

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 Reports¹ 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 facial⁹ and gait-recognition¹⁰ 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 microphones¹² or accessing smart power meters¹³ 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 access²⁸ — 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 viewing³⁵ and geolocation³⁶ 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 data³⁸ — 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

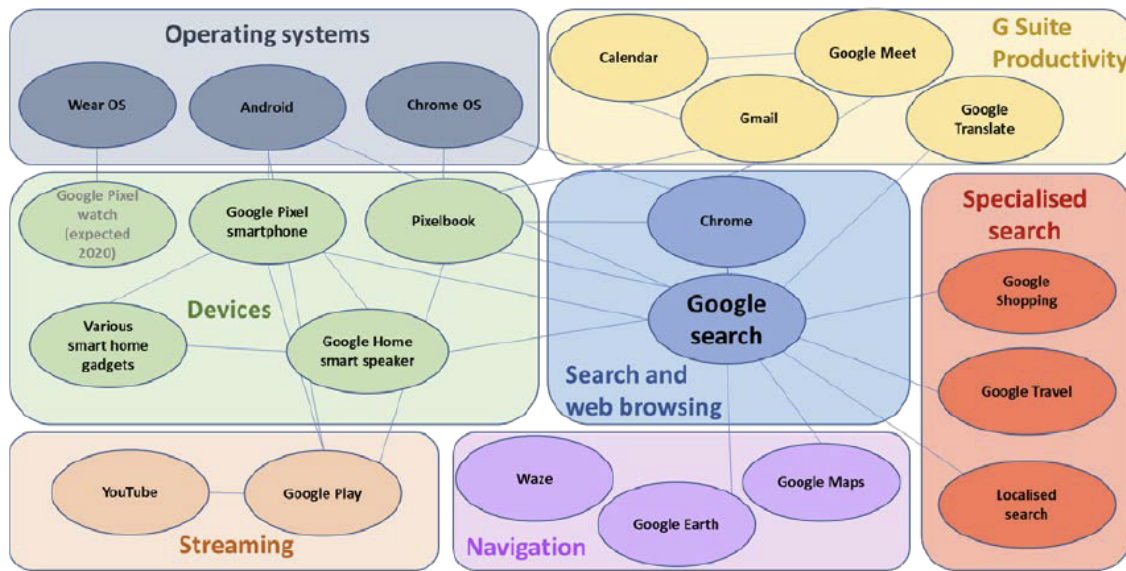
The current online market is dominated by giant online platforms like Facebook and Google that profit from commercial surveillance. This market power is persistent, not temporary. As the recent G7 communique notes:

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; Autorità 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.

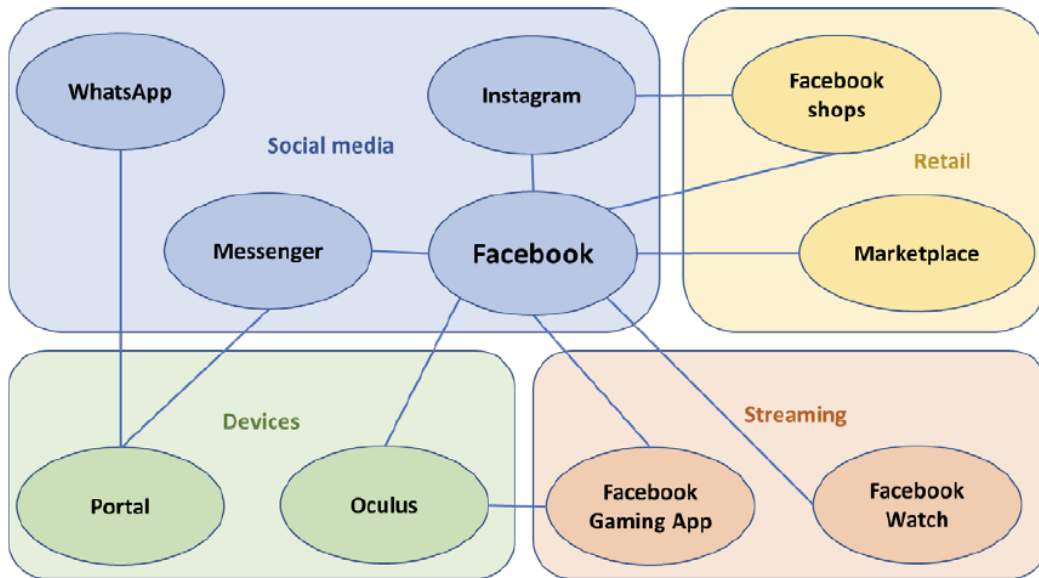
The harmful effects of this market power are widespread as the largest online platforms operate across the digital ecosystem providing a variety of online services and connected devices. The invasive data collection is an important contributor to this market power is also widespread as these giant online 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

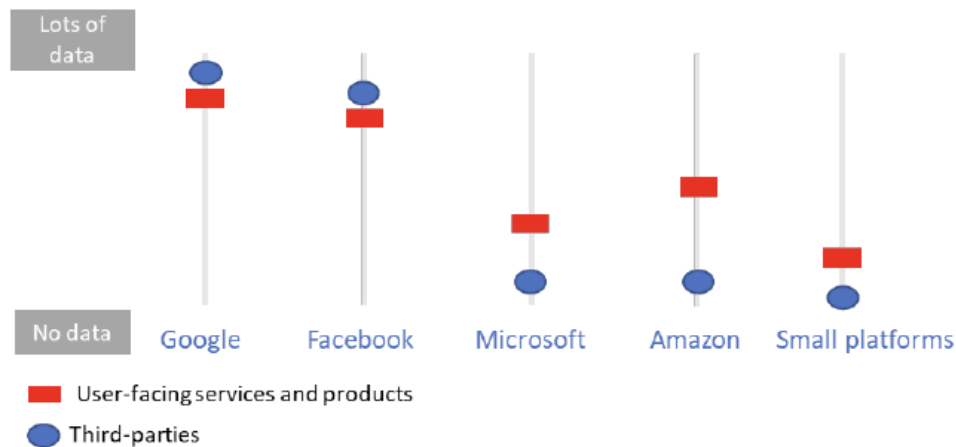


Source: Figure E.2., Appendix E: Ecosystems, Online platforms and digital advertising, Market Study Final Report, UK CMA, 1 July 2020.

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-spokespers-on-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/bills/117/congress-house/bills/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_FTCDDataMinimization_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,

⁸²E.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 assess 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 opt-out 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 taken 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.ca.gov/faces/codes_displaySection.xhtml?lawCode=BPC§ionNum=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 Commission 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.

How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking

January 26, 2022



epic.org

ELECTRONIC
PRIVACY
INFORMATION
CENTER

Executive Summary

Unfair data collection practices and surveillance have eroded consumer privacy, and this ever present and unwanted observation constitutes a substantial injury to consumers. This paper argues that the Federal Trade Commission (FTC) should use its Section 5 unfairness authority to establish a Data Minimization Rule to prohibit all secondary data uses with limited exceptions, ensuring that people can safely use apps and online services without having to take additional action. It also lays out two additional options to consider should the FTC decline to prohibit all secondary uses: prohibit specific secondary data uses, such as behavioral advertising or the use of sensitive data; or mandate a right to opt out of secondary data use, including through global opt-out controls and databases.

Additionally, to supplement this Data Minimization Rule, the FTC should adopt data transparency obligations for primary use of data; civil rights protections over discriminatory data processing; nondiscrimination rules, so that users cannot be charged for making privacy choices; data security obligations; access; portability; correction; and deletion rights. In addition, the FTC should prohibit the use of dark patterns with respect to data processing.

The FTC has wide authority to issue prescriptive rules in order to forestall business practices that can cause consumer injury. With respect to judicial interpretation, the courts generally give broad deference to expert agencies' interpretation of their substantive statutes, and these privacy regulations are likely to withstand First Amendment scrutiny.

Table of contents

Executive Summary	1
Introduction	3
Problem Statement: Unwanted Surveillance Harms Consumers	5
The FTC’s Authority to Promulgate Unfair Trade Practices Rules	8
Establishing a Data Minimization Rule Under Section 5 of the FTC Act	14
Option 1: Prohibit most secondary processing by default	16
Option 2: Prohibit specific secondary uses	19
Option 3: Mandate compliance with opt-outs (including universal opt-outs)	22
Other Privacy Protections That Should be Implemented Through Section 5 of the FTC Act	24
Primary Use Transparency	24
Civil Rights	26
Nondiscrimination	28
Data Security	29
Access, Portability, Correction, Deletion	32
Prohibition on the Use of Dark Patterns	34
Judicial Review of FTC Unfairness Rules	34
Deference to Agency Interpretation	35
Privacy Rules Can Be Crafted to Withstand First Amendment Scrutiny	37
Conclusion	38

I. Introduction

In the absence of comprehensive privacy rules, the surveillance of internet users has become omnipresent over the last thirty years and the profiling, targeting, and monetizing of consumers' online behaviors has become endemic.¹ The Federal Trade Commission ("FTC" or "Commission") has explored this problem in numerous workshops and studies,² and the European Union (EU), through the General Data Protection Regulation (GDPR), and some states, such as California through the California Consumer Privacy Act (CCPA), have begun to establish baseline privacy protections.³ Those protections, however, are largely procedurally focused, with far too little substantive protection. Crucially, there is no comprehensive federal privacy law in the United States that allocates responsibilities with respect to user data, restricts data collection and use, or establishes standards for data security, access, or accountability. The FTC has brought a number of important privacy enforcement actions against companies for violating general purpose consumer protection law or sectoral privacy legislation, but those actions have not been successful in comprehensively reforming industry practices. The President of the United States recently emphasized the need for federal guidelines to rein in data collection, use, and disclosure: His executive order encouraged the FTC to pursue a rulemaking to address "unfair data collection and surveillance practices that may damage competition, consumer autonomy, and consumer privacy."⁴

To address unfair surveillance and data collection practices that endanger consumer privacy and autonomy, it is necessary to limit wide scale tracking and profiling of consumers online. One of the core principles underlying modern privacy and data protection laws, the data minimization principle, provides that data should only be collected, used, or disclosed as reasonably necessary to provide the service requested by a consumer. People should be able to use the internet and apps, including for work and school, with their privacy protected by default. They should be able to take advantage of new technologies and services without fear that their choices and behaviors will be logged and tracked by other companies or used against

¹ Kaveh Waddell, *California Privacy Law Prompts Companies to Shed Consumer Data*, Consumer Reports (Feb. 11, 2020), <https://www.consumerreports.org/privacy/california-privacy-law-ccpa-prompts-companies-to-shed-consumer-data/>.

