation techniques can sometimes be reversed, Consumer Reports believes there is value to incentivizing companies to processing data in deidentified form. We would support an exception to the definition of personal data for deidentified data consistent with the formulation laid out in the FTC's 2012 Privacy Report for data that a company believes it could not reidentify even if it wanted to. We would propose the following language from our State Model Privacy Act:

> "Deidentified" means information that cannot reasonably identify, relate to, describe, reasonably be associated with, or reasonably be linked, directly or indirectly, to a particular consumer, provided that the business:
>
> > (1) Takes reasonable measures to ensure that the data could not be re-identified;
> >
> > (2) Publicly commits to maintain and use the data in a de-identified fashion and not to attempt to reidentify the data; and
> >
> > (3) Contractually prohibits downstream recipients from attempting to re-identify the data.[41]

To provide for external accountability, large companies that seek to take advantage of this provision however should be required to provide detailed documentation in a privacy policy as to their deidentification methods (*see infra* Question 89).[42]

---

[41] *Id.*, §3(h).
[42] *Id.*, §100(b)(9).

11. Which, if any, commercial incentives and business models lead to lax data security measures or harmful commercial surveillance practices? Are some commercial incentives and business models more likely to protect consumers than others? On which checks, if any, do companies rely to ensure that they do not cause harm to consumers?

For security, see response to Questions 2, 4, and 8.

For information about the opacity of commercial surveillance which makes it difficult for consumers to hold companies accountable for their behaviors, see response to Question 86.

Market structure also plays an important role in the current data ecosystem. Without policy interventions that limit commercial surveillance the harms to consumers will continue as the market is broken and will not self-correct

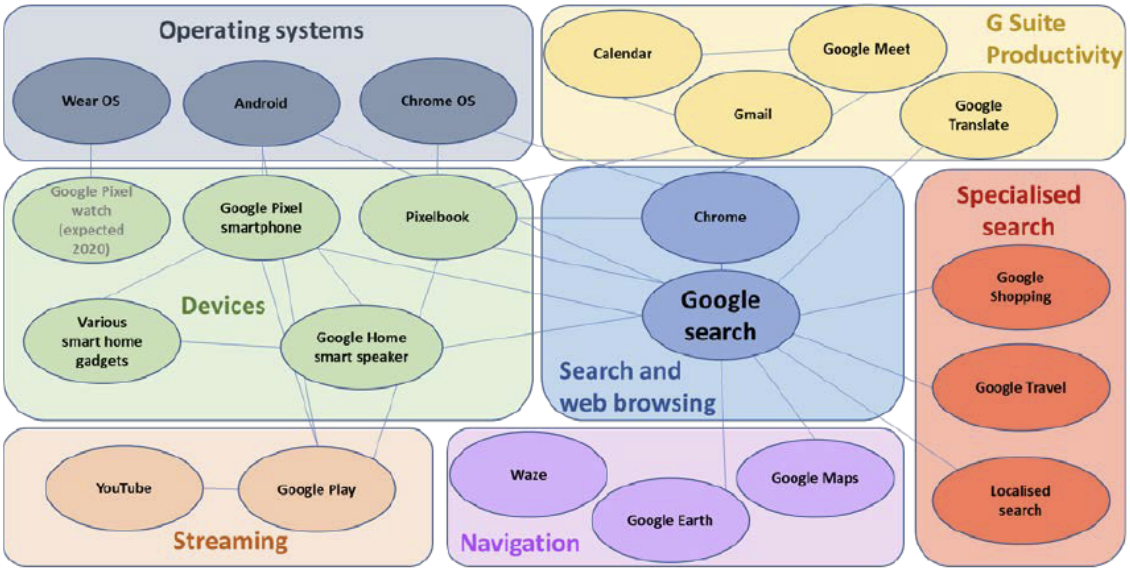
The current online market is dominated by giant online platforms like Facebook and Google that profit from commercial surveillance. This market power is persistent, not temporary. As the recent G7 communique notes:

> There are certain common features present in many digital markets which often lead to firms gaining a large and powerful position. These features may tend to increase market concentration, raise barriers to entry, and strengthen the durability of market power. These common features include: (i) network effects; (ii) multi-sided markets; and (iii) the role of data. This can cause markets to 'tip' in favour [sic] of one or a small number of large firms.[43]

[43] *Compendium of approaches to improving competition in digital markets*, G7 Germany, 12 October 2022. With contributions from Competition Bureau Canada; Autorité de la Concurrence, France; Bundeskartellamt, Germany; Autoritá Garante della Concorrenza e del Mercato, Italy; Japan Fair Trade Commission; UK Competition and Markets Authority, US - Federal Trade Commission and Department of Justice; European Commission Directorate-General for Competition; Australian Competition and Consumer Commission; Competition Commission of India; Competition Commission South Africa; and Korea Fair Trade Commission.

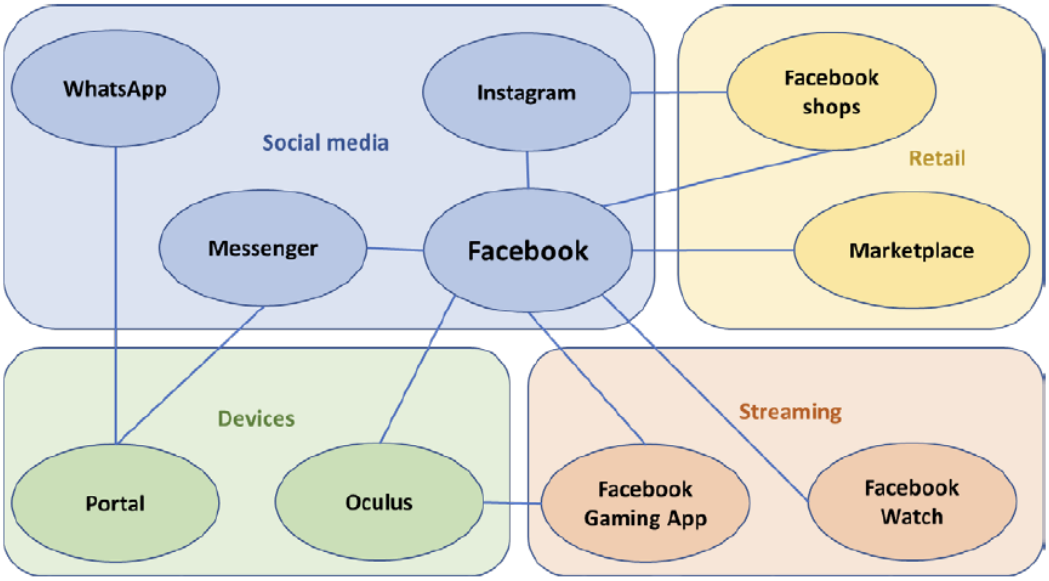
The harmful effects of this market power are widespread as the largest online platforms operate across the digital ecosystem providing a variety of online services and connected devices. The invasive data collection is an important contributor to this market power is also widespread as these giant online platforms can and do collect data from all the different services they provide. Figure 1 illustrates this for Google and Figure 2 does this for Facebook.

Figure 1: Google's online consumer facing services that can be used to collect first party data



Source: Figure E.1, Appendix E: Ecosystems, Online platforms and digital advertising, Market Study Final Report, UK CMA, 1 July 2020.

Figure 2: Facebook's online consumer facing services that can be used to collect first party data

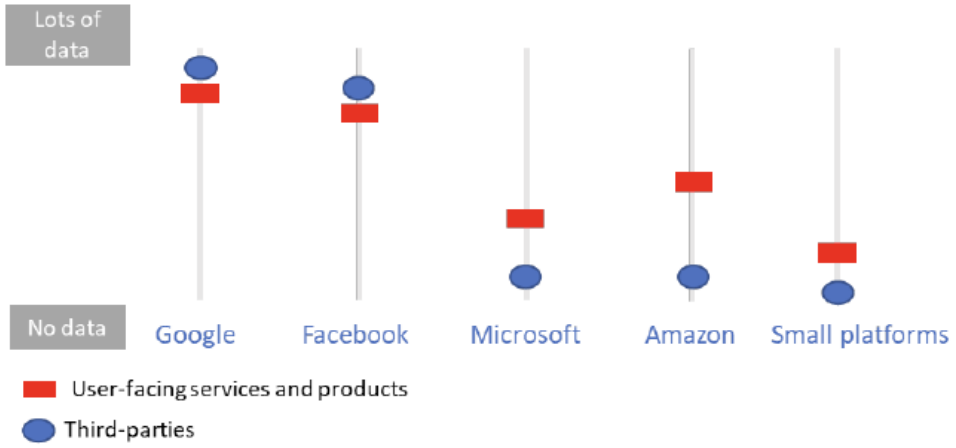


Source: Figure E.2., Appendix E: Ecosystems, Online platforms and digital advertising, Market Study Final Report, UK CMA, 1 July 2020.

In addition to collecting data directly from their own audiences and users, Google and Facebook also have an unmatched ability to collect data from third parties. The UK's CMA reports that multiple studies have found that Google tags are found on over 80% of the most popular websites, and Facebook's between 40-50% of the most popular websites. On mobile apps, Google has SDKs in over 85% of the most popular apps on the Play Store, and Facebook has again the second highest prevalence with SDKs in over 40% of the same.[44] This dominant data position is reflected in Figure 3 below.

Figure 3 : Google and Facebook's unmatched ability to collect data

[44] Market Study Final Report, *The role of data in digital advertising, Online platforms and digital advertising*, United Kingdom Competition and Markets Authority, (Jul. 1, 2020), Appendix F, ¶ 43, https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study#final-report.



Source: CMA.
Note: Small platforms include Twitter, Snap, TikTok and Pinterest.

Source: Figure F.1, Appendix F: The role of data in digital advertising, Online platforms and digital advertising, Market Study Final Report, UK CMA, 1 July 2020

The unmatched advantage of the largest platforms (particularly Google and Facebook) to collect data gives them a competitive advantage in not just in personally targeted advertising but also in providing verification and attribution services to advertisers. This superior ability to provide feedback to advertisers based on their ability to collect data on how the largest variety and number of users interact with the largest variety and number of targeted ads creates a data driven cycle which helps the largest platforms maintain their dominance.

Evidence reviewed by the UK CMA suggests these capabilities to personally target advertising generate higher revenues for both online platforms and publishers compared to other less intrusive forms of advertising like contextual advertising when both are available.

The potential loss of short-term revenues and the persistent dominant position and monopoly profits that platforms like Facebook and Google generate from personalized targeted advertising means the incentives, in the absence of any policy intervention, are skewed to continuing commercial surveillance practices and this is the current market equilibrium we are all stuck in. There is limited scope for alternative more privacy friendly business models like subscription-based models to challenge the status quo.

All this means, the harms to consumers from commercial surveillance will continue without policy intervention. The competitive process is broken and will not come to the rescue.

We need appropriate policy intervention so the market can evolve and move to more privacy enhancing business models in the medium-long term. Appropriate policy intervention could for example incentivize and push the market to develop new privacy enhancing technologies and more sophisticated approaches to contextual advertising. These market wide effects and market evolution are not captured by studies which compare revenues generated via personally targeted advertising and contextual advertising today.

12. **Lax data security measures and harmful commercial surveillance injure different kinds of consumers (e.g., young people, workers, franchisees, small businesses, women, victims of stalking or domestic violence, racial minorities, the elderly) in different sectors (e.g., health, finance, employment) or in different segments or "stacks" of the internet economy. For example, harms arising from data security breaches in finance or healthcare may be different from those concerning discriminatory advertising on social media which may be different from those involving education technology. How, if at all, should potential new trade regulation rules address harms to different consumers across different sectors? Which commercial surveillance practices, if any, are unlawful such that new trade regulation rules should set out clear limitations or prohibitions on them? To what extent, if any, is a comprehensive regulatory approach better than a sectoral one for any given harm?**

The rules promulgated by the Federal Trade Commission should generally be universal in nature. A Nondiscrimination Rule however should prohibit discrimination against protected characteristics such as race, religion, gender identity, or sexual orientation (*see infra* Question 66).

b. Harms to Children To what extent do commercial surveillance practices or lax data security measures harm children, including teenagers?)

13. **The Commission here invites comment on commercial surveillance practices or lax data security measures that affect children, including teenagers. Are there**

practices or measures to which children or teenagers are particularly vulnerable or susceptible? For instance, are children and teenagers more likely than adults to be manipulated by practices designed to encourage the sharing of personal information?

In general, we do not believe that the Commission should issue children- or teen-specific rules through this proceeding. First, there is already an existing framework for childrens' data collection and surveillance advertising — the Children's Online Privacy Protection Act. That law was passed in 1998 and postdates Section 5 of the FTC Act by fifty years. Enacting sector-specific rules through Section 5 on an area where Congress has subsequently legislated invites legal challenge as to whether the FTC retains the authority to issue such rules.