² See, e.g., *Protecting Consumers in the Next Tech-ade: A Report by the Staff of the Federal Trade Commission*, Fed. Trade Comm'n (Mar. 2008), <http://www.ftc.gov/os/2008/03/P064101tech.pdf>; *Self-Regulatory Principles For Online Behavioral Advertising, Behavioral Advertising Tracking, Targeting, & Technology*, Fed. Trade Comm'n Staff Report (Feb. 2009), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf>; *Protecting Consumer Privacy in an Era of Rapid Change: A Framework for Businesses and Policymakers*, Fed. Trade Comm'n (March 2012), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-behavioral-rapid-change-recommendations/120326privacyreport.pdf>.

³ Regulation (EU) 2016/679 (General Data Protection Regulation), <https://gdpr-info.eu/>; Cal. Civ. Code § 1798.100 et seq.

⁴ Executive Order on Promoting Competition in the American Economy (July 9, 2021), <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/>.

their interests. As the FTC begins to consider potential privacy rules in response to the President's executive order, it should prioritize restrictions that address and limit data collection as well as secondary uses and disclosure of the data that is amassed and stored.

This paper argues the FTC should promulgate a Data Minimization Rule under the unfairness prong of Section 5 to regulate secondary data processing. We present three different possible approaches for how the FTC could draft such a rule, and provide legal justification, as well as the policy considerations, for each path:

- Prohibit all secondary data uses with limited exceptions;
- Prohibit specific secondary data uses, such as behavioral advertising or the use of sensitive data; or
- Mandate a right to opt out of secondary data use, including through global opt-out controls and databases.

Of these options, we believe that the first — prohibiting secondary use with narrow carveouts — would be the most effective in safeguarding consumers' expectations and fundamental right to privacy. However, we also offer alternative paths that, while less expansive, could still offer robust protections to consumers without constantly burdening them with privacy choices and consent requests.

In addition, we propose that the FTC draft additional rules for consumers, consistent with the Fair Information Practices Principles, to better ensure data privacy and security. These provisions could be formulated in tandem with a Data Minimization Rule, or as part of separate proceedings:

- Establish data transparency obligations for primary use of data;
- Establish civil rights protections over discriminatory data processing;
- Establish nondiscrimination rules, so that users cannot be charged for making privacy choices;
- Establish data security obligations;
- Secure access, portability, correction, and deletion rights over data collected about a consumer; and
- Prohibit the use of dark patterns around data processing.

The FTC has over the last twenty years exercised regulatory authority under Section 5 of the FTC Act to limit unfair and deceptive privacy practices, but the Commission has not established comprehensive rules to prevent and limit privacy injuries. The FTC has ample authority to pursue such a rulemaking under Section 5. Courts have made clear that the FTC has broad authority to define unfair trade practices on a discretionary basis, and thus the power to address the substantial privacy harms caused by behavioral advertising and the related excessive collection, use, and disclosure of user data. In its privacy cases over the last twenty years, the FTC established that businesses can be liable when they collect, use, or disclose data in ways that exceed consumers' expectations. Further, recent FTC enforcement actions

highlight the breadth of privacy injuries that fall under the FTC’s Section 5 authority. For example, the FTC’s complaint and consent order with Zoom Video Communications showed that even potential exposure of personal data (and thus the risk of injury) can constitute a substantial injury, as can the circumvention of a platform’s privacy settings.⁵

This paper will first discuss the problem to be solved — the wholesale erosion of privacy in recent years. It will then analyze the FTC’s legal authority to issue regulations under its Section 5 unfairness authority. While the FTC has only used this authority sparingly, it has wide discretion in using this power to issue prescriptive rules to forestall business practices that can cause consumers substantial injury.

We then present the three potential options for a Data Minimization Rule to limit companies’ secondary use of consumers’ personal information, along with an analysis of how each could be justified under the FTC’s Section 5 authority. Next, we discuss other attributes of privacy law and how they would be justified under unfairness as well. Finally, we discuss potential judicial review of FTC privacy rules, describing how the courts generally give broad deference to expert agencies’ interpretation of their substantive statutes, and why privacy regulations are likely to withstand First Amendment scrutiny.

II. Problem Statement: Unwanted Surveillance Harms Consumers

Consumers are constantly tracked: online, through their use of apps, and in the physical world, via cameras and the like. This information reveals consumers’ most sensitive characteristics, including health conditions, sexual orientation, sexual activities, gender, political affiliations, and union membership, and is transferred to hundreds, if not thousands, of different companies, typically without their knowledge or consent.⁶ 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.

Fundamentally, much data processing — notably much *secondary data processing*, or processing not directly in service of fulfilling a consumer’s request — fundamentally violates consumers’ right to privacy — the “right to be let alone,” as articulated by Samuel Warren and

⁵ Compl., *In the Matter of Zoom Video Communications, Inc.*, Comm’n File No. 1923167 (Nov. 9, 2020).

⁶ See, e.g., Letter from Access Now et al., to Chair Khan and Commissioners Chopra, Slaughter, Phillips, and Wilson (Aug. 4, 2021), <https://www.lawyerscommittee.org/wp-content/uploads/2021/08/FTC-civil-rights-and-privacy-letter-Final-1.pdf>.

Louis Brandeis.⁷ This concept has been incorporated into federal privacy laws like the Privacy Act of 1974. It has been further developed by scholars, including Helen Nissenbaum, who has argued that much data disclosure and secondary use betrays the original purpose of the collection and expectations of individuals, which she describes as *contextual integrity*. Indeed, 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.

As such, rather than focus entirely on specific injuries tied to the collection and use of data, the FTC should recognize that the unwanted observation, through excessive data collection and use, is harmful in and of itself. It necessarily subjects consumers to the risk of data breaches, employee misuses, unwanted secondary uses, inappropriate government access, and can have a chilling effect on consumers' willingness to adopt new technologies, and to engage in free expression.⁸ Privacy scholars Danielle Citron and Daniel Solove have identified myriad privacy harms that go beyond economic and physical harm that stem from secondary data processing, including psychological harms, reputational damage, and restricting or unduly influencing consumers' choices.⁹ Given companies' strong incentives to continue to freely collect data, self-regulation has not been and will never be sufficient to protect consumers against these harms. And with the ever-growing sophistication of technology, without policy intervention, unwanted, unexpected, and ultimately disadvantageous (to individuals) surveillance will only become more widespread.

The tracking implemented by platforms like Google and Facebook is not technically necessary to rendering services, and it assaults long-held norms surrounding privacy. For instance, letter writing has long been a private activity, protected by law. Americans have a legally protected interest in the confidentiality of their postal mail and their telephonic conversations. Google's implementation of email, however, sought to track both content and the identity of communicating parties in a way that would violate criminal statutes if performed in the postal mail or telephone. For another example, consider search: the librarian who would assist a patron in finding information owed a duty of confidentiality to the patron and could not retain transactional records of book borrowing. Google's implementation of search turns this on its head, making information retrieval a commercial transaction, even where the user seeks knowledge of medical conditions.

At a time where it often feels like the country is deeply divided on policy issues, polls repeatedly show that Americans are unified on privacy. In a survey recently conducted by the Future of Technology Commission, a staggering eighty-six percent agreed that "it should be illegal for private companies to sell or share information about people no matter what" and only forty-six percent agreed that it would be okay for companies to "sell consumers' data as long as

⁷ Samuel Warren and Louis Brandeis, *The Right to Privacy*, Harvard L. Rev. IV (5): 193–220 (Dec. 15, 1890), <https://archive.org/details/jstor-1321160/page/n1/mode/2up>.

⁸ Justin Brookman and G.S. Hans, *Why Collection Matters: Surveillance as a De Facto Privacy Harm*, <https://cdt.org/wp-content/uploads/2018/08/September-2013-Brookman-Hans-Why-Collection-Matters.pdf>

⁹ Danielle Keats Citron and Daniel Solove, *Privacy Harms*, GWU Legal Studies Research Paper No. 2021-11 (Feb. 2021), <https://ssrn.com/abstract=3782222>.

they are transparent about how the data is used and make it clear to consumers.”¹⁰ Americans don’t want companies to put more disclosures in privacy policies, they want them to stop trafficking in personal data. And the number of consumers, and the amount of personal information, implicated by companies’ data practices is staggering. 90% of consumers reported that the internet has been either “essential or important” to them during the first year of the Covid-19 crisis and associated lockdowns.¹¹ The average consumer spends nearly seven hours online each day.¹² According to a recent FTC report, one ISP alone has 370 million consumer relationships (compared to a US population of nearly 330 million).¹³ Yet another ISP, according to the report, served one trillion ad requests each month.¹⁴

The risk of security incidents and breaches is amongst the strongest rationales for limiting unnecessary collection of personal information. Security incidents and breaches¹⁵ are commonplace. As former FBI Director Robert S. Mueller quipped, “There are only two types of companies: Those that have been hacked and those that will be hacked.” What this means is that companies that collect personal information routinely fail to live up to their security responsibilities and allow information to be acquired by hackers and hostile governments. In many cases, this information is not only stolen by hackers, but also uploaded to Torrent files, where they are available to anyone. Constella Intelligence found evidence of over 8,500 separate breaches — concerning 12 billion records — circulating on dark web services in 2020.¹⁶

Because companies routinely fail to implement even basic security precautions (despite legal obligations to do so), and because even sophisticated technical powerhouses such as Google fall victim to intrusions¹⁷ that result in total collapse of confidentiality, companies collect data at the peril of the consumer. Companies enjoy the benefit of data collection activities while externalizing the costs of insecurity. Furthermore, consumers have no ability to evaluate

¹⁰ Benson Strategy Group, *Future of Tech Commission: Tech Attitudes Survey (July 20, 2021 - July 29, 2021)*, https://d2e111jq13me73.cloudfront.net/sites/default/files/uploads/pdfs/bsg_future_of_technology_toplevel_c1-1.pdf.

¹¹ Colleen McClain et al., *The Internet and the Pandemic*, Pew Research Ctr. (Sept. 1, 2021), <https://www.pewresearch.org/internet/2021/09/01/the-internet-and-the-pandemic/>.

¹² Simon Kemp, *Digital 2021 April Global Statshot Report*, Data Reportal (Apr. 21, 2021), <https://datareportal.com/reports/digital-2021-april-global-statshot>.

¹³ *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers: An FTC Staff Report*, Fed. Trade Comm’n at 33 (Oct. 21, 2021), https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf.

¹⁴ *Id.*

¹⁵ See Mahmood Sher-Jan, *Is it an incident or a breach? How to tell and why it matters*, IAPP (Feb. 28, 2017), <https://iapp.org/news/a/is-it-an-incident-or-a-breach-how-to-tell-and-why-it-matters/> These are two distinct kinds of spills of personal information. Security incidents are revelations of user information that do not require notice to users and regulators. Security breaches are those incidents that require notice under state laws and other regulations.

¹⁶ *2021 Identity Breach Report*, Constella Intelligence at 5, <https://info.constellaintelligence.com/2021-identity-breach-report>.

¹⁷ See Nicole Perlroth, *This Is How They Tell Me The World Ends: The Cyberweapons Arms Race* (2021) (describing the “Aurora” hack).

security practices of companies and no defenses against hacks and dumps of their personal information. The most efficacious countermeasure for this peril is the limitation of how much and what data may be collected.

For these reasons, it is essential that the FTC pursue a privacy rulemaking to establish meaningful data minimization. Below, we outline the FTC's authority to pursue such a rule, lay out three possible approaches to minimizing data processing, and discuss key additional protections, such as transparency obligations for primary data use; civil rights protections; non-discrimination to prevent charging consumers for exercising their privacy rights; data security, access, portability, correction and deletion rights; and a prohibition on dark patterns.

III. The FTC's Authority to Promulgate Unfair Trade Practices Rules

The Federal Trade Commission is broadly charged with prohibiting unfair trade practices, which include “[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce.”¹⁸ “Unfair methods of competition” and “unfair or deceptive acts and practices” are separate legal authorities; while the FTC has traditionally viewed privacy issues through the lens of “unfair and deceptive,” the FTC has in some ways broader (if untested) authority under “unfair methods of competition,” including the ability to use Administrative Procedure Act rulemaking.¹⁹ Last year, the advocacy group Accountable Tech filed a petition with the FTC asking the agency to ban surveillance advertising under its “unfair methods of competition” authority.²⁰ This paper focuses instead on the FTC's powers under “unfair and deceptive acts and practices,” the traditional source of the FTC's privacy jurisprudence. Ultimately, however, our goal is to see the enactment of a robust Data Minimization Rule and related privacy protections; if the FTC decides it has a stronger case to justify such rules under “unfair methods of competition,” we would strongly support such an effort.

Under its authority to prevent unfair and deceptive practices,²¹ the Commission is specifically authorized to issue trade regulation rules “which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce[.]”²² As will be discussed below, this rulemaking authority is more constrained than traditional APA rulemaking, but the FTC nonetheless has broad discretion to issue regulations that proscribe “prevalent” business practices that cause consumers significant injury. A violation of a trade regulation rule constitutes an unfair or deceptive act or practice unless the Commission provides otherwise in the rule.²³

¹⁸ 15 U.S.C. § 45(a)(1).

¹⁹ Rohit Chopra and Lina Khan, *The Case for “Unfair Methods of Competition” Rulemaking*, 87 U Chi. L. Rev. 357 (2020).

²⁰ Accountable Tech, *Petition for Rulemaking to Prohibit Surveillance Advertising* (Sept. 28, 2021), <https://accountabletech.org/wp-content/uploads/Rulemaking-Petition-to-Prohibit-Surveillance-Advertising.pdf> [hereinafter Accountable Tech Rulemaking Petition].

²¹ 15 U.S.C. § 45(a)(2).

²² 15 U.S.C. § 57a(a)(1)(B).

²³ 16 C.F.R. § 1.8(a).

Congress has also charged the Commission with promulgating non-binding “interpretive rules and general statements of policy with respect to unfair or deceptive acts or practices in or affecting commerce” and also “rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce[.]”²⁴ Under Section 5(m)(1)(A) of the FTC Act, the FTC can pursue civil monetary penalties against any firm that knowingly violates a trade regulation rule with respect to unfair or deceptive acts or practices.²⁵ Finally, pursuant to its Penalty Offense Authority, the Commission may seek monetary penalties “against a party that engages in conduct it knows has been determined to be unlawful in a Commission order”²⁶ so long as the order is final and not a consent order.²⁷

Below is a table of the FTC’s authorities to promulgate unfair trade practice rules.

FTC’s Authority	Legal Basis	Legal Effect
Unfair and Deceptive Practices (“UDAP”) Power	The FTC is charged with prohibiting unfair trade practices, which include “[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce.” ²⁸	The Commission is empowered to prevent such practices. ²⁹
Trade Regulation Rules Power	The FTC is specifically authorized to issue trade regulation rules “which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce[.]” ³⁰	A violation of a trade regulation rule constitutes an unfair or deceptive act or practice unless the Commission provides otherwise in the rule. ³¹
Authority of Commission to prescribe rules and general statements of policy	Congress has charged the Commission with promulgating “interpretive rules and general statements of policy with respect to unfair or deceptive acts or practices in or affecting commerce” and also “rules which define with specificity	“These guidance documents are not substantive rules and do not have the force or effect of law. They are administrative interpretations of the statutes and rules administered by the

²⁴ 15 U.S.C. § 57a(a)(1)(A)-(B).

²⁵ 15 U.S.C. § 45(m)(1)(A).

²⁶ Rohit Chopra & Samuel A.A. Levine, *The Case for Resurrecting the FTC Act's Penalty Offense Authority* (Oct. 29, 2020), 169 U. Pa. L. Rev. 1, 12-13 (forthcoming 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3721256; See 15 U.S.C. § 45(m)(1)(B).

²⁷ 15 U.S.C. § 45(m)(1)(B).

²⁸ 15 U.S.C. § 45(a)(1)

²⁹ 15 U.S.C. § 45(a)(2).

³⁰ 15 U.S.C. § 57a(a)(1)(B).

³¹ 16 C.F.R. § 1.8(a).

	acts or practices which are unfair or deceptive acts or practices in or affecting commerce[.]” ³²	Commission, and they are advisory in nature.” ³³
Penalty Offense Authority	The Penalty Offense Authority “allows the Commission to seek penalties against a party that engages in conduct it knows has been determined to be unlawful in a Commission order[.]” so long as the order is final and not a consent order. ³⁴	“In order to trigger this authority, the Commission can send companies a ‘Notice of Penalty Offenses.’ This Notice is a document listing certain types of conduct that the Commission has determined, in one or more administrative orders (other than a consent order), to be unfair or deceptive in violation of the FTC Act. Companies that receive this Notice and nevertheless engage in prohibited practices can face civil penalties of up to \$43,792 per violation.” ³⁵
FTC Act Section 5(m)(1)(A) Authority	This authority allows the FTC to seek penalties against parties who have violated a Commission rule “with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive and is prohibited by such rule.”	The FTC can pursue civil monetary penalties against any firm that knowingly violates a trade regulation rule with respect to unfair or deceptive acts or practices. ³⁶

The FTC is tasked with using these broad and flexible authorities to address emerging and evolving injuries. The FTC has historically brought most of its privacy cases under its *deception* authority; however, in such cases, the FTC must demonstrate that an offender misled consumers. As a result, companies are incentivized to not make affirmative privacy representations, leading to evasive privacy policies and other consumer-facing statements that provide consumers little concrete information. The FTC has wider authority to rein in bad privacy behaviors under its unfairness prong. Here the FTC Act provides that an act or practice is unfair

³² 15 U.S.C. § 57a(a)(1)(A)-(B).

³³ *Guidance Documents*, Fed. Trade Comm’n, <https://www.ftc.gov/enforcement/guidance>.

³⁴ Chopra and Levine, *supra* note 26 at 12-13.

³⁵ *Notice of Penalty Offenses*, Fed. Trade Comm’n, <https://www.ftc.gov/enforcement/penalty-offenses>.

³⁶ 15 U.S.C. § 45(m)(1)(A).

when it “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.”³⁷ Per the Ninth Circuit Court of Appeals, “In determining whether consumers’ injuries were reasonably avoidable, courts look to whether the consumers had a free and informed choice.”³⁸ But courts have made clear that the Commission’s unfairness authority is not limited to “situations involving deception, coercion, or withholding of material information.”³⁹

Courts have had few opportunities to review the scope of FTC unfairness rules since the Commission issued its Policy Statement in 1980. Since its enactment, the FTC has promulgated only seven rules under Magnuson-Moss (“Mag-Moss”) that are active today.⁴⁰ Though not used frequently, the Commission has previously promulgated an unfair practices rule to prevent optometrists from withholding contact lens and eyeglass prescriptions from patients, known as the “Eyeglass Rule.”⁴¹ The rule prohibits an ophthalmologist or optometrist from “Fail[ing] to provide to the patient one copy of the patient’s prescription immediately after the eye examination is completed,” from “[c]ondition[ing] the availability of an eye examination to any person on a requirement that the patient agree to purchase any ophthalmic goods from the ophthalmologist or optometrist,” and from other related practices that deny the patient the ability to use their prescription in the best way they see fit.⁴² This rule ensures that consumers can “comparison shop when buying prescription eyewear,” and is not tied to any deceptive practice.⁴³ The FTC would similarly have the ability to promulgate rules that prevent online firms from subjecting consumers to unwanted tracking and behavioral advertising that would deprive them of the ability to use and enjoy internet services while maintaining their privacy.

In those few cases where courts have reviewed the scope of the FTC’s unfairness authority, courts have made clear that Congress delegated “broad discretionary authority” to the Commission to “define unfair trade practices on a flexible, incremental basis.”⁴⁴ Given its broad delegation of authority to define unfairness, the Commission has the power to address online data collection, tracking, profiling, and behavioral advertising practices that subject consumers

³⁷ 15 U.S.C. § 45(n).

³⁸ *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1158 (9th Cir. 2010), *as amended* (June 15, 2010); *See Am. Fin. Servs. Ass’n v. FTC*, 767 F.2d 957, 976 (D.C. Cir. 1985).

³⁹ *Am. Fin. Servs. Ass’n v. FTC*, 767 F.2d at 978.

⁴⁰ Jeffrey S. Lubbers, *It’s Time to Remove the “Mossified” Procedures for FTC Rulemaking*, 83 Geo. Wash. L. Rev. 1979, 1997 (2015); *See* Ophthalmic Practice Rules (Eyeglass Rule), 16 C.F.R. ch. I, subch. D, pt. 456 (1992; last amended 2004); *See* Labeling and Advertising of Home Insulation, 16 C.F.R. ch. I, subch. D, pt. 460 (1979; last amended 2019); *See* Credit Practices, 16 C.F.R. ch. I, subch. D, pt. 444 (1984); *See* Used Motor Vehicle Trade Regulation Rule, 16 C.F.R. ch. I, subch. D, pt. 429 (1984; last amended 2014); *See* Funeral Industry Practices, 16 C.F.R. ch. I, subch. D, pt. 453 (1994); *See* Business Opportunity Rule, 16 C.F.R. ch. I, subch. D, pt. 437 (2011); *See* Disclosure Requirements and Prohibitions Concerning Franchising, 16 C.F.R. ch. I, subch. D, pt. 436 (2007).