Perhaps more importantly, age-specific privacy protections create their own privacy issues, as determining whether or not a particular consumer is a child or not is intrinsically privacy-invasive. For example, the recently enacted Age Appropriate Design Code in California has been criticized for raising the prospect that companies will feel compelled to collect additional data or even authenticate all users in order to determine whether the law's protections apply.[45]

If the Commission does decide to issue children- or teen-specific rules, we urge it to clarify that companies are *not* mandated to collect additional information from consumers in order to determine if the children- or teen-specific rules apply. If a company's target audience is children or teens, then the rules should apply. If the company reasonably believes that a particular consumer is a child or teen, the rules should apply. Companies could even be explicitly required to analyze existing data that it possesses about a consumer or device in order to make that determination. But a mandate to collect additional data — or worse, to authenticate users — would be counterproductive and deeply deleterious for privacy.

Again, however, we do not believe that child- or teen-specific rules are necessary. Instead, the Commission should issue robust general purpose rules that will protect everyone by default. That way, consumers will not be stripped of reasonable privacy protections the moment

[45] Thomas Claburn, *California Governor signs child privacy law requiring online age checks*, The Register, (Sep. 15, 2022), https://www.theregister.com/2022/09/15/california_aaca_act_signed/.

they turn 14 or 18 — instead, they will be able to assume their privacy rights will be honored throughout their lifetimes.

14. **What types of commercial surveillance practices involving children and teens' data are most concerning? For instance, given the reputational harms that teenagers may be characteristically less capable of anticipating than adults, to what extent should new trade regulation rules provide teenagers with an erasure mechanism in a similar way that COPPA provides for children under 13? Which measures beyond those required under COPPA would best protect children, including teenagers, from harmful commercial surveillance practices?**
15. **In what circumstances, if any, is a company's failure to provide children and teenagers with privacy protections, such as not providing privacy-protective settings by default, an unfair practice, even if the site or service is not targeted to minors? For example, should services that collect information from large numbers of children be required to provide them enhanced privacy protections regardless of whether the services are directed to them? Should services that do not target children and teenagers be required to take steps to determine the age of their users and provide additional protections for minors?**
16. **Which sites or services, if any, implement child-protective measures or settings even if they do not direct their content to children and teenagers?**
17. **Do techniques that manipulate consumers into prolonging online activity (e.g., video autoplay, infinite or endless scroll, quantified public popularity) facilitate commercial surveillance of children and teenagers? If so, how? In which circumstances, if any, are a company's use of those techniques on children and teenagers an unfair practice? For example, is it an unfair or deceptive practice when a company uses these techniques despite evidence or research linking them to clinical depression, anxiety, eating disorders, or suicidal ideation among children and teenagers?**
18. **To what extent should trade regulation rules distinguish between different age groups among children (e.g., 13 to 15, 16 to 17, etc.)?**
19. **Given the lack of clarity about the workings of commercial surveillance behind the screen or display, is parental consent an efficacious way of ensuring child online**

privacy? Which other protections or mechanisms, if any, should the Commission consider?

20. **How extensive is the business-to-business market for children and teens' data? In this vein, should new trade regulation rules set out clear limits on transferring, sharing, or monetizing children and teens' personal information?**
21. **Should companies limit their uses of the information that they collect to the specific services for which children and teenagers or their parents sign up? Should new rules set out clear limits on personalized advertising to children and teenagers irrespective of parental consent? If so, on what basis? What harms stem from personalized advertising to children? What, if any, are the prevalent unfair or deceptive practices that result from personalized advertising to children and teenagers?**
22. **Should new rules impose differing obligations to protect information collected from children depending on the risks of the particular collection practices?**
23. **How would potential rules that block or otherwise help to stem the spread of child sexual abuse material, including content-matching techniques, otherwise affect consumer privacy?**

Dozens of essential consumer applications rely heavily on cryptography, including both encryption and digital signatures, in order to function, including:

- Consumers' health records, medical devices, and virtual healthcare visits;
- Personal banking transactions, online credit card use, and mobile payments;
- Software updates to our laptops, phones, and other devices;
- Billions of connected devices, including smart home appliances and the software in our cars;
- Emergency broadcast systems and other public communications channels;
- Nationally important infrastructure, including air traffic systems; and
- Emails, text messages, voice calls, and social media.[46]

[46] For a more thorough discussion of these and other consumer applications that depend on uncompromised cryptography, *see Beyond Secrets: The Consumer Stake in the Encryption Debate*, Consumers Union, (Dec. 21, 2017), https://advocacy.consumerreports.org/wp-content/uploads/2017/12/Beyond-Secrets-12.21.17-FINAL.pdf.

Consumer Reports would oppose any Rule that fundamentally compromises the effectiveness of cryptography, including mandated backdoors.[47]

c. Costs and Benefits (How should the Commission balance costs and benefits?)

24. The Commission invites comment on the relative costs and benefits of any current practice, as well as those for any responsive regulation. How should the Commission engage in this balancing in the context of commercial surveillance and data security? Which variables or outcomes should it consider in such an accounting? Which variables or outcomes are salient but hard to quantify as a material cost or benefit? How should the Commission ensure adequate weight is given to costs and benefits that are hard to quantify?

The FTC's unfairness authority prohibits commercial practices whose harm is not offset by countervailing benefits to consumers or competition. For this reason, the FTC's data security cases inherently involve a balancing test — if the cost of the security measures outweighs the security benefit to consumers, then companies do not have to implement them. Any Data Security Rule should be clear that only cost-effective and reasonable measures are required.

On Data Minimization, ad tech firms likely might argue that the economic benefits of ad targeting would also outweigh injuries resulting from unwanted surveillance, though estimates of these benefits vary widely, as do estimates of to whom those benefits accrue (*see infra* Question 42). Under Section 5, only the benefits that accrue to consumers or competition are relevant for consideration. As discussed above (*supra* Question 11) and in Accountable Tech's rulemaking petition,[48] there is a strong argument that the current behavioral advertising model has led to the consolidation of market power by giant technology companies such as Google and Facebook. Those two companies are also the biggest beneficiaries of secondary data collection, as they collect data from more third-party websites and mobile applications than any other business (*see supra* Question 1).

---

[47] Some advocates have argued that mandated client-side scanning and content matching fundamentally compromises the effectiveness of encryption technologies. *See* Erica Portnoy, *Why Adding Client-Side Scanning Breaks End-To-End Encryption*, Electronic Frontier Foundation, (Nov. 1, 2019), https://www.eff.org/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption

[48] Accountable Tech, *Petition for Rulemaking to Prohibit Surveillance Advertising* (Sept. 28, 2021), https://accountabletech.org/wp-content/uploads/Rulemaking-Petition-to-Prohibit-SurveillanceAdvertising.pdf.

Advertising firms might also argue that free online content is funded by secondary data collection, though ads have supported online content for decades, and few online ads were precisely behaviorally targeted to consumers until recent years (*see infra* Question 41). It is not clear that incrementally much more content is available because of behavioral ads, and if so what the quality and marginal value to consumers of such content is. One recent report from Carnegie Mellon found that individually targeted ads only increased publishers' advertising revenue by 4%, with an incremental increase of revenue of approximately $0.00008 per ad.[49] Even assuming some degree of value trickles down to consumers, it likely is not enough to offset the harms and loss of utility that consumers experience as a result of profligate data disclosure and secondary processing.

25. **What is the right time horizon for evaluating the relative costs and benefits of existing or emergent commercial surveillance and data security practices? What is the right time horizon for evaluating the relative benefits and costs of regulation?**
26. **To what extent would any given new trade regulation rule on data security or commercial surveillance impede or enhance innovation? To what extent would such rules enhance or impede the development of certain kinds of products, services, and applications over others?**

A Security Rule would require companies to expend resources to protect consumer data. However, this Rule would only mandate reasonable measures where the cost of the measures is less than the risk to consumers. At the margins there is some risk of ambiguity about the optimal level of expenditure, but on its face the Rule would only mandate societally efficient outlays.

A Nondiscrimination Rule would only prohibit discrimination against protected classes in the provision of economic opportunities or public accommodations. It is difficult to imagine what legitimate innovation such a rule would hinder. There may be narrow cases where such

[49] Veronica Marotta, Vibhanshu Abhishek, & Alessandro Acquisti, *Online Tracking and Publishers' Revenues: An Empirical Analysis*, Workshop on the Economics of Information Security (2019), https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf.

discrimination is justifiable — such as the offering of scholarships aimed at historically disadvantaged groups. However, the Rule can be written to allow for this type of discrimination designed to remedy historical wrongs.

For most companies, a Transparency Rule will simply require them to provide clear instructions on how to take advantage of new rights — this should have little impact on innovation. Large companies will have to spend money to document in detail data processing behaviors, but the benefits to public availability of information and external accountability should outweigh those costs.

An Access, Correction, Portability, and Deletion Rule would require expenditures of resources; however, it is worth noting that most companies are already required to make these expenditures in response to the GDPR and state specific requirements. Requiring companies to extend the use of already established processes and procedures would have limited incremental costs.

Finally, a Data Minimization law would only limit companies from engaging in offensive data behaviors such as the unwanted sharing of personal data with other companies. In truth, there has been far too much innovation in that space over the last thirty years. While many companies engage in such data monetization today, the benefits have mostly accrued to the largest companies such as Google and Facebook; it is debatable how much value seeps down to individual others in the ecosystem (*see infra* Question 41-42). Indeed, the rise of behavioral targeting has coincided with the growing dominance of these large platforms and shrinking revenues for smaller publishers (*see supra* Question 11).

Overall we share the view of the UK's Competition and Markets Authority and the Information Commissioner's office that:

> well-designed regulation and standards that preserve individuals' privacy and place individuals in control of their personal data can serve to promote effective competition and enhance privacy. This is achieved by ensuring that competitive pressures help drive innovations that genuinely benefit users, rather than encouraging behaviour [sic] that undermines data protection and privacy rights. With appropriate regulation, competitive pressures can be harnessed to drive innovations that protect and support users, such as the development of privacy-friendly technologies, clear, user-friendly controls, and the creation of

tools that support increased user-led data mobility. The incentives to deliver these forms of innovation are greater in the presence of targeted regulation than without.[50]

27. Would any given new trade regulation rule on data security or commercial surveillance impede or enhance competition? Would any given rule entrench the potential dominance of one company or set of companies in ways that impede competition? If so, how and to what extent?

See our response to Question 11 above.

28. Should the analysis of cost and benefits differ in the context of information about children? If so, how?

Consumer Reports recommends that the Commission's rulemaking focus on the general populace, not just children.

29. What are the benefits or costs of refraining from promulgating new rules on commercial surveillance or data security?

As discussed above (*see supra* Questions 1-4, 8), the FTC's case-by-case approach on privacy and security has been insufficient to meaningfully deter unwanted secondary use and tracking or to ensure consistent reasonable data security practices. If the FTC fails to issue regulations, consumers will continue under the status quo regime, where companies routinely collect and share personal data for their own purposes contrary to consumer interests and preferences, and consumer information is inadequately protected from attack. Consumers have waited for more than twenty years for Congress to try to pass comprehensive privacy legislation; during that period, the FTC has bided its time and withheld from issuing regulations under its

[50] *Competition and data protection in digital markets: a joint statement between the CMA and the ICO, UK CMA and ICO*, (May 19, 2021), at 61 https://ico.org.uk/media/about-the-ico/documents/2619797/cma-ico-public-statement-20210518.pdf.

Section 5 authority.[51] With the prospects of federal legislation in the near future continuing to look dim, the Commission should belatedly exercise its powers to protect consumers.[52]

d. Regulations (How, if at all, should the Commission regulate harmful commercial surveillance or data security practices that are prevalent?)

I. Rulemaking Generally

30. Should the Commission pursue a Section 18 rulemaking on commercial surveillance and data security? To what extent are existing legal authorities and extralegal measures, including self-regulation, sufficient? To what extent, if at all, are self-regulatory principles effective?

Yes, the Commission should pursue a Section 18 rulemaking on commercial surveillance and data security. Specifically we recommend the Commission pursue at least five separate rules:

- Data Minimization Rule (including the principle of Non-Retaliation)
- Security Rule
- Nondiscrimination Rule (including special rules for automated data processing)
- Transparency Rule
- Access, Correction, Portability, and Deletion Rule

As is evidenced by the prevalence of unwanted data processing and security breaches described above (supra, Questions 1-4, 8), existing legal frameworks and self-regulatory efforts have been insufficient to address the core privacy and security issues.

On Data Minimization, six states have passed laws giving consumers the right to opt out of the sale, sharing, and/or use of their data for targeting advertising. However, most of those

---

[51] Patrick Thibodeau, *FTC, Senator seek online privacy rules*, (May 26, 2000), https://www.computerworld.com/article/2594822/ftc--senator-seek-online-privacy-rules.html.
[52] Vincent Smolczynski, *United States: Federal Data Privacy Law May Have Hit Roadblock*, Mondaq, (Nov. 14, 2022), https://www.mondaq.com/unitedstates/privacy-protection/1250474/federal-data-privacy-law-may-have-hit-roadblock.

laws are not even in effect yet, and opt-out rights have proven difficult to use in practice.[53] The California Privacy Protection Act has been in place the longest; however, even for that law, there has only been one enforcement action to date.[54] Industry self-regulation has been performative and ineffectual, as tools offered by trade associations such as the Network Advertising Initiative and the Digital Advertising Alliance are largely unknown, difficult to use, apply only to member companies, do little to address underlying data collection, and are often, frankly, broken.[55] Industry leaders agreed to voluntarily honor browser "Do Not Track" signals in lieu of regulation during the Obama administration;[56] however, once the threat of legislation had abated, companies eventually abandoned their commitments, and browser Do Not Track signals are generally ignored by the advertising industry today.[57]

On Access, Correction, Portability, and Deletion, see *supra* Question 3.