⁴¹ 16 C.F.R. § 456.2.

⁴² 16 C.F.R. § 456.2.

⁴³ Leslie Fair, *A prescription for complying with the Eyeglass Rule*, Fed. Trade Comm’n, (Dec. 2020), <https://www.ftc.gov/news-events/blogs/business-blog/2020/12/prescription-complying-eyeglass-rule>.

⁴⁴ *Id.* at 967.

to significant privacy injuries. There is precedent for the FTC to promulgate a trade rule under its enforcement authority to prohibit unfair acts and practices in an industry.

The scope of privacy injuries, as with other injuries redressable under the FTC Act, is broad and varied. Courts have found that “businesses can cause direct consumer harm as contemplated by the FTC Act in a variety of ways. In assessing that harm, [courts] look of course to the deceptive nature of the practice, but the absence of deceit is not dispositive.”⁴⁵ The FTC has detailed many categories of consumer privacy harms that can give rise to actions and regulations under Section 5, including informational injuries from privacy and security incidents.⁴⁶ In the Commission’s Informational Injury Workshop Report, the FTC outlined both market-based injuries, such as financial costs to the consumer, which can be objectively measured, and non-market injuries, which can be harder to objectively measure, that harm consumer privacy.⁴⁷ Some examples include medical identity theft, doxing, disclosure of private information, thwarted expectations and choices, and erosion of trust.⁴⁸ The privacy injuries caused by surveillance advertising are substantial, and these business practices fall within the scope of the Commission’s Section 5 authority.

The recent enforcement action against Zoom Video Communications (“Zoom”) shows that even *potential* exposure of personal data can constitute a substantial injury, as can the circumvention of privacy-enhancing capabilities in consumers’ browsers and other devices. For example, the FTC filed a complaint and entered into a consent order with Zoom regarding Zoom’s failure to properly secure communications in its services. The FTC held that the secret implementation of a web server onto users’ computers, which circumvented Safari browser safeguards, was an unfair and deceptive trade practice.⁴⁹ But other FTC⁵⁰ and state Attorney General⁵¹ privacy enforcement cases have been predicated on the notion that unwanted collection of personal information was intrinsically harmful.

The FTC has recently explained that data security injuries can be privacy injuries. In her dissenting statement in the Zoom settlement, Commissioner Slaughter explained that the FTC needs to go further to ensure that consumer privacy is protected, noting that the order “requires Zoom only to establish procedures designed to protect user *security* and fails to impose any requirements directly protecting user *privacy*.” As Commissioner Slaughter explained, “[t]oo often we treat data security and privacy as distinct concerns that can be separately preserved. In reality, protecting a consumer’s privacy and providing strong data security are closely

⁴⁵ *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1156 (9th Cir. 2010), as amended (June 15, 2010).

⁴⁶ *FTC Informational Injury Workshop*, Fed. Trade Comm’n, (Oct. 2018), https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf.

⁴⁷ *Id.* at n.1.

⁴⁸ *Id.* at 1-3.

⁴⁹ Compl., *In the Matter of Zoom Video Communications, Inc.*, Comm’n File No. 1923167 (Nov. 9, 2020).

⁵⁰ Compl., *In the Matter of Sears Holdings Management Corp.*, Comm’n File No. 0823099 (Sept. 9, 2009).

⁵¹ Assurance of Voluntary Compliance, *In the Matter of Pointroll Inc.* (Dec. 10, 2014), https://portal.ct.gov/-/media/AG/Press_Releases/2014/20141211OAGDCPPointRollAVCpdf.pdf.

intertwined, and when we solve only for one we fail to secure either.”⁵² She further explained that “the reason customers care about security measures in products like Zoom is that they value their privacy.”⁵³ Thus, the FTC has recently articulated the importance of addressing privacy harms and it is therefore appropriate for the FTC to promulgate a trade regulation rule to protect consumers against business practices that invade their privacy.

Because the FTC has a broad toolkit that it can employ to protect consumers against general harms, the FTC is uniquely suited to prevent these injuries. According to privacy scholars Danielle Citron and Daniel Solove, “[T]he FTC is able to focus on harm to consumers generally, which allows it to look to harm in a broader manner than most tort and contracts cases, which involve specific individuals.”⁵⁴ Moreover, as explained by privacy scholars Woodrow Hartzog and Daniel Solove, “[T]he FTC is so critical in the modern privacy regulatory scheme” because “it has a considerably broad and diverse toolkit from which to fashion remedies which allows the commission to redress non-traditional forms of harm, balance data protection against countervailing interests in ways that other areas of law are currently unable to do, and create proactive solutions like those that rely upon design obligations to decrease risks of privacy and security harms ex ante.”⁵⁵ While calling the FTC the “Lynchpin of U.S. Data Protection Law[,]” academics have highlighted that “[r]apid technological change continues to vex courts and lawmakers or leave consumers vulnerable to privacy harms.”⁵⁶

Because incremental injuries that affect many people can be substantial and because their negative impacts can materialize over time, “The FTC can regulate with a much different and more flexible understanding of harm than one focused on monetary or physical injury.”⁵⁷ A practice causes “substantial injury” when it may cause serious harm to a small number of individuals or relatively small harms to many individuals.⁵⁸ According to Citron and Solove:

For many privacy harms, the injury may appear small when viewed in isolation, such as the inconvenience of receiving an unwanted email or advertisement or the failure to honor people’s expectation that your data would not be shared with third parties. But when done by hundreds or thousands of companies, the harm adds up. Moreover, these small harms are dispersed among millions (and sometimes billions)

⁵² Commissioner Rebecca Slaughter, *Dissenting Statement of Commissioner Rebecca Kelly Slaughter In the Matter of Zoom Video Communications, Inc.*, Comm’n File No. 1923167 (Nov. 9, 2020) at 1, 3.

⁵³ *Id.* at 3.

⁵⁴ Citron & Solove, *supra* note 9, at 17. See also Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 Geo. Wash. L. Rev. 2230, 2284.

⁵⁵ Hartzog & Solove, *supra* note 54, at 2276.

⁵⁶ *Id.* at 2266.

⁵⁷ *Id.*, at 2233–34.

⁵⁸ See Cobun Keegan & Calli Schroeder, *Unpacking Unfairness: The FTC’s Evolving Measures of Privacy Harms*, 15 J.L. Econ. Pol’y 19, 27 (2019), <https://jlep.net/home/wp-content/uploads/2019/01/JLEP-Volume-15-1.pdf> (citing Letter from Federal Trade Commission to Senators Ford and Danforth (Dec. 17, 1980), appended to International Harvester 104 F.T.C. 949, 1070 (1984), <https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness>).

of people. Over time, as numerous people are each inundated by a swarm of small harms, the overall societal impact is significant.⁵⁹

Privacy and data security cases show that the harms of violations often cause broad societal, as well as individual, harm and the “FTC has better tools than those that exist in many other areas of law to address this kind of impact.”⁶⁰

The FTC has brought a significant number of enforcement actions in privacy cases over the last twenty years, and in all cases the Commission has established that consumers expect businesses that collect their data to limit its unauthorized dissemination and use, and that when businesses violate that expectation, they are potentially liable.⁶¹

The greatest potential for establishing a robust unfairness test lies in an explicit acknowledgment of the intrinsic value of personal data. The fact that an entity did not sell consumers’ personal data in a particular case, but nevertheless violated consumers’ established privacy expectations, should not prevent an unfairness case when the value of the data collected, exposed, or shared can in fact be established with reference to the millions of data-fueled transactions taking place every day.⁶²

The “core of fairness in the privacy context” is the premise that data collectors must “refrain from sharing consumer’s sensitive or confidential data with unknown third parties.”⁶³

IV. Establishing a Data Minimization Rule Under Section 5 of the FTC Act

Arguably the most important element of any privacy legislation is how to constrain — or to empower consumers to constrain — secondary use of their information, including the transfer and use of that data for advertising. Primary uses of data — processing that is necessary to provide the functionality by consumers — is typically understandable and noncontroversial.⁶⁴ For example, a company may collect a person’s mailing address to send them a product they ordered or to process a credit card transaction. On the other hand, secondary use of data is often not well understood, and the benefits often do not accrue directly to consumers — indeed, in many cases, the uses seem downright adversarial or antithetical to people’s interests, only serving the interests of companies. Much of the privacy controversy⁶⁵ in recent years and motivation for regulation⁶⁶ has centered around businesses’ disclosure of personal data to data

⁵⁹ Citron & Solove, *supra* note 9, at 3-4.

⁶⁰ Hartzog & Solove, *supra* note 54, at 2283.

⁶¹ Keegan & Schroeder, *supra* note 54, at 32.

⁶² *Id.* at 38.

⁶³ *Id.* at 34.

⁶⁴ That is not to say there should be no rules around primary data processing, but they likely should be considerably less stringent than the rules around secondary — especially adversarial — uses. See *infra* Section V.A-B (“Primary Use Transparency,” “Civil Rights”).

⁶⁵ See, e.g., Farhad Manjoo, *Tackling the Internet’s Central Villain: The Advertising Business*, N.Y. Times (Jan. 31, 2018), <https://www.nytimes.com/2018/01/31/technology/internet-advertising-business.html>.

⁶⁶ Nicholas Confessore, *The Unlikely Activists Who Took On Silicon Valley—And Won*, N.Y. Times (Aug. 14, 2018), <https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html>

brokers and for online advertising. As described above, intrusion upon seclusion has long been recognized as a privacy tort, and consumers have a legitimate interest in constraining functionally unnecessary processing of their data.

For years, the Federal Trade Commission embraced a policy of “notice-and-choice” — companies would publish privacy policies outlining their data processing activities, and consumers would be deemed to have chosen to accept those practices as a condition of using the site.⁶⁷ In practice, however, few consumers actually read privacy policies,⁶⁸ and when they do, the policies typically include limited practical information.⁶⁹ As a practical matter, notice and choice delivers neither notice nor choice.⁷⁰ Few would argue that consumers are better off under this regime.