---

[53] See Attachment 3, Maureen Mahoney, *California Consumer Privacy Act: Are Consumers' Digital Rights Protected?*, Consumer Reports, (Oct.1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2021/05/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf2.pdf. We are hopeful that recognition that universal opt-out signals are binding legal requests will help make exercising privacy rights easier, as California has mandated that companies comply with Global Privacy Control signals. *See* Press Release, *Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act*, State of California Department of Justice, (Aug. 24, 2022), https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement; *CCPA Frequently Asked Questions*, California Department of Law, https://oag.ca.gov/privacy/ccpa. However, of the only six states that mandate consumer opt-out rights, still fewer — only three — of those specifically mandate compliance with universal signals.

[54] Press Release, *Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act*, State of California Department of Justice, (Aug. 24, 2022), https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement.

[55] Testimony of Justin Brookman Director, Privacy and Technology Policy, Consumers Union, Before the House Subcommittee on Digital Commerce and Consumer Protection, Hearing on "Understanding the Digital Advertising Ecosystem," (Jun. 14, 2018), https://docs.house.gov/meetings/IF/IF17/20180614/108413/HHRG-115-IF17-Wstate-BrookmanJ-20180614.pdf; Testimony of Justin Brookman, Director, Consumer Privacy, Center for Democracy & Technology Before the U.S. Senate Committee on Commerce, Science, and Transportation, Hearing on "A Status Update on the Development of Voluntary Do-Not-Track Standards," (Apr. 24, 2013), https://cdt.org/wp-content/uploads/pdfs/Brookman-DNT-Testimony.pdf.

[56] Press Release, *We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online*, The White House, (Feb. 23, 2012), https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.

[57] Glenn Fleishman, *How the tragic death of Do Not Track ruined the web for everyone*, Fast Company (Mar. 17, 2019), https://www.fastcompany.com/90308068/how-the-tragic-death-of-do-not-track-ruined-the-web-for-everyone.

On Nondiscrimination, we refer to the comment of other privacy and civil rights groups on the adequacy of existing legal protections.

On the justification for a Security Rule, *see infra* Question 31 and *supra* Question 2.

On Transparency, *see infra* Questions 83-85.

II. Data Security

31. Should the Commission commence a Section 18 rulemaking on data security? The Commission specifically seeks comment on how potential new trade regulation rules could require or help incentivize reasonable data security.

Yes, the Commission should commence a Section 18 rulemaking on data security. As discussed above, while the FTC has a strong enforcement record, the threat of a potential action has been insufficient to incentivize companies to invest sufficient resources on security (*see supra* Question 2). The FTC should implement a rule incorporating the agency's long-standing policy that Section 5 of the FTC Act requires companies to use reasonable safeguards to protect consumer data (*see infra* Question 32).

The FTC should also clarify that companies are obligated to protect connected devices for the reasonable lifetime of those products. Companies should also be required to prominently disclose to consumers the minimum length of time that connected products will be supported.[58] As noted previously, there are few clear norms and expectations when it comes to support periods for Internet of Things devices, and many devices receive little to no continuing support from manufacturers, leaving these devices vulnerable to attack (*see supra* Question 2).

---

[58] *Cf.* Press Release, Statement by NSC Spokesperson Adrienne Watson on the Biden-Harris Administration's Effort to Secure Household Internet-Enabled Devices, The White House, (Oct. 20, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/20/statement-by-nsc-spokesperson-adrienne-watson-on-the-biden-harris-administrations-effort-to-secure-household-internet-enabled-devices/.

32. Should, for example, new rules require businesses to implement administrative, technical, and physical data security measures, including encryption techniques, to protect against risks to the security, confidentiality, or integrity of covered data? If so, which measures? How granular should such measures be? Is there evidence of any impediments to implementing such measures?

Given that the Section 18 process is time-intensive, it will be difficult for the Commission to constantly revise and update the Security Rule. As such, rather than being specific and prescriptive, the Rule should be relatively high-level and principles-based. The nuances of what constitutes a reasonable practice will necessarily evolve as technology evolves; those specific nuances can be captured through the FTC's enforcement record as well as more easily revised informal guidance published by the Commission.

Specifically, while we are flexible as to the level of detail to be contained in a Security Rule, we would recommend an approach comparable to the language contained in the Consumer Reports Model State Privacy Act:

> Reasonable security. (a) A business or service provider shall implement and maintain reasonable security procedures and practices, including administrative, physical, and technical safeguards, appropriate to the nature of the information and the purposes for which the personal information will be used, to protect consumers' personal information from unauthorized use, disclosure, access, destruction, or modification.[59]

Alternatively, the Commission could adopt a somewhat more prescriptive approach, such as the approach taken in the American Data Privacy and Protection Act that passed the House Energy and Commerce Committee this summer by a 53-2 vote.[60] However, we feel that level of

---

[59] *See* Attachment 2, Consumer Reports, *Model State Privacy Act*, (Feb. 2021), § 2-128, https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf.

[60] See American Data Privacy and Protection Act, H.R. 8152, 117th Cong., § 208, https://www.congress.gov/bill/117th-congress/house-bill/8152/text#toc-H4B489C75371741CBAA5F38622BF082DE.

detail is unnecessary and may impose unreasonable burdens on small businesses. We would recommend against a highly detailed and prescriptive approach such as is contained in some state regulations.[61]

As discussed above, we also recommend that the FTC's regulations clarify that connected device manufacturers are required to provide product security support for the reasonable life of those products, and that they be required to make prominent pre-purchase disclosures to consumers about the minimum period for which those products will be supported (*see supra* Question 31).

33. Should new rules codify the prohibition on deceptive claims about consumer data security, accordingly authorizing the Commission to seek civil penalties for first-time violations?

Yes, in addition to affirmatively requiring reasonable data security, the Security Rule should codify Section 5's prohibition on deceptive claims about data security. While many of the Commission's security enforcement actions to date have included charges related to deceptive statements, the relatively low risk of getting caught combined with the FTC's lack of penalty authority has proven to be insufficient to deter companies from overstating the effectiveness of their solutions or otherwise misleading consumers about the scope of protections.[62] Prohibiting deceptive practices related to security in a Security Rule would deter potential wrongdoers by significantly raising the potential cost of misleading consumers.

---

[61] *E.g.*, Mass. 201 CMR 17.00: Standards for the protection of personal information of residents of the Commonwealth, https://www.mass.gov/regulations/201-CMR-1700-standards-for-the-protection-of-personal-information-of-residents-of-the-commonwealth.

[62] Amir Tarighat, *Ending deceptive cybersecurity marketing*, Fast Company, (Jul. 29, 2022), https://www.fastcompany.com/90771546/ending-deceptive-cybersecurity-marketing ("Fewer industries suffer from more blatant misinformation in their marketing campaigns than cybersecurity. The primary goal of cybersecurity companies is to keep people safe. However, many of these companies target unsophisticated consumers with misleading ads that misrepresent what their products actually do. In some instances, cybersecurity companies may even make people less safe.").

34. **Do the data security requirements under COPPA or the GLBA Safeguards Rule offer any constructive guidance for a more general trade regulation rule on data security across sectors or in other specific sectors?**
35. **Should the Commission take into account other laws at the state and federal level (e.g., COPPA) that already include data security requirements. If so, how? Should the Commission take into account other governments' requirements as to data security (e.g., GDPR). If so, how?**
36. **To what extent, if at all, should the Commission require firms to certify that their data practices meet clear security standards? If so, who should set those standards, the FTC or a third-party entity?**

The Security Rule does not need to require firms to certify that their data practices meet a separate set of security standards. The Security Rule itself should set forth the relevant legal standard; the specifics of compliance responsibilities will evolve over time and be reflected in the Commission's enforcement cases and informal guidance. We also would object to an explicit safe harbor in the Security Rule for compliance with NIST or industry standards as is included in certain state security laws.[63] Compliance with such standards should be a relevant factor in determining whether a company used reasonable measures or not, but the FTC should not make its legal authority contingent upon an external standard over which it has no control.

III. Collection, Use, Retention, and Transfer of Consumer Data

37. **How do companies collect consumers' biometric information? What kinds of biometric information do companies collect? For what purposes do they collect and use it? Are consumers typically aware of that collection and use? What are the benefits and harms of these practices?**

See response to Question 1.

[63] *See*, *e.g.*, Ohio Revised Code, Title 13, Chapter 1354, § 1354.2 ("Safe harbor requirements"), https://codes.ohio.gov/ohio-revised-code/section-1354.02.

38. **Should the Commission consider limiting commercial surveillance practices that use or facilitate the use of facial recognition, fingerprinting, or other biometric technologies? If so, how?**

The Commission should issue rules on Data Minimization, Security, Nondiscrimination, Transparency, and Access, Correction, Portability, and Deletion of general applicability. These rules should apply to the processing of biometric data as they apply to other categories of data. However, these Rules should include special additional protections for especially sensitive data such as biometric data such as: (1) heightened security obligations to account for the sensitivity of the data, (2) a need to demonstrate a more compelling case for processing under a data minimization standard, and (3) in some cases special notice requirements to ensure that consumers understand that sensitive data is being processed in order to provide a good or service they have requested.

39. **To what extent, if at all, should the Commission limit companies that provide any specifically enumerated services (e.g., finance, healthcare, search, or social media) from owning or operating a business that engages in any specific commercial surveillance practices like personalized or targeted advertising? If so, how? What would the relative costs and benefits of such a rule be, given that consumers generally pay zero dollars for services that are financed through advertising?**

The Commission's rules do not need to specifically limit companies that provide enumerated services from engaging in commercial surveillance or personalized or targeted advertising. The Data Minimization Rule should apply to *all companies* under the FTC's purview and should by default prohibit most tracking and targeted advertising (*see infra* Question 43), or at the very least allow consumers to universally opt to turn off most tracking and targeted advertising (*see infra* Questions 80-82).

Digital advertising and online technologies are constantly changing. In order for a trade rule to stand the test of time and be technology and competitively neutral, the rule should be

general and apply to all sectors and services. This will also minimize unintended effects where a proposed trade rule incentivizes different business models in different sectors.

The fact that consumers often do not pay for services financed through advertising should be immaterial to the Commission's inquiry and not factor into its final rules. Even if consumers do provide monetary consideration for these services, they do provide their time and attention which platforms are able to monetize through advertising. In response to Facebook's argument that the District of Columbia's consumer protection laws do not apply to Facebook because consumers are not charged money in the *Muslim Advocates v. Zuckerberg* case, Consumer Reports explained in its *amicus* brief:

> Facebook's value to shareholders — its profitability — depends on the value of the time and attention that its users provide in accessing the social network. And indeed, the time and attention made available by Facebook users for advertisers have proven immensely valuable to Facebook's bottom line. In 2020, the average U.S. Facebook user spent fifty-eight minutes per day on the platform. Facebook has an estimated 178 million adult U.S. users. Assuming an opportunity cost equal to the federal minimum wage — a very conservative assumption — U.S. Facebook users supply $1.25 billion dollars per day of their time and attention in exchange for access to Facebook's products. In the final quarter of 2020, Facebook earned an average of $53.56 per user in the U.S. and Canada.
>
> In short, users' time and attention are valuable. Only by parting with them can consumers access and use Facebook's products. Facebook users' provision of time and attention are thus a portion of the price Facebook receives when [it] sells access to its social network.[64] [citations omitted]

40. How accurate are the metrics on which internet companies rely to justify the rates that they charge to third-party advertisers? To what extent, if at all, should new rules limit targeted advertising and other commercial surveillance practices

[64] *See* Memorandum of Consumer Reports, Public Knowledge, and Upturn as *amici curiae*, *Muslim Advocates v. Zuckerberg*, Superior Court of the District of Columbia, 2021 CA 001114B, at 7-8, https://oag.dc.gov/sites/default/files/2021-12/2021-12.06-Proposed-Brief-.pdf.

beyond the limitations already imposed by civil rights laws? If so, how? To what extent would such rules harm consumers, burden companies, stifle innovation or competition, or chill the distribution of lawful content?

For recommendations on rules to limit targeted advertising and other commercial surveillance practices, see *infra* Questions 43, 80-82.

41. To what alternative advertising practices, if any, would companies turn in the event new rules somehow limit first- or third-party targeting?

Presumably companies would return to the traditional advertising practices that have existed for decades. Online, that could include general brand advertising, contextual advertising, and potentially advertising targeted to rough location such as metropolitan area. Depending on the breadth of the rules, a first-party publisher may be able to target advertising in that first-party context based on its own stores of data about a consumer.[65]

It should also be noted that until very recently, behaviorally targeted advertising constituted a very small percentage of online ads. While tracking and cookies had been around since the advent of the internet, most ads in fact were not personally targeted to consumers based on cross-site data. For decades, non-behaviorally-targeted ads successfully monetized free content on the internet for consumers.[66] As Jason Kint, CEO of Digital Content Next (a trade association of online publishers) testified to the FTC at its 2016 workshop on Cross-Device Tracking:

---

[65] The Consumer Reports Model State Privacy Act prohibits cross-context third-party ad targeting, but allows limited first-party targeting subject only to an opt-out. While we believe this narrower approach is justified, we would alternatively support a more comprehensive prohibition on targeting. See Attachment 2, Consumer Reports, *Model State Privacy Act*, (Feb. 2021), § 2-128, https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf.

[66] Statement of Justin Brookman Director, Privacy and Technology Policy, Consumers Union, Before the House Subcommittee on Digital Commerce and Consumer Protection, Understanding the Digital Advertising Ecosystem (June 14, 2018), https://advocacy.consumerreports.org/wpcontent/uploads/2019/07/Brookman-Testimony-June-14-2018.pdf.

> So there's a fundamental problem there, and I always look back at just the economics discussion. The earlier panel made this point, I've heard it before, that online behavioral advertising pays for all this free content on the web. When I look across our 70 premium publishers that most of you use in the room, I'm sure. And those are up starts [sic]. And media companies have been around for 100 plus years. Online behavioral advertising is a very low single digit percentage of their advertising. Let's pop that bubble right now. We've popped it before. I'm popping it.
>
> We act like this online behavioral advertising pays for all the free content on the web. It doesn't. It's a low single digit percentage of our advertising. And I'm looking now at ad blocking as this emerging issue where consumers are opting out entirely from advertising. And it's very, very concerning.[67]

42. How cost-effective is contextual advertising as compared to targeted advertising?

It is not clear that incrementally much more content is available because of behavioral ads, and if so what the quality and marginal value to consumers of such content is.[68] Industry has financed some studies, though much of that data is dated, and these studies often suffer from significant methodological flaws.[69]

---

[67] Transcript, *Cross-Device Tracking Workshop*, Federal Trade Commission, (Nov. 16, 2016), Transcript Segment 2 at 6-7, https://www.ftc.gov/system/files/documents/videos/cross-device-tracking-part-2/ftc_cross-device_tracking_workshop_-_transcript_segment_2.pdf.

[68] Eric Zeng *et al.*, *Bad News: Clickbait and Deceptive Ads on News and Misinformation Websites*, ConPro Workshop on Technology and Consumer Protection (2020), https://homes.cs.washington.edu/~yoshi/papers/ConPro_Ads.pdf.

[69] For example, one widely-cited 2010 paper from former FTC economist Howard Beales argues that targeted ads can generated 2.68% more revenue than other advertising. However, this paper only compared behaviorally targeted ads to "run-of-network" ads — not contextually targeted or other ads targeted in more privacy preserving ways. The paper also does not explore what percentage of higher ad rates would go to publishers and what percentage would be collected by ad intermediaries such as Google and Facebook. Howard Beales, *The Value of Behavioral Targeting*, (2010), https://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00117/544506-00117.pdf.

Another frequently cited paper from Avi Goldfarb and Catherine Tucker employed a highly questionable methodology: it compared two sets of audience data provided by an unnamed ad tech company — one subject to Europe's ePrivacy Directive and one not. However, the researchers were not provided with information about how companies had changed business practices in response to the ePrivacy Directive,

One recent report from Carnegie Mellon — presented at the FTC's PrivacyCon — found that individually targeted ads only increased publishers' advertising revenue by 4%, with an incremental increase of revenue of approximately $0.00008 per ad.[70] Even assuming some degree of value, it is unlikely to be enough to offset the harms and loss of utility that consumers experience as a result of profligate data disclosure and secondary processing.

43. **To what extent, if at all, should new trade regulation rules impose limitations on companies' collection, use, and retention of consumer data? Should they, for example, institute data minimization requirements or purpose limitations, i.e., limit companies from collecting, retaining, using, or transferring consumer data beyond a certain predefined point? Or, similarly, should they require companies to collect, retain, use, or transfer consumer data only to the extent necessary to deliver the specific service that a given individual consumer explicitly seeks or those that are compatible with that specific service? If so, how? How should it determine or define which uses are compatible? How, moreover, could the Commission discern which data are relevant to achieving certain purposes and no more?**

We recommend that the Commission establish a Data Minimization Rule that would — with limited and specifically enumerated exceptions — limit companies' collection, use, sharing, and retention of data to what is functionally necessary to fulfill a consumer's request. We propose this model to avoid subjecting consumers to constant consent dialogs or forcing them to navigate laborious and confusing opt-out processes (*see infra* Question 73-74, 80-82). The Consumer Reports Model State Privacy Act includes first-party marketing as a permitted use subject to an opt-out; however, we would also support a stronger model that also prohibits first-party marketing by default. Our model bill provides:

---

including restricting use of cookies or targeting. The comparative effectiveness of advertising between the two audiences was then measured only through later surveying users about stated purchase intent based on being subject to different advertising campaigns in EU and non-EU jurisdictions. Avi Goldfarb and Catherine Tucker, *Privacy Regulation and Online Advertising*, (2010), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259.

[70] Veronica Marotta, Vibhanshu Abhishek, & Alessandro Acquisti, Online Tracking and Publishers' Revenues: An Empirical Analysis, Workshop on the Economics of Information Security (2019), https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf.

Data minimization and opt out of first party advertising.

> (a) A business that collects a consumer's personal information shall limit its collection and sharing of that information with third parties to what is reasonably necessary to provide a service or conduct an activity that a consumer has requested or is reasonably necessary for security or fraud prevention. Monetization of personal information shall not be considered reasonably necessary to provide a service or conduct an activity that a consumer has requested or reasonably necessary for security or fraud prevention.
>
> (b) A business that collects a consumer's personal information shall limit its use and retention of that information to what is reasonably necessary to provide a service or conduct an activity that a consumer has requested or a related operational purpose, provided that data collected or retained solely for security or fraud prevention may not be used for operational purposes.
>
> (c) A consumer shall have the right, at any time, to direct a business that uses personal information about the consumer to personalize advertising not to use the consumer's personal information to personalize advertising, and the business shall have the duty to comply with the request, promptly and free of charge, pursuant to regulations developed by the Attorney General. A business that uses a consumer's personal information to personalize advertising shall provide notice that consumers have the "right to opt out" of the use of their personal information to personalize advertising.[71]

The model bill then defines the following permitted operational purposes:

---

[71] See Attachment 2, Consumer Reports, Model State Privacy Act, (Feb. 2021), § 2-103, https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf.

> "Operational purpose" means the use of personal information when reasonably necessary and proportionate to achieve one of the following purposes, if such usage is limited to the first-party relationship and customer experience:
>
> > (1) Debugging to identify and repair errors that impair existing intended functionality.
> >
> > (2) Undertaking internal research for technological development, analytics, and product improvement, based on information collected by the business.
> >
> > (3) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, or to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.
> >
> > (4) Customization of content based on information collected by the business.
> >
> > (5) Customization of advertising or marketing based on information collected by the business.[72]

Alternatively, if the Commission rejects this approach as too ambitious, we recommend a regime offering consumers the ability to opt out of most secondary use and sharing through global opt-out mechanisms such as platform-level controls (*see infra* Questions 80-82).

Non-Retaliaton

[72] *Id.*, § 3(n).

We also recommend that the FTC's Data Minimization Rule include the principle of non-retaliation: the Rule should prohibit businesses from providing differential treatment to consumers who opt out of or do not consent to targeted offers, or the sale of information about customer habits to third-party data brokers. Consumers will be less likely to exercise their privacy rights if businesses charge them for doing so.

Instead, privacy should be recognized as an inalienable and fundamental right, not merely an asset to be bartered away. Charging consumers for privacy could have a disparate impact on the economically disadvantaged and members of protected classes who may not be able to afford the luxury of paying for fundamental privacy rights. (These rules should not, however, inhibit true loyalty programs that keep track of consumer purchases in order to incentivize repeat business, where the data collection and usage is strictly necessary for the fundamental purpose of the program, and which falls squarely within consumers' expectations for primary use.)

A prohibition on discriminatory treatment would recognize that forcing consumers to choose between unwanted sharing and use of their information on the one hand, and higher prices or inferior service on the other hand, constitutes an injury that consumers would understandably want to avoid. Privacy should be treated as an intrinsic right with positive societal externalities for free expression and experimentation, and policies that incentivize individuals to waive privacy will lead to worse outcomes.[73]

Specifically, we recommend implementing non-retaliation language consistent with language proposed in the Consumer Reports Model State Privacy Act:

No discrimination by a business against a consumer for exercise of rights.

---

[73] Stacy-Ann Elvy, Paying for Privacy and the Personal Data Economy, 117 Columbia L. Rev. 6 (Oct. 2017), https://ssrn.com/abstract=3058835;Accountable Tech, Petition for Rulemaking to Prohibit Surveillance Advertising (Sept. 28, 2021), at 25-35 https://accountabletech.org/wp-content/uploads/Rulemaking-Petition-to-Prohibit-SurveillanceAdvertising.pdf.

(a) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, or did not agree to information processing for a separate product or service, including, but not limited to, by:

(1) Denying goods or services to the consumer.

(2) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(3) Providing a different level or quality of goods or services to the consumer.

(4) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(5) This title shall not be construed to prohibit a business from offering discounted or free goods or services to a consumer if the offering is in connection with a consumer's voluntary participation in a program that rewards consumers for repeated patronage, if personal information is used only to track purchases for loyalty rewards, and the business does not share the consumer's data with third parties pursuant to that program.[74]

Finally, we recommend providing access, correction, portability, and deletion rights as laid out in the Consumer Reports State Model Privacy Act.[75]

[74] See Attachment 2, Consumer Reports, Model State Privacy Act, (Feb. 2021), § 2-125, https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf.
[75] *Id.*, §§ 2-105, 2-110, 2-115, 2-120.

44. By contrast, should new trade regulation rules restrict the period of time that companies collect or retain consumer data, irrespective of the different purposes to which it puts that data? If so, how should such rules define the relevant period?

A hard-and-fast rule that all companies must delete data after a predetermined period of time — regardless of the purposes for which that data is stored — would likely be counterproductive and contrary to consumer interests. For example, many consumers rely upon companies for indefinite cloud storage of emails, photos, and other personal data. Instead, companies should be limited to retaining the data that is necessary and proportionate to the narrow set of operational purposes defined in the Rule. Large companies could be required to provide transparency about retention periods for these purposes pursuant to a Transparency Rule (*see infra* Question 89).

45. Pursuant to a purpose limitation rule, how, if at all, should the Commission discern whether data that consumers give for one purpose has been only used for that specified purpose? To what extent, moreover, should the Commission permit use of consumer data that is compatible with, but distinct from, the purpose for which consumers explicitly give their data?

Due to the opacity of many data practices (*see infra* Question 86), the FTC may not have perfect visibility into companies' compliance. Further, given the FTC's limited staffing, it would likely not be practical to mandate periodic Commission audits even of the biggest companies. However, the threat of significant statutory penalties for noncompliance will still meaningfully deter companies if there is a risk that illegal behavior may be detected or reported. The Commission should also consider including explicit whistleblower protections in its Rules to encourage employees to report violations and prevent companies from engaging in retaliatory behavior.[76]

[76] For example, Representative Trahan's Digital Services Safety and Oversight Act includes whistleblower protections for employees who report wrongdoing to government regulators. *See* Digital Services Safety and Oversight Act, H.R. 6796, 117th Cong., https://www.congress.gov/bill/117th-congress/house-bill/6796/text.

We are skeptical that the concept of "compatible purposes" is a useful one in privacy regulation — it is indefinite and confusing, and offers companies a potentially broad loophole to launder unwanted and adversarial data practices. Just as the term "legitimate interest" in Europe's General Data Privacy Regulation has been abused to justify cross-site targeting,[77] companies may similarly abuse the idea of "compatible purposes." Instead, the FTC should define specific excepted operational purposes for which data may be processed. By their nature, purposes such as "product improvement" are still quite expansive, and if the purposes are well-crafted, companies should be able to fit legitimate and beneficial processing within those categories without the regulation including nebulous catch-all terms such as "compatible purposes."

46. Or should new rules impose data minimization or purpose limitations only for certain designated practices or services? Should, for example, the Commission impose limits on data use for essential services such as finance, healthcare, or search—that is, should it restrict companies that provide these services from using, retaining, or transferring consumer data for any other service or commercial endeavor? If so, how?

No, the Data Minimization Rule should apply universally. Secondary processing of data is a universal problem that plagues many (if not all) industries. Moreover, if the Commission were to use its Section 18 rulemaking authority to only cover industries already covered by statutory privacy regimes (regimes that were enacted after the passage of Section 5), it would be inviting legal challenge from companies arguing that the Commission was superseding its legal authority and circumventing the will of Congress.