Balancing user autonomy with hard-and-fast rules for secondary processing can be quite challenging in practice. Legislative proposals to limit secondary uses of personal data have typically applied either “opt-in” or “opt-out” frameworks — a requirement that companies must either ask for affirmative permission for secondary processing, or that they must give consumers the ability to turn off secondary processing. Both models can be flawed in practice: opt-in models can overwhelm consumers with constant requests for permission, as many websites have done in response to European privacy law. Companies may use dark patterns to coax consumers already weary so they click “OK” to cede permission for any and all uses. Meanwhile opt-out regimes such as the CCPA are both difficult to use and wildly impractical if one is to protect oneself in any meaningful way, if consumers have to manually opt out of secondary use for every website, app, or business they interact with, which can amount to thousands of organizations.⁷¹ As a result of both approaches, consumers are forced to take too many steps to safeguard their data. A better model would either constrain data processing to conform to expected privacy norms, or to at least empower consumers to make simple, universal choices regarding their personal information.

Privacy regulation has struggled to find the appropriate role for user choice. Rather than advocating for one particular solution, this paper presents three different approaches for how the Federal Trade Commission could regulate secondary data processing through rulemaking

(“Mactaggart’s proposal instead took aim at the so-called third-party market for personal data, in which companies trade and sell your information to one another, mostly without your knowing about it.”).

⁶⁷ *Privacy Online: A Report to Congress*, Fed. Trade Comm’n (June 1998),

<https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf>.

⁶⁸ Aleecia M. McDonald, Robert W. Reeder, Patrick Kelley, Lorrie Faith Cranor, *A Comparative Study of Online Privacy Policies and Formats* at 6, <https://www.robreeder.com/pubs/PETS2009.pdf>.

⁶⁹ See, e.g., Florencia Marotta-Wurgler, *Understanding Privacy Policies: Content, Self-Regulation, and Markets*, NYU Law and Economics Research Paper No. 16-18 at 4 (Jan. 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2736513.

⁷⁰ See, e.g., Woodrow Hartzog, *Privacy’s Blueprint: The Battle to Control the Design of New Technologies*, Harvard University Press (2018); Neil Richards, *Why Privacy Matters*, Oxford University Press (2021).

⁷¹ *Consumer Reports Study Finds Significant Obstacles to Exercising California Privacy Rights*, Consumer Reports (Oct. 1, 2020), https://advocacy.consumerreports.org/press_release/consumer-reports-study-finds-significant-obstacles-to-exercising-california-privacy-rights/.

interpreting the unfairness prong of Section 5 of the FTC Act. *All three models were developed to minimize the burden on consumers to safeguard their personal information:*

- Prohibit all secondary data uses with limited exceptions;
- Prohibit specific secondary data uses, such as behavioral advertising or the use of sensitive data; or
- Mandate a right to opt out of secondary data use, including through global opt-out controls and databases.

The authors of this paper recommend the first approach — to prohibit all secondary uses with limited exceptions — but offer the other approaches as alternatives that could still provide meaningful privacy protections to consumers. We describe these three models in more detail below.

A. Prohibit most secondary processing by default

One option is to ban most secondary use and third-party disclosure, while explicitly carving out certain exceptions. This approach relies heavily on the principle of data minimization by limiting data processing to what is reasonably necessary to achieve the consumer's specific purpose for dealing with the company or organization.⁷² This is the approach taken by several recent bills, including Senator Sherrod Brown's Data Accountability and Transparency Act of 2020,⁷³ California Assemblymember Buffy Wicks's Minimization of Consumer Data Processing Act,⁷⁴ New York Assemblymember Ron Kim's It's Your Data Act,⁷⁵ as well as Consumer Reports' model state privacy bill.⁷⁶

Many privacy advocates had traditionally argued for requiring *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.⁷⁷ 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.

⁷² It should go without saying that monetizing data in order to fund a service should not be interpreted as "reasonably necessary" to provide a service requested by a consumer.

⁷³ Data Accountability and Transparency Act of 2020, https://www.banking.senate.gov/404?notfound=download/brown_2020-data-discussion-draft;%20california.

⁷⁴ The Minimization of Consumer Data Processing Act, CA AB 3119 (2020), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB3119.

⁷⁵ It's Your Data Act, NY A. 3586 (2021), <https://www.nysenate.gov/legislation/bills/2021/A3586>.

⁷⁶ *Model State Data Privacy Act*, Consumer Reports (Feb. 2021), <https://advocacy.consumerreports.org/research/consumer-reports-model-state-data-privacy-act/>.

⁷⁷ *Most Cookie Banners are Annoying and Deceptive. This Is Not Consent*, Privacy International (May 21, 2019), <https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent>.

An approach that broadly prohibits secondary uses arguably avoids these problems raised by opt-in frameworks, as user consent is insufficient to justify secondary processing: instead processing is limited to (1) what is reasonably necessary to fulfill the consumer's request and (2) other specific use cases as defined by the statute.

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.

To justify such an approach under the FTC's prohibition on unfair business practices, the FTC would have to adopt an expansive interpretation of privacy injury, that unwanted observation and data processing is inherently harmful. The FTC has adopted such a framework in the past: for example, in its 2017 settlement with Vizio, the FTC alleged that collecting and disclosing television viewing data without user permission was likely to cause those users substantial injury.⁷⁸ While the FTC emphasized that such viewing data is inherently "sensitive," it is not clear that television viewing behavior is inherently more personal than any other activity. It would be difficult to argue that purchases or web browsing, for example, is any less revealing and sensitive than information about television programming viewed. More to the point, so much of the information collected is as revealing and sensitive as our intellectual habits (like television viewing) including even seemingly prosaic information like our purchase of alcohol swabs because our everyday purchases and interactions often reveals our health conditions (for instance, Type 1 diabetics use alcohol swabs), sexual orientation, gender, close relationships, and other intimate information.

It is worth noting that the FTC may have a stronger case to prohibit secondary *collection* and *retention* of personal information, as those necessitate companies possessing personal data that they wouldn't otherwise, exposing consumers to potential exposure or misuse. Secondary *use* of already collected and retained data does not generate such additional risk of injury, though the use itself may well be deemed offensive, adversarial, or harmful (see *infra* Section IV.B ("Prohibit specific secondary uses")).

In any event, the FTC should have no difficulty demonstrating that secondary data processing is "prevalent" as required for Section 18 rulemaking. Framing the harms of tracking

⁷⁸ Compl., *Fed. Trade Comm'n, v. Vizio, Inc.*, No. 2:17-cv-00758 (Feb. 6, 2017), https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf; *VIZIO to Pay \$2.2 Million to FTC, State of New Jersey to Settle Charges it Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent*, Fed. Trade Comm'n (Feb. 6, 2017), <https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it>.

broadly makes the prevalence inquiry easier, though many narrower rulemakings, such as only on targeted advertising, would also easily satisfy this test.

While recognizing that data collection and disclosure gives rise to inherent intrusions and risk, most would agree that some exceptions to a general prohibition on secondary processing are functionally necessary and can be crafted in ways to minimize intrusion and risk. Data security, analytics, product improvement, and, potentially, first-party marketing⁷⁹ are common exceptions in privacy legislation, though additional measures should be included to constrain these exceptions and to ensure that they do not swallow the general rule:

- Processing for these purposes should be limited to what is reasonably necessary to achieve the secondary purpose and proportionate to the privacy intrusion.⁸⁰
- Service providers who process data on behalf of a consumer should segment the data from other clients, and should be prohibited from engaging in secondary uses of their own.⁸¹
- Secondary processing should, where possible, be limited to data already collected and retained for a primary purpose in order to minimize new risk of secondary exposure or misuse.
- 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.

The narrower the allowed secondary uses, the higher the FTC’s burden will be to argue that the remaining universe of prohibited uses is harmful. Certain uses — such as for security and fraud prevention — provide concrete benefits that may well countervail the injuries associated with surveillance.

Advertising firms likely would 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.⁸² Under Section 5, only the benefits

⁷⁹ The CR model privacy bill allows for first-party marketing with an opt out. See *Model State Data Privacy Act*, Consumer Reports (Feb. 2021), <https://advocacy.consumerreports.org/research/consumer-reports-model-state-data-privacy-act/>. Other advocates have largely called for the prohibition of any targeting advertising. See *International coalition calls for action against surveillance-based advertising*, Norwegian Consumer Council (Jun. 22, 2021), <https://www.forbrukerradet.no/side/new-report-details-threats-to-consumers-from-surveillance-based-advertising/>.

⁸⁰ See, e.g., Mark Zuckerberg, *The Facts About Facebook*, Wall St. J. (Jan. 24, 2019), <https://www.wsj.com/articles/the-facts-about-facebook-11548374613> (arguing that Facebook needs the ability to use information from cross-site web traffic for fraud deterrence).

⁸¹ It may be reasonable to allow service providers the ability to engage in their own narrow secondary uses — such as service improvement — but they should certainly be prohibited from using other parties’ data for purposes such as their own marketing.

⁸² See, e.g., Veronica Marotta et al., *Who Benefits from Targeted Advertising?*, Carnegie Mellon University, https://www.ftc.gov/system/files/documents/public_comments/2015/10/00037-100312.pdf; Howard Beales, *The Value of Behavioral Advertising*, https://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00117/544506-00117.pdf.

that accrue to *consumers* or *competition* are relevant for consideration. As demonstrated in the Accountable Tech petition, there is a strong argument that the behavioral advertising model has led to the consolidation of market power by giant technology companies such as Google and Facebook.⁸³ 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.⁸⁴

Advertising firms would also likely 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 targeted until recent years.⁸⁵ 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.⁸⁶ 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.⁸⁷ Even assuming some degree of value, it may not be enough to offset the harms and loss of utility that consumers experience as a result of profligate data disclosure and secondary processing.

B. Prohibit specific secondary uses

Another approach to privacy rulemaking would be to prohibit certain secondary uses of data, rather than prohibit all secondary uses by default and then claw back certain acceptable uses. This is the approach taken, for example, by the Center for Democracy & Technology model bill, which prohibits the processing of biometrics, geolocation, and cross-device tracking for secondary purposes.⁸⁸ One significant downside of this approach is that it presumes a less expansive conception of privacy injury — namely, that intrusion on seclusion and the risks posed by additional data storage are not intrinsically harmful and in and of themselves justify

⁸³ Accountable Tech Rulemaking Petition, *supra* note 20.

⁸⁴ Justin Brookman et al., *Cross-Device Tracking: Measurement and Disclosures*, Proceedings on Privacy Enhancing Technologies, 2017 (2):133–148, <https://www.petsymposium.org/2017/papers/issue2/paper29-2017-2-source.pdf>; Steve Englehardt and Arvind Narayanan, *Online Tracking: A 1-million-site Measurement and Analysis*, https://www.cs.princeton.edu/~arvindn/publications/OpenWPM_1_million_site_tracking_measurement.pdf; Altaweel, Good, and Hoofnagle, *Web Privacy Census*, Technology Science (Dec. 14, 2015), <https://techscience.org/a/2015121502/>.