47. To what extent would data minimization requirements or purpose limitations protect consumer data security?

Fundamentally, if companies retain less data because they may only use data for a carefully defined set of purposes, then consumers are at a lower risk of experiencing a data

[77] Natasha Lomas, *Behavioral ad industry gets hard reform deadline after IAB's TCF found to breach Europe's GDPR*, TechCrunch, (Feb. 2, 2022), https://techcrunch.com/2022/02/02/iab-tcf-gdpr-breaches/.

breach. Requiring companies to regularly query whether data is necessary and proportionate for a permissible purpose will necessarily lessen the attack surface available to bad actors to target. As a result, consumers will be safer. Companies too will have lower security compliance costs if there are fewer stores of data, and fewer systems have access to those stores.

Indeed, the principle that retaining data without a legitimate business purpose inherently constitutes an unreasonable and unfair business practice goes all the way back to the FTC's first data security action against BJ's Warehouse in 2005. In that case, the Commission alleged that BJ's "created unnecessary risks to the information by storing it for up to 30 days when it no longer had a business need to keep the information."[78] Since that time, the FTC has repeatedly told companies that retaining unnecessary data without a defined business purpose is prohibited by Section 5 of the FTC Act.[79]

48. To what extent would data minimization requirements or purpose limitations unduly hamper algorithmic decision-making or other algorithmic learning-based processes or techniques? To what extent would the benefits of a data minimization or purpose limitation rule be out of proportion to the potential harms to consumers and companies of such a rule?

As discussed above (*supra* Question 43), we would support an exception to the Data Minimization Rule for data processing that is "reasonably necessary and proportionate" to the purpose of "internal research for technological development, analytics, and product improvement, based on information collected by the business" so long as such research is "limited to the first-party relationship and customer experience."[80] However, companies should not be entitled to track consumers across multiple contexts or aggregate third-party data sets

---

[78] Complaint, *In the Matter of BJ's Wholesale Club, Inc.*, 042 3160 Docket No. C-4148 , ¶ 7, (Jun. 16, 2005), https://www.ftc.gov/legal-library/browse/cases-proceedings/042-3160-bjs-wholesale-club-inc-matter.

[79] *E.g.*, *Start with Security, A Guide for Business: Lessons Learned from FTC Cases*, Federal Trade Commission, at 2, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (identifying "Hold on to information only as long as you have a legitimate business need" as a core element of "Start with Security").

[80] *See* Attachment 2, Consumer Reports, *Model State Privacy Act*, (Feb. 2021), § 3(n), https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf.

simply in order to refine their own algorithms. Such an exception would undermine the core intent of this privacy rulemaking to ensure that consumers are entitled to reasonable privacy protections as they go about their lives.

49. **How administrable are data minimization requirements or purpose limitations given the scale of commercial surveillance practices, information asymmetries, and the institutional resources such rules would require the Commission to deploy to ensure compliance? What do other jurisdictions have to teach about their relative effectiveness?**

As noted above (*see supra* Question 45), while the FTC is understaffed and will not be able to ensure full compliance, the promulgation of a Data Minimization Rule will threaten significant first-time penalties for bad actors and will be effective in deterring most (if not all) violations. Statutory penalties tend to far outstrip the benefits of wrongdoing for the very reason that the chances of detection and enforcement are necessarily low.

However, it is useful to consider Europe's experience with the GDPR, where a combination of confusing and vague language with weak enforcement has hamstrung the law's effectiveness in meaningfully constraining unwanted data practices. The Federal Trade Commission should learn from the history of the GDPR and commit to writing clear and precise rules and backing them up with robust enforcement.

50. **What would be the effect of data minimization or purpose limitations on consumers' ability to access services or content for which they are not currently charged out of pocket? Conversely, which costs, if any, would consumers bear if the Commission does not impose any such restrictions?**

See supra Questions 41-42.

51. **To what extent, if at all, should the Commission require firms to certify that their commercial surveillance practices meet clear standards concerning collection,**

use, retention, transfer, or monetization of consumer data? If promulgated, who should set those standards: the FTC, a third-party organization, or some other entity?

As noted above, (*supra* Question 36), the Commission does not need to require certification against a separate standard. The Data Minimization (and other) Rules should set the relevant standard to which companies need to adhere.

52. **To what extent, if at all, do firms that now, by default, enable consumers to block other firms' use of cookies and other persistent identifiers impede competition? To what extent do such measures protect consumer privacy, if at all? Should new trade regulation rules forbid the practice by, for example, requiring a form of interoperability or access to consumer data? Or should they permit or incentivize companies to limit other firms' access to their consumers' data? How would such rules interact with general concerns and potential remedies discussed elsewhere in this ANPR?**

We strongly disagree with the premise that a platform taking steps to limit companies' access to third-party data should be prohibited by a privacy rule. Worse, the idea that a privacy rule should affirmatively *require* franchising personal data to third parties is absurd.

A better solution would be to enact a Data Minimization Rule that limits all companies' secondary use of personal data. While the Consumer Reports Model State Privacy Act allows some affordance for first-party use of data for marketing, we would strongly prefer a model where every company is prohibited from behavioral targeting to one where every company has an intrinsic right to your personal information in the name of competition. Moreover, even if first parties do retain some right to use data for marketing, a Rule could clarify that *platforms* such as operating systems or browsers should not be considered first parties for consumer interactions with other companies. As we urged in our white paper on FTC rulemaking:

> Platforms that facilitate communication or interactions among other companies — such as ISPs and social media companies — should generally be considered

"third parties" with regard to the interaction between a consumer and other companies.[81]

A new trade regulation which prohibits most secondary uses of data — including among services provided by the same firm — and third party disclosure should enable more competition as publishers and other single service platform companies would face a more level playing field when it comes to collecting and using data to provide services and raise revenues using digital advertising.

On the other hand, a trade regulation mandating some form of interoperability or access to consumer data may also provide third parties access to data which would allow them to compete more effectively in digital advertising markets. But privacy concerns would likely override any efficiency or competition benefits given the exposure and sharing of user data with third parties. This is also likely to be against users' interests in terms of both privacy and in terms of their ability to control their own data. Such an intervention would also enable the continued use of data for personally targeted advertising and there would be fewer incentives for companies and the market to evolve and move privacy enhancing business models.

IV. Automated Systems (see other doc for these two)

53. How prevalent is algorithmic error? To what extent is algorithmic error inevitable? If it is inevitable, what are the benefits and costs of allowing companies to employ automated decision-making systems in critical areas, such as housing, credit, and employment? To what extent can companies mitigate algorithmic error in the absence of new trade regulation rules?

54. What are the best ways to measure algorithmic error? Is it more pronounced or happening with more frequency in some sectors than others?

55. Does the weight that companies give to the outputs of automated decision-making systems overstate their reliability? If so, does that have the potential to lead to greater consumer harm when there are algorithmic errors?

---

[81] *See* Attachment 1, Consumer Reports and the Electronic Privacy Information Center, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking*, (Jan. 26, 2022), at 18, https://advocacy.consumerreports.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf.

Some AI companies claim that their technology is capable of doing certain things that are not substantiated by science or claim certain accuracy rates of their technology without third-party validation. Some of these pseudoscientific algorithms can cause real harm. In the employment space, companies like HireVue have been criticized for building video interviewing software that claims to rank job applicants based on the tone of their voice and facial expressions. There is little evidence that these factors are related to job performance; more importantly, these kinds of algorithms have the potential to discriminate against those with certain skin colors, accents, or disabilities. Using AI to predict subjective processes like job success and recidivism may result in discriminatory outcomes; trying to quantify subjective processes where the goals might be different depending on who designs the AI system tends to hurt marginalized populations. The FTC has a long history of requiring meaningful substantiation before making marketing claims;[82] it should consider formalizing this principle into a rule if it decides to specifically regulate AI systems as part of this proceeding.

Furthermore, companies today are not generally required to undergo audits or external review. It is difficult to know whether a company claiming a certain accuracy rate for their technology is accurate or not, particularly since there are no regulations around standardized testing. Companies may claim high accuracy rates based on testing their algorithms on a certain dataset, while a potential external reviewer could obtain a different accuracy rate testing the same algorithm on a different dataset. In promulgating its rules, the Commission should establish guidelines around testing standardization, transparency around the reporting of accuracy rates (including reporting demographics that the company has tested their algorithms on), and in some cases require third party auditing.

56. To what extent, if at all, should new rules require companies to take specific steps to prevent algorithmic errors? If so, which steps? To what extent, if at all, should the Commission require firms to evaluate and certify that their reliance on automated decision-making meets clear standards concerning accuracy, validity,

[82] *E.g.*, *POM Wonderful, LLC v. Federal Trade Commission*, POM Wonderful, LLC v. Federal Trade Commission, 777 F.3d 478 (D.C. Cir. 2015), https://casetext.com/case/pom-wonderful.

reliability, or error? If so, how? Who should set those standards, the FTC or a third-party entity? Or should new rules require businesses to evaluate and certify that the accuracy, validity, or reliability of their commercial surveillance practices are in accordance with their own published business policies?

We recommend that companies whose algorithms have significant legal effects should be required by the Commission to undergo mandatory third-party audits to asses their systems for bias, discrimination, and other potential harms. And while auditing can be used to identify harms and improve transparency, we also need regulation for independent groups to be able to audit algorithms in a meaningful way. Today, there are far too many technical and legal barriers to meaningful independent testing and research into algorithmic systems.[83]

Even with an audit mandate, private auditing companies may not be incentivized to provide the most accurate, honest, and transparent audits. If a company conducts an audit, they may not necessarily be required to fully address any issues brought up by the auditing process. Regulation that mandates third-party audits for particular AI applications and provides a process for private auditing companies to get accredited in order to carry out these audits could help address these problems. The accreditation process would need a standardized testing procedure for algorithms depending on the application, and would also need to require companies to provide certain data and information to the auditors. Such regulations should include algorithms in the employment, housing, credit, and criminal justice sectors. While there are other federal agencies that regulate these areas, the Commission should work with them to establish guidelines on what auditing should look like in these sectors.

The audits performed by companies or the auditing firms they hire on their own algorithms may not be meaningful unless there are standardized requirements. Some argue that open-ended questions that invite "bottom-up" questions are more beneficial, rather than a checklist that a standard audit could provide. These can be included in requirements for deliverables like algorithmic impact assessments or model cards (documents that provide evaluations of how the algorithm works under various conditions and in what circumstances the

---

[83] *See* Attachment 4, Nandita Sampath, *Opening Black Boxes: Addressing Legal Barriers to Public Interest Algorithmic Auditing*, Consumer Reports Digital Lab, (Oct. 2022), https://digital-lab-wp.consumerreports.org/wp-content/uploads/2022/10/CR_Algorithmic_Auditing_Final_10_2022VF2.pdf.

model is intended to be used). Ultimately, though, standardized requirements for audits must be broad enough to encompass a wide variety of algorithms but nuanced enough that the disparate impacts and other harms are made clear through the evaluation process.

We recommend that the Commission require that algorithms that may have significant legal effects must undergo third party audits before deployment, and regularly after deployment; we also recommend that these auditors are required to undergo an accreditation process to evaluate algorithms that can have significant legal effects. In order for these audits to be effective, companies should be required to disclose specific data to the auditors, such as training data used to develop the model, a standardized API to easily test the system, or even the code itself, depending on the case. We also recommend that specific issues be investigated by auditors such as discrimination against protected classes, etc. Finally, the results of the audit should be made public if the algorithm has already been deployed to the public. If not, the company must address the results of the audit in a timely manner, and before deployment.

57. To what extent, if at all, do consumers benefit from automated decision-making systems? Who is most likely to benefit? Who is most likely to be harmed or disadvantaged? To what extent do such practices violate Section 5 of the FTC Act?

Automated decision-making systems can generally benefit some consumers in terms of efficiency. For example, using Apple's TouchID or FaceID to get into your phone is faster than typing in a password. AI can also allow for automation of certain tasks, which can either benefit a consumer directly (if they would otherwise have to do the tasks themselves) or indirectly (if a company can offer lower prices due to improved efficiency). However, when algorithms are used to determine people's access to life opportunities, they can cause serious harm.

While there are many sources of bias in algorithms, a major reason why algorithms can perpetuate discrimination against minorities is due to biases that often stem from societal inequities. For example, some police departments have begun to use predictive policing algorithms, which aim to predict where and when a crime is going to occur (or even who is likely to have committed a crime), with the goal of better allocating policing resources to these predicted areas. These algorithms use historical data from crime reports on where and when

crimes take place to make predictions about future occurrences of crime.[84] However, this historical data tends to be skewed, since Black communities tend to be overpoliced, so alleged crimes are reported more often than they are in whiter areas.[85] If algorithms use data from sources like past arrests or crime reports, it is likely that these algorithms will point police officers to locations that are already being heavily policed, which reinforces the already biased decisions about where officers should patrol.

While the previous example discussed overrepresentation in datasets, underrepresentation of Blacks and minorities in training data can be equally harmful. Facial recognition algorithms are becoming more common in everyday life, being used in anything from security systems to identifying potential suspects in alleged crimes by law enforcement. Studies have shown that many facial recognition algorithms perform worse for those with darker skin. A well-known study by Joy Buolamwini and Timnit Gebru tested facial recognition algorithms from three different companies and found that they all consistently performed best when identifying lighter-skinned males and worst on darker-skinned females, by significant percentages.[86] Darker-skinned men also had higher error rates compared to lighter-skinned males. As these technologies become more embedded into our society, we should consider the consequences of discrepancies in error rates of people with different skin colors. Some of these algorithms are already being used in law enforcement to identify people suspected of crime, and false positives have tended to arise more often for Black individuals.[87]

Even if companies are able to mitigate bias efficiently in their algorithms, many automated decision-making systems that use complex algorithms like neural networks lack sufficient transparency; even engineers who design these systems cannot explain how they arrive at their final decisions. An FTC Nondiscrimination Rule should provide that companies may not illegitimately discriminate against individuals or groups of people from a particular demographic — even if the company does not intend or cannot explain the result.

---

[84] Eva Ruth Moravec, Do Algorithms have a Place in Policing? The Atlantic, (Sep. 5, 2019), https://www.theatlantic.com/politics/archive/2019/09/do-algorithms-have-place-policing/596851/.
[85] Renata M. O'Donnell, Challenging Racist Predictive Policing Algorithms Under the Equal Protection Clause, New York University Law Review, Vol 94:544, (Jun. 2019), https://www.nyulawreview.org/wp-content/uploads/2019/06/NYULawReview-94-3-ODonnell.pdf.
[86] Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research 81:1–15, 2018 Conference on Fairness, Accountability, and Transparency, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.
[87] Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where it Falls Short,* New York Times, (Jan. 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.

58. **Could new rules help ensure that firms' automated decision-making practices better protect non-English speaking communities from fraud and abusive data practices? If so, how?**
59. **If new rules restrict certain automated decision-making practices, which alternatives, if any, would take their place? Would these alternative techniques be less prone to error than the automated decision-making they replace?**

Restriction of the use of automated decision-making does not necessarily restrict the use of other computational tools to make decisions about people. For example, consider an HR department within a company using an automated resume reader to parse resumes for an open job position. Using a simple computing tool that can identify the number of years an individual has worked based on their college graduation date obtained from their resume is much different from using a neural network to holistically look at a resume and determine whether someone is qualified for a job. Not only does this use more objective criteria to make decisions about people's access to life opportunities, but the decision is also very explainable to the job applicant. An important note about many kinds of complex algorithms is that they are often very opaque, even to the engineers that design them.

Furthermore, using more objective criteria to make decisions about people can also provide individuals with helpful feedback when they are rejected from an opportunity. The Equal Credit Opportunity Act has mandated explainability in credit decisioning for decades.[88] In May 2022, the Consumer Financial Protection Bureau released a blog post that stated companies using algorithms to decide an individual's access to credit still had to provide a meaningful explanation as to why an applicant was rejected, and that using complex algorithms was not reason enough to avoid this requirement.[89] When these algorithms are used to make important

[88] 15 U.S. Code § 1691. *See also* Elisa Jillson, *Aiming for truth, fairness, and equity in your company's use of AI*, Federal Trade Commission, (Apr. 19, 2021), https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai; , Andrew Smith, *Using Artificial Intelligence and Algorithms*, Federal Trade Commission, (Apr. 8, 2020), https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms.

[89] Press Release, *CFPB Acts to Protect the Public from Black-box Credit Models Using Complex Algorithms, Consumer Financial Protection Bureau*, (May 26, 2022), https://www.consumerfinance.gov/about-us/newsroom/cfpb-acts-to-protect-the-public-from-black-box-credit-models-using-complex-algorithms/.

decisions regarding people's life opportunities, people deserve a meaningful explanation as to how the automated decision system comes to a result.

60. **To what extent, if at all, should new rules forbid or limit the development, design, and use of automated decision-making systems that generate or otherwise facilitate outcomes that violate Section 5 of the FTC Act? Should such rules apply economy-wide or only in some sectors? If the latter, which ones? Should these rules be structured differently depending on the sector? If so, how?**

We believe that the FTC should promulgate rules of general applicability for all sectors of the economy that it regulates. That would include Nondiscrimination protections as described below (*see infra* Question 66) as well as special rules for automated processes such as substantiation, explainability, and processes to root out discrimination during all phases of design, including in some cases third-party audits.

61. **What would be the effect of restrictions on automated decision-making in product access, product features, product quality, or pricing? To what alternative forms of pricing would companies turn, if any?**
62. **Which, if any, legal theories would support limits on the use of automated systems in targeted advertising given potential constitutional or other legal challenges?**
63. **To what extent, if at all, does the First Amendment bar or not bar the Commission from promulgating or enforcing rules concerning the ways in which companies personalize services or deliver targeted advertisements?**
64. **To what extent, if at all, does Section 230 of the Communications Act, 47 U.S.C. 230, bar the Commission from promulgating or enforcing rules concerning the ways in which companies use automated decision-making systems to, among other things, personalize services or deliver targeted advertisements?**

V. Discrimination

65. How prevalent is algorithmic discrimination based on protected categories such as race, sex, and age? Is such discrimination more pronounced in some sectors than others? If so, which ones?

A Nondiscrimination Rule should be universal in application across all industries and sectors regulated by the FTC. The Consumer Reports Model State Privacy Act contains two sections prohibiting discrimination in economic opportunities and discrimination in public accommodations under a traditional disparate impact rubric:

Discrimination in economic opportunities.

(a) It is unlawful to process information for the purpose of advertising, marketing, soliciting, offering, selling, leasing, licensing, renting, or otherwise commercially contracting for housing, employment, credit, or insurance, in a manner that discriminates against or otherwise makes the opportunity unavailable on the basis of a person or class of persons' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability.

(b) The unlawful processing of personal information based on disparate impact is established under this subsection only if:

(1) A complaining party demonstrates that the processing of personal information causes a disparate impact on the basis of a protected characteristic; and

(2) The respondent fails to demonstrate that the challenged processing of information is necessary to achieve one or more substantial, legitimate, nondiscriminatory interests; or

(3) The complaining party shows that an alternative policy or practice could serve such interests with a less discriminatory effect.

(c) With respect to demonstrating that a particular processing of personal information causes a disparate impact as described in paragraph (a), the complaining party shall demonstrate that any particular challenged component of the processing of personal information causes a disparate impact, except that if the components of the respondent's processing of personal information are not

reasonably capable of separation for analysis, the processing of personal information may be analyzed as a whole. Machine learning algorithms are presumed to be not capable of separation for analysis unless respondent proves otherwise by a preponderance of the evidence.

Discrimination in public accommodations.

(a) It is unlawful to process personal information in a manner that segregates, discriminates in, or otherwise makes unavailable the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation on the basis of a person or class of persons' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, or disability.

(b) The standards for disparate impact cases stated in Section 126(b)-(c) shall apply to disparate impact cases with respect to this paragraph.

(c) It is unlawful for any person to:

(1) Withhold, deny, deprive, or attempt to withhold, deny, or deprive, any person of any right or privilege secured by this paragraph;

(2) Intimidate, threaten, coerce, or attempt to intimidate, threaten, or coerce, any person with the purpose of interfering with any right or privilege secured by this paragraph; or

(3) Punish or attempt to punish any person for exercising or attempting to exercise any right or privilege secured by this paragraph.[90]

66. How should the Commission evaluate or measure algorithmic discrimination? How does algorithmic discrimination affect consumers, directly and indirectly? To what extent, if at all, does algorithmic discrimination stifle innovation or competition?

67. How should the Commission address such algorithmic discrimination? Should it consider new trade regulation rules that bar or somehow limit the deployment of

[90] See Attachment 2, Consumer Reports, Model State Privacy Act, (Feb. 2021), §§ 3-126, 3-127, https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf.

any system that produces discrimination, irrespective of the data or processes on which those outcomes are based? If so, which standards should the Commission use to measure or evaluate disparate outcomes? How should the Commission analyze discrimination based on proxies for protected categories? How should the Commission analyze discrimination when more than one protected category is implicated (e.g., pregnant veteran or Black woman)?

The FTC can address algorithmic discrimination through the enactment of the Nondiscrimination protections as described above (*see supra* Question 66) as well as special rules for automated processes such as substantiation, explainability, and processes to root out discrimination during all phases of design, including in some cases third-party audits.

68. **Should the Commission focus on harms based on protected classes? Should the Commission consider harms to other underserved groups that current law does not recognize as protected from discrimination (e.g., unhoused people or residents of rural communities)?**

See our response to Question 66.

69. **Should the Commission consider new rules on algorithmic discrimination in areas where Congress has already explicitly legislated, such as housing, employment, labor, and consumer finance? Or should the Commission consider such rules addressing all sectors?**

The FTC should promulgate rules of generally applicability that apply to all commercial sectors it regulates.

70. **How, if at all, would restrictions on discrimination by automated decision-making systems based on protected categories affect all consumers?**

71. **To what extent, if at all, may the Commission rely on its unfairness authority under Section 5 to promulgate antidiscrimination rules? Should it? How, if at all, should antidiscrimination doctrine in other sectors or federal statutes relate to new rules?**
72. **How can the Commission's expertise and authorities complement those of other civil rights agencies? How might a new rule ensure space for interagency collaboration?**

While other agencies regulate algorithms in the housing, employment, credit/lending sectors, and others, the Commission can still play an important role in providing guidelines on testing requirements, auditing standards, and more, regardless of sector. As mentioned above, requiring third party auditing for significant life decisions should be a primary goal for the Commission, and the Commission should work with these other agencies to dictate what mandatory auditing looks like in practice.

VI. Consumer Consent

73. **The Commission invites comment on the effectiveness and administrability of consumer consent to companies' commercial surveillance and data security practices. Given the reported scale, opacity, and pervasiveness of existing commercial surveillance today, to what extent is consumer consent an effective way of evaluating whether a practice is unfair or deceptive? How should the Commission evaluate its effectiveness?**

As we expect most commentators will tell you, the current "notice and choice" regime, in which consumers are expected to read extensive privacy policies and make "all or nothing" decisions about whether to use an online service or app, makes it impossible for consumers to meaningfully participate in the market while protecting their privacy. Even if consumers had the time to read every privacy policy and statement, they would in most cases come away with woefully incomplete information. Such policies tend to be vague and expansive, designed to protect a company from liability rather than inform privacy-conscious consumers. In

many cases, the companies themselves have not decided to whom data will be sold and the purposes for which it will be used. It is impossible for consumers to assess the cost of a loss of control over their personal information, or to determine a value and "trade" their data for goods or services.

Many privacy advocates had traditionally argued for requiring more explicit consent for secondary uses. However, experiences with manipulative European cookie consent interfaces and other consent dialogs designed to nudge (or confuse) consumers into granting permission for expansive permission has led to some rethinking. While long boilerplate contracts and license agreements may purport to obtain consent for all sorts of unwanted data processing, it is difficult to argue that consumers have made a conscious and deliberate choice to allow it. Even when regulation mandates that consent be obtained in response to a dedicated and separate prompt, companies today have the ability to utilize artificial intelligence and iterative A/B testing to land on the phrasing and design that maximizes the desired results. Underfunded and understaffed regulators do have the capacity to monitor let alone evaluate millions of ever evolving consent interfaces.

Policymakers do not want to subvert consumer free will. If a consumer in fact does want to share data with a company, that should be their choice. However, it should be the primary purpose of an interaction: if Google offers a product whereby Google offers to track users around the web in exchange for showing tailored ads, consumers can freely choose to participate in such a program. However, Google should not purport to obtain consent for tracking as part of a consumer's use of an unrelated product, such as Gmail. This framework is designed to enable processing and sharing of personal data that reflects the volition of the consumer, instead of permissions obtained under the fiction of informed consent.

74. In which circumstances, if any, is consumer consent likely to be effective? Which factors, if any, determine whether consumer consent is effective?

Rather than focusing on a consumer's *consent* to practices the value of which may only accrue to a company, the FTC should think in terms of consumer *volition*. The FTC should allow data practices that are consistent with the will and intention of the user. If a consumer clearly wants to allow a company to track them around the internet for the purpose of serving targeted ads, they are entitled to do that. However, the FTC should not create a regime where consumers are beleaguered for requests for consent for unrelated data practices when their *volition* is simply to browse a site or purchase a product. The FTC should focus on disambiguating operational data processing for a service the consumer wants from unrelated data processing that a company wants to engage in.

75. **To what extent does current law prohibit commercial surveillance practices, irrespective of whether consumers consent to them?**
76. **To what extent should new trade regulation rules prohibit certain specific commercial surveillance practices, irrespective of whether consumers consent to them?**

See the responses above to Questions 73-74. The intention of a Data Minimization Rule is not to prohibit consumers from engaging in behavior they want to engage in. It is intended to limit data processing to what is necessary to deliver the products and services they request. However, the Rule should recognize the practical reality that many online consent mechanisms today do not reflect the volition of the individual.

77. **To what extent should new trade regulation rules require firms to give consumers the choice of whether to be subject to commercial surveillance? To what extent should new trade regulation rules give consumers the choice of withdrawing their**

duly given prior consent? How demonstrable or substantial must consumer consent be if it is to remain a useful way of evaluating whether a commercial surveillance practice is unfair or deceptive? How should the Commission evaluate whether consumer consent is meaningful enough?

See responses to Questions 73-74 and 82.