⁸⁵ 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/wp-content/uploads/2019/07/Brookman-Testimony-June-14-2018.pdf>.

⁸⁶ 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.

⁸⁷ 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.

⁸⁸ *Federal Baseline Privacy Legislation Discussion Draft*, Center for Democracy & Technology (Dec. 13, 2018), <https://cdt.org/collections/federal-privacy-legislation/>.

policy intervention. At the very least it sublimates the intrinsic harms of privacy invasion to other, more specific harms. On the other hand, focusing regulation on specific practices that lead to greater injuries to consumers may be more likely to withstand legal challenges to a privacy rule.

To justify such an approach under unfairness, each of the specific uses must be tied to substantial injuries, those injuries must not be reasonably avoidable by consumers, and the injuries must not be outweighed by countervailing benefits to consumers or competition. Some examples of specific harmful practices that some have called to be prohibited include:

- Discriminatory use of data that deprives consumers of opportunities based on protected characteristics (see *infra* Section V.B (“Civil Rights”))
- Tracking users across different devices
- Personalization based on sensitive attributes
- Facial recognition and other biometric identification
- Collection and use of intimate information — about the human body, health, innermost thoughts and searches, sex, sexuality, and gender, and close relationships⁸⁹
- Disclosure of personal information of minors (or children under the age of 13)

Surveillance Advertising

One obvious candidate for specific use restriction is targeted advertising. In recent months, several privacy advocates have called upon regulators to specifically ban surveillance advertising.⁹⁰ Recently, Accountable Tech petitioned the FTC to ban surveillance advertising under its unfair methods of competition authority, arguing that targeted ads perpetuate discrimination, exploit kids and teens, fuel extremism and misinformation, and advantage the largest technology companies over rivals.⁹¹

By banning targeted advertising instead of the underlying data collection and retention associated with it, the FTC would be relying not upon intrusion upon seclusion and the risks associated with data storage, but that the manipulation and coercion associated with ads fueled by data profiles are injuries meriting a prohibition.

This prohibition could focus specifically on cross-context targeted advertising — that is, the targeting of ads based on a consumer’s activity across different websites, apps, and physical locations. Such “behavioral advertising” has been the bugbear of privacy advocates for

⁸⁹ Danielle Keats Citron, *A New Compact for Sexual Privacy*, 62 Wm. & Mary L. Rev. 1763 (2021), <https://scholarship.law.wm.edu/wmlr/vol62/iss6/2>; see also Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* (W.W. Norton, Penguin Vintage UK forthcoming 2022).

⁹⁰ *International coalition calls for action against surveillance-based advertising*, Norwegian Consumer Council (Jun. 22, 2021), <https://www.forbrukerradet.no/side/new-report-details-threats-to-consumers-from-surveillance-based-advertising/>.

⁹¹ Accountable Tech Rulemaking Petition, *supra* note 20.

years.⁹² Moreover, state level comprehensive privacy legislation — both enacted and proposed — has generally targeted cross-context ad targeting rather than first-party marketing.⁹³ However, many privacy groups have made more aggressive calls for regulation in recent years, arguing that a prohibition on targeting should extend to first-party data sets as well, pointing to large technology companies like Google and Facebook that have the ability to amass substantial personal data sets even without supplementing them with third-party data.⁹⁴

Under either approach, while the injuries alleged, for example, in the Accountable Tech petition are undoubtedly substantial, the FTC would need to demonstrate the extent to which of those injuries are attributable to targeted advertising. If that case is made, it would be difficult to argue that such injuries are readily avoidable by consumers — most Americans do not currently have the legal right to turn off ad targeting. Even when consumers do have the ability to opt out of targeting — either under state law or due to self-regulation — those tools turn out to be confusing, incomplete, and impractical for consumers to use at scale.⁹⁵ A Consumer Reports study on the efficacy of CCPA opt-out rights, for example, found that consumers tasked with opting out of data sales from just one data broker were often frustrated and unable to meaningfully limit sale or associated cross-context targeting.⁹⁶

As with the approach of broadly banning secondary use, opponents would likely argue that the economic benefits of ad targeting outweigh the injuries to consumers. However, the same counterarguments apply as well: that targeted advertising appears to be harmful to consumers, harmful to competition as the benefits flow primarily to large internet companies, and that free online content long predates the prevalence of targeted display ads.⁹⁷

⁹² Center for Democracy and Technology et al., *Re: In advance of the FTC Town Hall, “Behavioral Advertising: Tracking, Targeting, and Technology,” to be held November 1-2, 2007 in Washington, D.C.*, <https://cdt.org/wp-content/uploads/privacy/20071031consumerprotectionsbehavioral.pdf>.

⁹³ E.g., Cal. Civ. Code § 1798.100 et seq.; Washington SB 5062 (2021), Amendment by Committee on Civil Rights & Judiciary, <https://lawfilesexternal.wa.gov/biennium/2021-22/Pdf/Amendments/House/5062-S2%20AMH%20CRJ%20H1373.1.pdf>.

⁹⁴ It is worth noting, however, that these two companies are also the largest aggregators and users of third-party data. See, e.g., Justin Brookman et al., *Cross-Device Tracking: Measurement and Disclosures, Proceedings on Privacy Enhancing Technologies*, 2017 (2):133–148, <https://www.petsymposium.org/2017/papers/issue2/paper29-2017-2-source.pdf>; Steve Englehardt and Arvind Narayanan, *Online Tracking: A 1-million-site Measurement and Analysis*, https://www.cs.princeton.edu/~arvindn/publications/OpenWPM_1_million_site_tracking_measurement.pdf; Altaweel, Good, and Hoofnagle, *Web Privacy Census*, Technology Science (Dec. 14, 2015), <https://techscience.org/a/2015121502/>.

⁹⁵ Statement 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” at 3 (Apr. 24, 2013), <https://cdt.org/wp-content/uploads/pdfs/Brookman-DNT-Testimony.pdf>.

⁹⁶ *Consumer Reports Study Finds Significant Obstacles to Exercising California Privacy Rights*, Consumer Reports (Oct. 1, 2020), https://advocacy.consumerreports.org/press_release/consumer-reports-study-finds-significant-obstacles-to-exercising-california-privacy-rights/.

⁹⁷ *Id.*

C. Mandate compliance with opt-outs (including universal opt-out settings and databases)

Finally, the FTC might require companies to honor universal opt-out requests for secondary (non-necessary) processing. 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.⁹⁸ 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 opt-out 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), 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.

Under an opt-out model, companies should be legally obligated to honor browser privacy signals, such as Do Not Track or the Global Privacy Control as an opt out of secondary data uses, so that consumers can stop secondary processing of their personal information to every company with which their browser interacts in a single step. Otherwise, consumers would have to opt out individually at hundreds, if not thousands, of different websites, which is not practical. For unauthenticated data not associated with a specific person, platform-level controls are the most efficient manner to globally convey opt-out requests.

This is the approach taken in newly-adopted legislation in California and Colorado. For example, California law requires companies to honor browser privacy signals, as well as requests submitted by authorized agents, as a valid opt out of sale under the California Consumer Privacy Act. The California Attorney General's office recently updated their guidance to clarify that companies must honor the Global Privacy Control specifically — a CCPA-compliant browser signal that conveys a “Do Not Sell” command — as an opt out. Further, they have sent enforcement letters to companies that are not honoring GPC.⁹⁹ The California Privacy

⁹⁸ Cal. Civ. Code § 1798.100 et seq.; 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>.

⁹⁹ Kate Kaye, *California's Attorney General Backs Call for Global Privacy Control Adoption with Fresh Enforcement Letters to Companies*, Digiday (July 16, 2021), <https://digiday.com/marketing/californias->

Rights Act (Proposition 24) adds the requirement to honor browser privacy signals to the text of the statute.¹⁰⁰ The Colorado Privacy Act, which will go into effect in 2023, also requires companies to honor browser privacy controls as an opt out of processing for the purposes of sale and targeted advertising.¹⁰¹

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.¹⁰² 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.

Second, the FTC could create and house a Do Not Sell registry, modeled on the popular Do Not Call (DNC) registry, that businesses would be required to check before selling consumer data tied to those identifiers. The Commission would collect consumers' identifiers, such as emails and phone numbers, and companies would pay in order to consult the list (thus ensuring that companies seeking to sell data would absorb the costs for the operation of the website). Consumers could add their identifiers to the registry through a public portal, much like Do Not Call. This would enable consumers to easily and globally express their preferences to opt-out of the sale of data tied to specific identifiers (or hashes of specific identifiers). Companies would be required to check this database before disclosing or tracking based on consumers' information, much as they do today for the DNC registry. The DNC registry currently includes 244.3 million active registrations, indicating that this is an easy way for consumers to opt out of telemarketing messages.¹⁰³ On the other hand, compliance with Do Not Call has been inconsistent given the ease of creating difficult-to-trace voice-over-internet calls. One downside of a registry approach would be to make such identifiers publicly available to bad faith actors and more susceptible to spam. The rule would need to be paired with aggressive FTC enforcement as well as technical measures to remediate registry access and misuse.

Such a registry approach would work in tandem with Global Privacy Controls — a registry would only govern data sets tied to persistent real-world identifiers, but would also

attorney-general-backs-call-for-global-privacy-control-adoption-with-fresh-enforcement-letters-to-companies/.

¹⁰⁰ Cal. Civ. Code § 1798.135(e).

¹⁰¹ Colorado S. 21-190 (2021),

https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_rer.pdf.

¹⁰² Kaveh Waddell, *California's New Privacy Rights Are Tough To Use, Consumer Reports Study Finds* Consumer Reports (Mar. 16, 2021), <https://www.consumerreports.org/privacy/californias-new-privacy-rights-are-tough-to-use/>.

¹⁰³ *National Do Not Call Registry Data Book FY 2021*, Fed. Trade Comm'n at 5 (Nov. 2021), <https://www.ftc.gov/reports/national-do-not-call-registry-data-book-fiscal-year-2021>. The efficacy of the DNC registry is also limited by the fact that it only applies to telemarketing, and that it does not hinder scammers, debt collectors, and others in their communications.

govern offline data transactions. Global Privacy Controls would apply to data tied only to pseudonymous or short-term identifiers, but in many cases only apply to the platform that is sending the signals, such as a browser.¹⁰⁴ Senator Ron Wyden, in his privacy bill, the Mind Your Own Business Act, outlines a similar system to facilitate global opt outs through registries as well as persistent opt-out signals for both unauthenticated and authenticated data.¹⁰⁵

Mandating compliance with opt-out requests would rely upon similar theories of unfairness discussed in the previous two sections — that unwanted surveillance or specific prohibited practices lead to substantial injuries to consumers, that they are not reasonably avoidable, and they are not offset by countervailing benefits to consumers or competition.