78. **What would be the effects on consumers of a rule that required firms to give consumers the choice of being subject to commercial surveillance or withdrawing that consent? When or how often should any given company offer consumers the choice? And for which practices should companies provide these options, if not all?**

See responses to Questions 73-74 and 82.

79. **Should the Commission require different consent standards for different consumer groups (e.g., parents of teenagers (as opposed to parents of pre-teens), elderly individuals, individuals in crisis or otherwise especially vulnerable to deception)?**

As discussed previously, consent is not the best frame to consider consumer free will and privacy choices. However, to the extent that a company is marketing a product to a target audience, it should frame its description of the product in language appropriate to the nature of that audience.

80. Have opt-out choices proved effective in protecting against commercial surveillance? If so, how and in what contexts?

Opt-out rights can be extremely difficult to use in practice — especially if consumers are forced to manually opt out separately for every website, app, and offline business they interact with.

In May and June 2020, Consumer Reports' Digital Lab conducted a mixed methods study to examine whether the new California Consumer Privacy Act (CCPA) is working for consumers. This study focused on the Do-Not-Sell provision in the CCPA, which gives consumers the right to opt out of the sale of their personal information to third parties through a "clear and conspicuous link" on the company's homepage. As part of the study, 543 California residents were asked to make just one Do-Not-Sell request to 234 data brokers listed in the California Attorney General's data broker registry. Participants reported their experiences via survey. The study resulted in the following findings:[91]

- Consumers struggled to locate the required links to opt out of the sale of their information. For 42.5% of sites tested, at least one of three testers was unable to find a DNS link. All three testers failed to find a "Do Not Sell" link on 12.6% of sites, and in several other cases one or two of three testers were unable to locate a link.
    - Consumers struggled to locate the required links to opt out of the sale of their information. For 42.5% of sites tested, at least one of three testers was unable to find a DNS link. All three testers failed to find a "Do Not Sell" link on 12.6% of sites, and in several other cases one or two of three testers were unable to locate a link.

[91] *See* Attachment 3, Maureen Mahoney, *California Consumer Privacy Act: Are Consumers' Digital Rights Protected?*, Consumer Reports, (Oct.1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2021/05/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf2.pdf.

    - All three testers were unable to find the DNS links for five additional companies, though follow-up research revealed that the companies did have DNS links on their homepages. This also raises concerns about compliance, since companies are required to post the link in a “clear and conspicuous” manner.
- Many data brokers’ opt-out processes are so onerous that they have substantially impaired consumers’ ability to opt out, highlighting serious flaws in the CCPA’s opt-out model.
    - Some DNS processes involved multiple, complicated steps to opt out, including downloading third-party software.
    - Some data brokers asked consumers to submit information or documents that they were reluctant to provide, such as a government ID number, a photo of their government ID, or a selfie.
    - Some data brokers confused consumers by requiring them to accept cookies just to access the site.
    - Consumers were often forced to wade through confusing and intimidating disclosures to opt out.
    - Some consumers spent an hour or more on a request.
    - At least 14% of the time, burdensome or broken DNS processes prevented consumers from exercising their rights under the CCPA.
- At least one data broker used information provided for a DNS request to add the user to a marketing list, in violation of the CCPA.
- At least one data broker required the user to set up an account to opt out, in violation of the CCPA.
- Consumers often didn’t know if their opt-out request was successful. Neither the CCPA nor the CCPA regulations require companies to notify consumers when their request has

been honored. About 46% of the time, consumers were left waiting or unsure about the status of their DNS request.

- About 52% of the time, the tester was “somewhat dissatisfied” or “very dissatisfied” with the opt-out processes.
- On the other hand, some consumers reported that it was quick and easy to opt out, showing that companies can make it easier for consumers to exercise their rights under the CCPA. About 47% of the time, the tester was “somewhat satisfied” or “very satisfied” with the opt-out process.

For opt-out rights to be functionally usable by consumers, they must be scalable. An opt-out regime can only work if consumers can opt out universally from secondary processing across entire platforms with simple tools (*see supra* Question 81).

81. Should new trade regulation rules require companies to give consumers the choice of opting out of all or certain limited commercial surveillance practices? If so, for which practices or purposes should the provision of an opt-out choice be required? For example, to what extent should new rules require that consumers have the choice of opting out of all personalized or targeted advertising?

While Consumer Reports would prefer a Data Minimization Rule that prohibits most secondary use and sharing by default, we could alternatively support a model that allows consumers to universally opt out of most secondary data processing and sharing through global opt-out mechanisms.

Under this model, any secondary processing would be allowable by default, however consumers would be legally entitled to turn off either specific categories of secondary process, or all secondary processing (with some exceptions). This is the model so far adopted in states such as California, Virginia (VCDPA), and Colorado (CPA), as well as federal legislation

proposed by Senator Ron Wyden.[92] The bulk of other state legislative proposals introduced in recent years follows this model as well. Such an approach should be considered the bare minimum that could be done to address secondary data processing — otherwise, consumers would not be able to practically take action to constrain unwanted secondary processing.

For opt-out rights to be functionally usable by consumers, they must be scalable. An op-tout regime can only work if consumers can opt out universally from secondary processing across entire platforms with simple tools. In the absence of a default prohibition on most secondary data use, the FTC should (1) mandate that companies need to comply with platform-level opt-outs such as Global Privacy Control (GPC),[93] IoS Limit Ad Tracking, and Do Not Track (DNT). For other types of data processing, the FTC could also (2) set up a registry of identifiers — such as email addresses, phone number, etc. — for users to globally opt out of the disclosure or secondary processing of those identifiers and any linked information.

Opting out one-by-one is particularly impractical because under the CCPA, which has an opt-out model, many companies have developed complicated and onerous opt-out processes. Some companies ask consumers to go through several different steps to opt out. In some cases, the opt outs are so complicated that they have actually prevented consumers from stopping the sale of their information.[94] This is expected to improve, as the California Attorney General has since prohibited the use of dark patterns in opt-out processes, and is stepping up their enforcement efforts. Nevertheless, in the absence of a ban of most secondary use, it is important for consumers to have (at least) a one-step option for stopping the secondary use of their information.

---

[92] Cal. Civ. Code § 1798.100 et seq, https://thecpra.org/; Colorado S. 21-190 (2021), https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_rer.pdf; Virginia S. 1392 (2021), https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+SB1392; S. 1444 § 6 (2021), https://www.congress.gov/bill/117th-congress/senate-bill/1444.

[93] Global Privacy Control, https://globalprivacycontrol.org/.

[94] See Attachment 3, Maureen Mahoney, California Consumer Privacy Act: Are Consumers' Digital Rights Protected?, Consumer Reports, (Oct.1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2021/05/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf2.pdf.

82. How, if at all, should the Commission require companies to recognize or abide by each consumer's respective choice about opting out of commercial surveillance practices—whether it be for all commercial surveillance practices or just some? How would any such rule affect consumers, given that they do not all have the same preference for the amount or kinds of personal information that they share?

If the Commission decides to implement an opt-out based system instead of a more robust prohibition on tracking practices, we recommend that companies be required to adhere to a set of global opt-out signals by ceasing the processing of cross-service data except for certain narrow excepted purposes. We also recommend that the FTC create and maintain a registry of signals that companies must honor as legally binding opt-out requests.[95]

Re-opt-in

Despite the use of a global privacy signal, some consumers may still want the ability to grant permission to individual sites and services to sell their data or to engage in cross-site tracking. However, this seems unlikely to be the norm. Unlike rights such as access and deletion where consumers' choices are likely to be heterogeneous, a consumer who generally does not want their data tracked across services likely wants no one to do so — this is the reason for the creation of global opt-out mechanisms.

In practice, a provision allowing for consumer re-opt-in may primarily empower companies to pester users into granting permission to ignore the global signal. Many (if not most) companies confronting the ePrivacy Directive and Global Data Privacy Regulation in Europe adopted just this approach to a consent requirement for tracking: rather than limit their data processing to what was functionally necessary in response to the law, they instead

[95] *See* Comments of Consumer Reports In Response to the California Privacy Protection Agency on the Text of Proposed Rules under the California Privacy Rights Act of 2020, (Aug. 23, 2022), at 3-5, https://advocacy.consumerreports.org/wp-content/uploads/2022/08/CPPA-regs-comments-summer-2022-1.pdf

bombarded consumers with overwhelming, confusing, or downright abusive interfaces to simulate consent to maintain the status quo of data sharing and ad targeting.[96]

If the functional result of using a global privacy control is simply that every site or app will then harass you for permission to ignore, the controls will end up being ineffective failures for consumers. For this reason, there is a strong policy argument to prohibit re-opt-in to ignore global signals since the costs of re-opt-in (hassle, user experience, inadvertently granting consent) will almost certainly outweigh the benefits to the narrow slice of consumers who want to make targeted exceptions to a universal opt-out choice, though such a prohibition. This is the approach take by S. 6701-B introduced by Senator Thomas in the New York legislature which states that companies:

> MUST NOT REQUEST THAT A CONSUMER WHO HAS OPTED OUT OF CERTAIN PURPOSES OF PROCESSING PERSONAL DATA OPT BACK IN, UNLESS THOSE PURPOSES SUBSEQUENTLY BECOME NECESSARY TO PROVIDE THE SERVICES OR GOODS REQUESTED BY A CONSUMER. TARGETED ADVERTISING AND SALE OF PERSONAL DATA SHALL NOT BE CONSIDERED PROCESSING PURPOSES THAT ARE NECESSARY TO PROVIDE SERVICE OR GOODS REQUESTED BY A CONSUMER.[97]

At the very least, the rules should disincentivize unwanted nudges, require a very high standard for consent for re-opt-in, and aggressively constrain the use of dark patterns to subvert user intentions.

In the event that a newly invoked global control setting contradicts an earlier permission to engage in targeted advertising or data sales, the newer global signal should control. At this point, if allowed, a company may ask for consent to engage in targeted advertising or data sale notwithstanding the general preference articulated by the signal. If the user's consent is

---

[96] Jennifer Bryant, *Belgian DPA fines IAB Europe 250K euros over consent framework GDPR violations*, IAPP, (Feb. 2, 2022), https://iapp.org/news/a/belgian-dpa-fines-iab-europe-250k-euros-over-consent-framework-gdpr-violations.

[97] Senate Bill S6701B, https://www.nysenate.gov/legislation/bills/2021/S6701.

consistent with the rule's strict requirements, then it could be reasonable to allow the company to prospectively disregard the general global privacy setting unless and until they revoke the specific exception granted to the company.[98]

Given the significant potential for abuse of re-opt-in, companies should be required to respond to global privacy signals with a prominent and persistent notice about the user's opt-out or re-opt-in state — as has been proposed in regulations proposed by the California Privacy Protection Agency and Colorado Department of Law.[99] A user would then always be able to see if their opt-out preferences were being honored, and could take steps to adjust their settings if they were different than expected. Alternatively, the rules could provide that consumers should be able to assume that global privacy controls are operative, and only companies that *disregard* an global privacy control — either because the company believes it has re-opt-in consent or because it does not believe the signal conforms to the FTC's requirements for a global signals — must provide prominent notice to consumers that the signal is not considered an operative opt-out. This approach would incentivize companies to respect global signals and disincentivize bad faith efforts to generate spurious consent. For either of these approaches, a company providing notice that a global signal is being disregarded should include clear instructions on how to remedy a defective setting or how to revoke consent if the consumer so desires.

VII. Notice, Transparency, and Disclosure

83. To what extent should the Commission consider rules that require companies to make information available about their commercial surveillance practices? What kinds of information should new trade regulation rules require companies to make available and in what form?

---

[98] Such an approach would be consistent with what has been proposed under California law by the CPPA. See California Privacy Protection Commission, Text of Proposed Regulations, (Jul. 8, 2022), § 7025(c)(3), https://cppa.ca.gov/regulations/pdf/20220708_text_proposed_regs.pdf.

[99] *Id.*, § 7025(c)(6); Colorado Department of Law, Consumer Protection Section, Colorado Privacy Act Rules, 4 CCR-904-3, Rule 5.08(E), https://coag.gov/app/uploads/2022/10/CPA_Final-Draft-Rules-9.29.22.pdf. In the original version of the draft California regulations published this summer, companies were required to display opt-out state to consumers. In the current versions of both regulations, this visual indication is only optional.

The current “notice and choice” regime, in which consumers are expected to read extensive privacy policies and make “all or nothing” decisions about whether to use an online service or app, makes it impossible for consumers to meaningfully participate in the market while protecting their privacy. Even if consumers had the time to read every privacy policy and statement, they would in most cases come away with woefully incomplete information. Such policies tend to be vague and expansive, designed to protect a company from liability rather than inform privacy-conscious consumers. In many cases, the companies themselves have not decided to whom data will be sold and the purposes for which it will be used. It is impossible for consumers to assess the cost of a loss of control over their personal information, or to determine a value and “trade” their data for goods or services.

The solution to this problem is not simply better privacy policies. Even if such policies contained complete and understandable information, no consumer has the capacity or would want to process such policies for every website, app, and service they use and make discrete choices about their personal privacy. Even asking consumers to manage cookie settings on individual pages is overly burdensome and impractical; expecting consumers to read hundreds of different privacy policies is absurd. Simply put, privacy policies are not a useful mechanism for providing information to consumers.

That said, privacy policies may still play some role in a privacy regulation regime. While consumers should not be expected to read privacy policies in the ordinary course of business, they can still provide simple and clear instructions to consumers on how to exercise privacy rights such as the right of access. Moreover, privacy policies can serve another role in providing detailed information to regulators, advocates, researchers, and journalists to ensure that information practices of the biggest companies are consistent with the Data Minimization and other privacy rules.

As detailed in our Model State Privacy Act, Consumer Reports recommends a bifurcated approach to privacy policies: (1) all companies should provide a short, accessible, and clear description on how consumers should exercise privacy rights and (2) the largest and most sophisticated companies should provide detailed information about their data processing activities to create transparency and external accountability for what they do with personal

data.[100] For the latter function, privacy policies should thus function more like SEC filings — providing detailed information to the most sophisticated audiences but which no ordinary consumer is expected to read or understand. However, the mandate to provide this information to the public will still serve as a meaningful check on companies who might otherwise prefer that questionable data processing go unnoticed.

84. **In which contexts are transparency or disclosure requirements effective? In which contexts are they less effective?**
85. **Which, if any, mechanisms should the Commission use to require or incentivize companies to be forthcoming? Which, if any, mechanisms should the Commission use to verify the sufficiency, accuracy, or authenticity of the information that companies provide?**

Without clear mandates, it is unlikely that companies will be sufficiently forthcoming about their data processing practices. Since 2004, California has required that companies publish privacy policies; however that law did not provide details about what information needs to be presented in such a policy.[101] On the other hand, regulators' enforcement of prohibitions on deceptive business practices penalizes companies for making inaccurate statements about data processing in such a policy. As a result, privacy policies have evolved to be nebulous and evasive documents, providing legal cover for current and future business practices while offering insufficient concrete information about what companies are actually doing with data.

The Commission should implement a Transparency Rule to provide for clear transparency and disclosure requirements — at least for the largest and most sophisticated companies — to ensure that their data processing activities accords with the Data Minimization and other Rules that are promulgated. Smaller companies' obligations would be limited to providing clear instructions on how to take advantage of new privacy rights (*see infra* Question 88).

---

[100] *See* Attachment 2, Consumer Reports, *Model State Privacy Act*, (Feb. 2021), § 100, https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf.

[101] The Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575-22579 (2004), https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=BPC&sectionNum=22575.

Without a dramatic expansion of FTC staff (which Consumer Reports has repeatedly recommended),[102] the Commission will have difficulty policing the accuracy and sufficiency of privacy policies — even if such a requirement is limited to the largest companies. However, by mandating such transparency, journalists, advocates, researchers, and other regulators can play a role in evaluating this documentation and holding companies to account.

a. What are the mechanisms for opacity?

86. The Commission invites comment on the nature of the opacity of different forms of commercial surveillance practices. On which technological or legal mechanisms do companies rely to shield their commercial surveillance practices from public scrutiny? Intellectual property protections, including trade secrets, for example, limit the involuntary public disclosure of the assets on which companies rely to deliver products, services, content, or advertisements. How should the Commission address, if at all, these potential limitations?

It is extremely difficult for even sophisticated consumers to understand how companies collect, use, process, and retain data. Most data processing is functionally invisible to consumers; some first-party data collection may be expected given the nature of a customer interaction. However, what happens to that data on a company's servers is inscrutable — it may be retained indefinitely, used for unexpected purposes, sold to data brokers, or inadvertently exposed to hackers.

Offline data sharing is completely unobservable to consumers. Much online data sharing is facilitated directly by a user's browser — consumers can install a special extension to see which third parties a website is sharing data with. However, few consumers actually take the time to do that. Moreover, these tools are less readily available for mobile platforms let alone Internet of Things devices such as smart televisions. Even when data collection is technically observable, it may be encrypted by the company; this prevents inspection by outside hackers but also may prevent inspection by the device's owner.

---

[102] *E.g.*, Letter from Consumer Reports to Honorable Rosa L. DeLauro *et al.*, (May 25, 2021), https://advocacy.consumerreports.org/wp-content/uploads/2021/05/CR-letter-on-FTC-appropriations-052521.pdf.

Consumers who encounter retargeted or surprisingly targeted ads often wonder how companies were able to gain such insights. Even when the source of targeting seems straightforward, consumers cannot know for sure the reason. For example, a recent Consumer Reports study showed that even when manually opting out of cookies on a publisher site, researchers later saw ads from that same company on other sites.[103] However, while it seems likely that the cookie controls on the original site simply did not work, there is no way to know for certain — consumers do not have access to the targeting logic used by marketing companies.

Many companies actively deliberately frustrate efforts of consumers and researchers to hold them accountable for their data practices. For example, researchers at New York University created a tool called Ad Observatory, where they obtained consent from volunteer Facebook users who gave the researchers access to the ads the users were seeing on their newsfeed. This study gave the researchers insight into how political ads were algorithmically targeted to users, and the collected ads were put into a publicly available database for other researchers and journalists to examine.[104] However, in August 2021, Facebook disabled the accounts of the researchers conducting the study, effectively halting their research.[105] As detailed in a recent Consumer Reports white paper, companies can use any number of technical and legal mechanisms to frustrate external research into data practices, including contract terms, computer trespass laws, and intellectual property rights.[106] As a result, it is functionally very difficult to understand how consumers are monitored and tracked online.

b. Who should administer notice or disclosure requirements?

---

[103] Thomas Germain, *I Said No to Online Cookies. Websites Tracked Me Anyway.*, Consumer Reports, (Sep. 29, 2022), https://www.consumerreports.org/electronics-computers/privacy/i-said-no-to-online-cookies-websites-tracked-me-anyway-a8480554809/; *see also* Justin Brookman *et al.*, *Cross-Device Tracking: Disclosures and Measurements*, Privacy Enhancing Technologies Symposium (PETS) 2017 (2):133–148, https://petsymposium.org/2017/papers/issue2/paper29-2017-2-source.pdf.

[104] Shirin Ghaffary, *People do not trust that Facebook is a healthy ecosystem*, Vox, (Aug. 6, 2021), https://www.vox.com/recode/22612151/laura-edelson-facebook-nyu-ad-observatory-social-media-researcher.

[105] Lois Anne DeLong, *Facebook Disables Ad Observatory; Academicians and Journalists Fire Back*, NYU Center for Cybersecurity, (Aug. 21, 2021), https://cyber.nyu.edu/2021/08/21/facebook-disables-ad-observatory-academicians-and-journalists-fire-back.

[106] *See* Attachment 4, Nandita Sampath, *Opening Black Boxes: Addressing Legal Barriers to Public Interest Algorithmic Auditing*, Consumer Reports Digital Lab, (Oct. 2022), https://digital-lab-wp.consumerreports.org/wp-content/uploads/2022/10/CR_Algorithmic_Auditing_Final_10_2022VF2.pdf.

87. **To what extent should the Commission rely on third-party intermediaries (e.g., government officials, journalists, academics, or auditors) to help facilitate new disclosure rules?**
88. **To what extent, moreover, should the Commission consider the proprietary or competitive interests of covered companies in deciding what role such third-party auditors or researchers should play in administering disclosure requirements?**

c. What should companies provide notice of or disclose?

89. **To what extent should trade regulation rules, if at all, require companies to explain (1) the data they use, (2) how they collect, retain, disclose, or transfer that data, (3) how they choose to implement any given automated decision-making system or process to analyze or process the data, including the consideration of alternative methods, (4) how they process or use that data to reach a decision, (5) whether they rely on a third-party vendor to make such decisions, (6) the impacts of their commercial surveillance practices, including disparities or other distributional outcomes among consumers, and (7) risk mitigation measures to address potential consumer harms?**

Consumer Reports recommends the implementation of a Transparency Rule which would provide for a bifurcated model for privacy policies: (1) all companies should provide a short, accessible, and clear description on how consumers should exercise privacy rights and (2) the largest and most sophisticated companies should provide detailed information about their data processing activities to create transparency and external accountability for what they do with personal data.

We recommend the FTC require the following (as adapted from the Consumer Reports Model State Privacy Act):

Transparency about the collection, use, retention, and sharing of personal Information.

(a) A business that collects a consumer's personal information shall disclose the following general information in its privacy policy or policies and update that information at least once every 12 months.

(1) A description of how an individual may exercise their rights pursuant to subsections 103, 105, 110, 115, and 120 and one or more designated methods for submitting requests.

(2) The privacy policy shall be:

(A) Clear and written in plain language, such that an ordinary consumer would understand it;

(B) Conspicuous and posted in a prominent location, such that an ordinary consumer would notice it; and

(C) Made publicly accessible before the collection of personal information.

(b) A large business that collects a consumer's personal information shall also disclose the following comprehensive information in an online privacy policy or policies, and update that information at least once every 12 months:

(1) The personal information it collects about consumers.

(2) The categories of sources from which the personal information is collected.

(3) A reasonably full and complete description of the methods it uses to collect personal information.\

(4) The specific purposes for collecting, disclosing, or retaining personal information.

(5) The personal information it discloses about consumers, or if the business does not disclose consumers' personal information, the business shall disclose that fact.

(6) The categories of third parties with whom it shares personal information, or if the business does not disclose consumers' personal information to third parties, the business shall disclose that fact.

(7) The categories of service providers with whom it shares personal information, or if the business does not

> disclose consumers' personal information to service providers, the business shall disclose the fact.
>
> (8) A description of the length(s) of time for which personal information is retained.
>
> (9) If personal information is deidentified such that it is no longer considered personal information but subsequently retained, used, or shared by the company, a description of the method(s) of deidentification.[107]

90. Disclosures such as these might not be comprehensible to many audiences. Should new rules, if promulgated, require plain-spoken explanations? How effective could such explanations be, no matter how plain? To what extent, if at all, should new rules detail such requirements?

As noted above, (supra Question 83), the audience for privacy policies should not be general audience consumers. Instead, the disclosures should be aimed at sophisticated audiences who have the ability to understand detailed descriptions of how data is collected, used, transferred, and stored. As such, a requirement that a privacy policy be in "plain-spoken" terms would be counterproductive. No consumer should be expected to navigate and digest a company's privacy policy in order to decipher what suspicious data behaviors they may be up to — instead consumers should be able to just reasonably assume there is no suspicious behavior at all.

However, all companies should provide a "plain-spoken" explanation of how to exercise data rights at the beginning of a privacy policy (or in some other standardized and easily accessible place). For example, companies should be required to provide clear and simple instructions on how consumers can access and delete the data that a company has about them, or how to port that data to another service.

---

[107] *See* Attachment 2, Consumer Reports, *Model State Privacy Act*, (Feb. 2021), § 2-100, https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf.

91. Disclosure requirements could vary depending on the nature of the service or potential for harm. A potential new trade regulation rule could, for example, require different kinds of disclosure tools depending on the nature of the data or practices at issue (e.g., collection, retention, or transfer) or the sector (e.g., consumer credit, housing, or work). Or the agency could impose transparency measures that require in-depth accounting (e.g., impact assessments) or evaluation against externally developed standards (e.g., third-party auditing). How, if at all, should the Commission implement and enforce such rules?

See response to Question 83.

92. To what extent should the Commission, if at all, make regular self-reporting, third-party audits or assessments, or self-administered impact assessments about commercial surveillance practices a standing obligation? How frequently, if at all, should the Commission require companies to disclose such materials publicly? If it is not a standing obligation, what should trigger the publication of such materials?

93. To what extent do companies have the capacity to provide any of the above information? Given the potential cost of such disclosure requirements, should trade regulation rules exempt certain companies due to their size or the nature of the consumer data at issue?

See response to Question 83.

VIII. Remedies

94. How should the FTC's authority to implement remedies under the Act determine the form or substance of any potential new trade regulation rules on commercial surveillance? Should new rules enumerate specific forms of relief or damages that are not explicit in the FTC Act but that are within the Commission's authority? For example, should a potential new trade regulation rule on commercial surveillance explicitly identify algorithmic disgorgement, a remedy that forbids companies

from profiting from unlawful practices related to their use of automated systems, as a potential remedy? Which, if any, other remedial tools should new trade regulation rules on commercial surveillance explicitly identify? Is there a limit to the Commission's authority to implement remedies by regulation?

IX. Obsolescence

95. **The Commission is alert to the potential obsolescence of any rulemaking. As important as targeted advertising is to today's internet economy, for example, it is possible that its role may wane. Companies and other stakeholders are exploring new business models. Such changes would have notable collateral consequences for companies that have come to rely on the third-party advertising model, including and especially news publishing. These developments in online advertising marketplace are just one example. How should the Commission account for changes in business models in advertising as well as other commercial surveillance practices?**

The principles promulgated by the Commission should be relatively high-level and universal in application. But we are confident that the general principles of Data Minimization; Security; Nondiscrimination; Access, Deletion, Portability, and Deletion; and Transparency are evergreen.

****

We thank the Federal Trade Commision for its consideration of these points, and for its work to secure strong privacy protections for consumers. We are happy to answer any questions you may have, and to discuss these issues in more detail. Please contact Justin Brookman (justin.brookman@consumer.org) for more information.