By only prohibiting secondary processing upon the objection of a user, the FTC may be on even stronger ground, as in each case the consumer has evinced that they experience some loss of utility due to such processing. The FTC also has previous precedent for the proposition that evading platform-level privacy settings such as the Global Privacy Control is unfair and deceptive. For example, as noted above, the FTC’s recent Zoom settlement held that circumventing platform privacy protections is inherently harmful.¹⁰⁶

Finally, a Data Minimization Rule could rely on a combination of approaches (B) and (C) — that is, certain data practices could be prohibited as a matter of law, and users would have the ability to opt out of certain other secondary processing. Or the agency could require opt-in consent for certain secondary data processing, though as discussed earlier, privacy law should not encourage companies to bombard consumers with requests for secondary data collection and use. The FTC might decide there was a stronger case for banning certain practices by default, but certain others only with consent or when a consumer has affirmatively asserted an objection. Again, however, such an approach would minimize the inherent invasiveness of secondary data processing, and would potentially leave consumers exposed to unwanted and unnecessary data practices.

V. Other Privacy Protections That Should be Implemented Through Section 5 of the FTC Act

A. Primary Use Transparency

As opposed to secondary use, primary use is likely to be more intuitive and less objectionable to users. As such, it merits less strict regulation than secondary use. While some privacy models have argued that consumers should provide explicit consent even for primary use, such an approach has significant drawbacks.¹⁰⁷ As virtually every consumer interaction

¹⁰⁴ However, if a company receives a Global Privacy Control signal tied to data authenticated to a real-world identifier, it could be obligated to apply the user’s opt-out choice to data on other platforms.

¹⁰⁵ S. 1444, § 6 (2021), <https://www.congress.gov/bill/117th-congress/senate-bill/1444>.

¹⁰⁶ Compl., *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>.

¹⁰⁷ See, e.g., New York S. 6701 (2021), <https://www.nysenate.gov/legislation/bills/2021/s6701>.

involves some degree of data processing, consumers would be overwhelmed with privacy information and choices. This torrent of consent interfaces could make it difficult for consumers to distinguish between commonplace, expected data processing and requests to engage in processing for new, potentially unwanted, activities. Consumers would likely become enured to giving consent in order to go about their lives. The frequent use of dark patterns in opt-in interfaces, for example those used to comply with the GDPR, ePrivacy Directive, and CCPA, pose further challenges to obtaining meaningful consumer consent. It is possible — though certainly debatable — that these consent dialogs would give consumers more information and relatively empower them to make decisions in the marketplace, but the countervailing cost of subjecting consumers to dozens of privacy choices in a given day would likely offset any benefits.

However, a privacy rulemaking may still dictate some heightened degree of transparency around even primary use. If a certain activity involves processing especially sensitive data in potentially nonintuitive ways, a privacy rule could provide some obligation to ensure that consumers understand the consequences of the transaction they have initiated.¹⁰⁸ Such disclosures should be the exception and not the rule, however. This requirement could be justified under the FTC’s unfairness authority: failing to provide heightened disclosure around potentially and unexpected processing of certain data could easily lead to unexpected and unavoidable injuries for a consumer. An obligation to provide such heightened transparency has precedent in the Funeral Rule. The FTC clarified, under its Section 5 authority, that “it is an unfair or deceptive act or practice for a funeral provider to fail to furnish accurate price information disclosing the cost to the purchaser for each of the specific funeral goods and funeral services used in connection with the disposition of deceased human bodies...”¹⁰⁹ It requires funeral homes to provide clear, accurate information in an itemized list, to better enable consumers to compare offerings from multiple providers.¹¹⁰ Given the heightened sensitivity of the transactions and the vulnerability of the consumers involved, these labeling requirements are particularly appropriate.

Further, the FTC should establish some documentation requirements for all processing behaviors. Privacy policies should not be intended for consumers, who cannot reasonably be expected to read these complicated disclosures, but for intermediaries like ratings services, the press, academics, and regulators. Consumers dislike reading privacy policies,¹¹¹ but they serve a real purpose. Because there are no requirements for these disclosures, and because most FTC privacy cases are predicated upon a specific misstatement in a privacy policy or

¹⁰⁸ For example, the Colorado Privacy Act requires opt-in consent for the processing of a limited category of sensitive data, though that rule is not limited to scenarios where consumers would be likely to be surprised or offended by the data processing. Colorado S. 21-190 § 6-1-1308(7) (2021), https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_rer.pdf.

¹⁰⁹ 16 C.F.R. § 453.2.

¹¹⁰ Robert Benincasa, *You Could Pay Thousands Less For A Funeral Just By Crossing The Street*, NPR (Feb. 17, 2017), <https://www.npr.org/2017/02/07/504020003/a-funeral-may-cost-you-thousands-less-just-by-crossing-the-street>.

¹¹¹ Aleecia M. McDonald, Robert W. Reeder, Patrick Kelley, Lorrie Faith Cranor, *A Comparative Study of Online Privacy Policies and Formats* at 6, <https://www.robreeder.com/pubs/PETS2009.pdf>.

elsewhere, companies tend to make privacy policies as expansive as possible, so as to shield themselves from lawsuits and other enforcement actions.¹¹² To address this problem, privacy policies must provide reasonably detailed information about practices. These transparency requirements for primary use fall squarely within the FTC's authority to issue rules to prevent unfair practices, since they merely provide information to the marketplace, providing accountability for companies' practices; the FTC could consider instituting a size threshold for such privacy policy requirements to excuse small businesses who may not have the resources or sophistication to provide such documentation.

B. Civil Rights

Primary data processing should also be constrained to ensure that it is not discriminatory in nature.¹¹³ In recent years, it has become clear that the issues of privacy and civil rights are directly related. Companies have access to more and more data points about consumers and have a greater ability to provide differential experiences, offers, and advertisements to smaller and smaller segments of the population. Even if this segmentation is not explicitly based on protected characteristics such as race and gender identity, companies may (intentionally or inadvertently) use proxies for these factors that result in unfair treatment. Moreover, even when there is no intention to discriminate, black box algorithms can produce discriminatory results by replicating patterns of inequity that are already present in societal data inputs. This segmentation is often done through algorithms that are inherently difficult for external observers to test and hold accountable — especially when companies take affirmative measures to frustrate researchers testing for potential bias.¹¹⁴

Ad targeting based on this data can perpetuate historic patterns of discrimination and unequal outcomes among protected classes.¹¹⁵ For example, the Department of Housing and Urban Development has charged Facebook for targeting housing advertisements based on protected categories like race and religion.¹¹⁶ These targeting systems have been used to

¹¹² *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, Fed. Trade Comm'n, at 61 (2012),

<https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

¹¹³ See, e.g., Gaurav Laroia, David Brody, *Privacy Rights Are Civil Rights. We Need to Protect Them* (Mar. 14, 2019), <https://www.freepress.net/our-response/expert-analysis/insights-opinions/privacy-rights-are-civil-rights-we-need-protect-them>; *The Online Civil Rights and Privacy Act of 2019*, Free Press Action and the Lawyers' Committee for Civil Rights Under Law, Section 3(a) (Mar. 11, 2019), https://www.freepress.net/sites/default/files/2019-03/online_civil_rights_and_privacy_act_of_2019.pdf.

¹¹⁴ See, e.g., Letter from Acting Director of the Bureau of Consumer Protection Samuel Levine to Facebook (Aug. 5, 2021), <https://www.ftc.gov/news-events/blogs/consumer-blog/2021/08/letter-acting-director-bureau-consumer-protection-samuel>.

¹¹⁵ See *Letter from Lawyers' Committee for Civil Rights Under the Law et al. to Chair Lina Khan and Commissioners Chopra, Slaughter, Phillips, and Wilson*, Fed. Trade Comm'n (Aug. 4, 2021), <https://www.lawyerscommittee.org/wp-content/uploads/2021/08/FTC-civil-rights-and-privacy-letter-Final-1.pdf>.

¹¹⁶ *Sec'y of Hous. & Urban Dev. v. Facebook, Inc.*, No 01-18-0323-8, 1, Charge of Discrimination, FHEO No. 01- 18-0323-8 (Mar. 28, 2019), https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf.

interfere with elections and fuel voter suppression efforts and to carry out disinformation campaigns that undermine public trust.¹¹⁷ Further, some data brokers provide this information to employers, landlords, and others, while evading the Fair Credit Reporting Act, giving consumers next to no control over these uses.¹¹⁸ The increasing use of automated decision-making can further exacerbate these problems, as opaque algorithms, often trained on historical data, can perpetuate existing inequalities.¹¹⁹

As part of a set of privacy protections, the FTC should formalize a rule stating that companies are prohibited from discriminating against protected classes in the offering of economic opportunities or online public accommodations.¹²⁰ This prohibition on discrimination should apply to both intentional discrimination and practices that produce a discriminatory disparate impact. Such a rule should include a typical disparate impact analysis,¹²¹ which involves (1) the demonstration of a disparate impact on the basis of a protected characteristic, (2) an opportunity for a respondent to articulate a substantial, legitimate, and nondiscriminatory purpose for the practice, and (3) if there is a legitimate purpose, a showing that a less discriminatory alternative is available or that the purpose is pretextual. This disparate impact standard is well established in case law and is well understood by businesses — for example, all businesses must already comply with this standard in their employment practices, pursuant to Title VII of the Civil Rights Act of 1964.¹²²

Such a rule is straightforward to justify under the FTC’s unfairness authority. Practices that have an otherwise unjustified disparate impact on protected classes’ access to economic opportunities or public accommodations are undoubtedly harmful.¹²³ The FTC has found that injuries that fall specifically or disproportionately on disadvantaged classes are covered by Section 5, such as its recent settlement with Bronx Honda over charging higher prices to Black

¹¹⁷ *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, Fed. Trade Comm’n (July 24, 2019), <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>.

¹¹⁸ *Spokeo to Pay \$800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA*, Fed. Trade Comm’n (June 12, 2012), <https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed>; *Big Data, A Big Disappointment for Scoring Consumer Credit Risk*, Nat’l Consumer Law Ctr. at 26 (Mar. 2014), <https://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf>.

¹¹⁹ See Erin Simpson & Adam Conner, *How to Regulate Tech: A Technology Policy Framework for Online Services*, Ctr. for Am. Progress (Nov. 16, 2021) (discussing the extensive literature on civil rights harms caused by automated decision-making systems, biometric surveillance, amplification of civil-rights suppressing content, and reification of prejudice), <https://www.americanprogress.org/article/how-to-regulate-tech-a-technology-policy-framework-for-online-services/>.

¹²⁰ Kristen Clarke and David Brody, *It’s time for an online Civil Rights Act*, The Hill (Aug. 3, 2018), <https://thehill.com/opinion/civil-rights/400310-its-time-for-an-online-civil-rights-act>.

¹²¹ See Title VI Legal Manual, Dep’t of Justice (Apr. 22, 2021) at Section VII, <https://www.justice.gov/crt/book/file/1364106/download>.

¹²² 42 U.S.C. § 2000e, *et seq.*

¹²³ Elisa Jillson, *Aiming for truth, fairness, and equity in your company’s use of AI*, Fed. Trade Comm’n (Apr. 19, 2021), <https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai> (“[R]esearch has highlighted how apparently ‘neutral’ technology can produce troubling outcomes – including discrimination by race or other legally protected classes... [H]ow can we harness the benefits of AI without inadvertently introducing bias or other unfair outcomes?”).

and Latino customers.¹²⁴ It is difficult to imagine how such discrimination would be avoidable by consumers, particularly when the source of such discrimination is a black box algorithm or other data practice that lacks transparency. Unfairness's third prong should be satisfied by the disparate impact test, which evaluates whether a discriminatory behavior can be justified by a substantial, legitimate, and nondiscriminatory purpose, as well as whether such purpose can be achieved by less harmful alternatives.

C. Nondiscrimination

Privacy regulation should also 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. Such practices sometimes occur under the guise of loyalty programs¹²⁵ — in 2013, for example, CVS asked consumers to waive their HIPAA rights in return for participation in the ExtraCare rewards program.¹²⁶

Instead, privacy should be recognized as an inalienable and fundamental right, not merely an asset to be bartered away. Further, 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.)

Particularly where consumers have few choices, market forces fail to impose sufficient constraints on companies from penalizing exercising privacy rights. Low-income consumers may feel coerced into granting unfettered access to and use of their personal information for targeting or other purposes. For example, from 2013 to 2016, AT&T charged users who did not agree to the use of their internet data for ad targeting around \$30 per month — a significant portion of the monthly charge for internet service.¹²⁷

¹²⁴ Compl. for Permanent Injunction and other Equitable Relief, Fed. Trade Comm'n, v. Liberty Chevrolet, Inc., No. 20-CV-3954 (May 27, 2020), https://www.ftc.gov/system/files/documents/cases/bronx_honda_complaint_0.pdf; Statement of Commissioner Rohit Chopra In the Matter of Liberty Chevrolet, Inc., Comm'n File No. 1623238 (May 27, 2020), https://www.ftc.gov/system/files/documents/public_statements/1576002/bronx_honda_final_rchopra_bronx_honda_statement.pdf.

¹²⁵ Chloe Liu, *CVS, Walgreens, and Rite Aid Loyalty Programs Compared: How to Get the Best Deals (Without the Mile-Long Receipts)*, N.Y. Times Wirecutter (May 24, 2021), <https://www.nytimes.com/wirecutter/money/drugstore-loyalty-programs/>.

¹²⁶ David Lazarus, *CVS thinks \$50 is enough reward for giving up healthcare privacy*, L.A. Times (Aug. 15, 2013), <https://www.latimes.com/business/la-xpm-2013-aug-15-la-fi-lazarus-20130816-story.html>.

¹²⁷ Jon Brodtkin, *AT&T to end targeted ads program, give all users lowest available price*, ArsTechnica (Sept. 30, 2016), <https://arstechnica.com/information-technology/2016/09/att-to-end-targeted-ads-program-give-all-users-lowest-available-price/>.

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.¹²⁸

Some state privacy measures already put limits on the most exploitative practices, but still have loopholes that could permit inappropriate charges for exercising privacy rights. The CCPA includes language prohibiting discrimination “against a consumer because the consumer exercised any of the consumer’s rights under this title[.]” including by denying goods or services, or charging a different price or providing a different level or quality of goods or services for doing so.¹²⁹ However, confusingly, it notes that a company may do so if it is “is reasonably related to the value provided to the business by the consumer’s data[.]”¹³⁰ and if such incentives programs are not unfair or usurious. CPRA adds to the measure a clarification that loyalty programs are permitted under the CCPA.¹³¹ Virginia¹³² and Colorado¹³³ have similar language prohibiting non-discrimination but allowing certain incentives programs. (In contrast, pending privacy legislation in Washington State includes consensus language that prohibits the disclosure of personal information to third parties pursuant to loyalty programs).¹³⁴

D. Data security

The accumulation of consumer data — from the consumer directly, scraped from public sources, and purchased from data brokers — creates serious security risks.¹³⁵ Data collection, retention, and inadequate internal controls also leave users vulnerable to employees who abuse their power. Uber, Facebook, and NSA employees have used location data in order to stalk the objects of their romantic interest.¹³⁶ The Federal Trade Commission arguably has the strongest

¹²⁸ See, e.g., Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 Columbia L. Rev. 6 (Oct. 2017), <https://ssrn.com/abstract=3058835>; See also Accountable Tech Rulemaking Petition, *supra* note 20 at 25-35, on the harms associated with unrestricted data collection, use, and sharing.

¹²⁹ Cal. Civ. Code § 1798.125(a)(1).

¹³⁰ *Id.* at § 1798.125(a)(2).

¹³¹ Cal. Civ. Code § 1798.125(a)(3).

¹³² VA SB 1392 § 59.1-574(A)(4) (2021), <https://lis.virginia.gov/cgi-bin/legp604.exe?211+ful+SB1392ES1+pdf>.

¹³³ CO S. 21-190 § 6-1-1308(1)(c)-(d), https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf.

¹³⁴ WA SB 5062 (2021).

¹³⁵ Brookman and Hans, *supra* note 8.

¹³⁶ Alex Hern, *Uber Employees ‘Spied on Ex-Partners, Politicians and Beyonce,’* The Guardian (Dec. 13, 2016), <https://www.theguardian.com/technology/2016/dec/13/uber-employees-spying-ex-partners-politicians-beyonce>; Siobahn Gorman, *NSA Officers Spy On Love Interests*, Wall St. J. (Aug. 23, 2013), <https://www.wsj.com/articles/BL-WB-40005>; Karen Hao, *Review: Why Facebook Can Never Fix Itself*, MIT Technology Review (Jul. 21, 2021), <https://www.technologyreview.com/2021/07/21/1029818/facebook-ugly-truth-frenkel-kang-nyt/>.

grounds in implementing *security obligations* as part of a privacy rule. Since 2005,¹³⁷ the Commission has brought 80 cases alleging that companies' failure to use reasonable security measures to safeguard data constitutes unfair business practice.¹³⁸ As the FTC has alleged in cases against InfoTrax¹³⁹ and SkyMed,¹⁴⁰ retention of the data puts users at risk for data breach, is largely unavoidable by consumers as the data resides on a company's servers, often unbeknownst to them, and is not offset by countervailing benefits if the data deletion processes are reasonably cost effective.

Clearly, breaches are particularly harmful with respect to sensitive data, but there should be protections over less sensitive data too. For example, a security glitch exposed users' private tweets for more than four years; though that would not count as personal information under many state data security and data breach notification laws, inadvertent disclosure could have significant reputational damage to consumers.¹⁴¹ Indeed, the FTC has a stronger need to mandate data security as consumers may find it difficult to plead Article III standing for security violations where the harms are unknown or difficult to articulate.¹⁴² The scope of the FTC's authority to articulate and pursue bad security practices is not so constrained.

The second two parts of the unfairness test are easily met. Security breaches are certainly unavoidable from the consumer perspective — the company's own practices are responsible for such breaches. Not only are companies better positioned than consumers to engineer security solutions, but in the case of data brokers and credit bureaus (such as Equifax), consumers do not have a choice as to whether their information is collected. In the case of certain internet-connected devices, consumers could use resources such as Consumer Reports to choose more secure products, but nevertheless, there are significant information asymmetries that prevent consumers from consistently and effectively making choices to protect their data.

The FTC's reasonableness standard addresses the third element of the unfairness test — companies need not take unduly burdensome measures, the costs of which outweigh any likely benefits to consumers. Indeed, the standard is flexible enough so that any measures taken are appropriate to the company's unique circumstances. As Andrea Arias of the FTC

¹³⁷ *BJ's Wholesale Club Settles FTC Charges: Agency Says Lax Security Compromised Thousands of Credit and Debit Cards*, Fed. Trade Comm'n (Jun. 16, 2005), <https://www.ftc.gov/news-events/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges>; *DSW Inc. Settles FTC Charges: Agency Says Company Failed to Protect Sensitive Customer Data*, Fed. Trade Comm'n (December 1, 2005), <https://www.ftc.gov/news-events/press-releases/2005/12/dsw-inc-settles-ftc-charges>.

¹³⁸ *Federal Trade Commission 2020 Privacy and Data Security Update*, Fed. Trade Comm'n at 3 (2021), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-2020-privacy-data-security-update/20210524_privacy_and_data_security_annual_update.pdf.

¹³⁹ Compl., *FTC v. Infotrax Systems L.C.*, at ¶ 10 (Jan. 6, 2020), https://www.ftc.gov/system/files/documents/cases/162_3130_infotrax_complaint_clean.pdf.

¹⁴⁰ Compl., *FTC v. SkyMed International, Inc.*, at ¶ 12(e) (Dec. 16, 2020), https://www.ftc.gov/system/files/documents/cases/skymed_-_complaint.pdf.

¹⁴¹ Sam Schechner, *Twitter Data Case Sparks Dispute, Delay Among EU Privacy Regulators*, Wall St. J (Aug. 20, 2020), https://www.wsj.com/articles/twitter-data-case-sparks-dispute-delay-among-eu-privacy-regulators-11597921201?mod=article_inline.

¹⁴² See, e.g., *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021).

pointed out, “[T]he touchstone of the FTC’s approach to data security has been reasonableness—that is, a company’s data security measures must be reasonable in light of the volume and sensitivity of information the company holds, the size and complexity of the company’s operations, the cost of the tools that are available to address vulnerabilities, and other factors. Moreover, the FTC’s cases focus on whether the company has undertaken a reasonable process to secure data.”¹⁴³ For example, in its 2020 Privacy & Data Security Update, the FTC explained that in each of their data security cases from that year, the Commission directed the company to “implement a comprehensive security program, obtain robust biennial assessments of the program, and submit annual certifications by a senior officer about the company’s compliance with the order.”¹⁴⁴ Such requirements should be the baseline for any company collecting consumers’ data, given the widespread incidence of data breaches.

Arguably the most difficult question on data security rules is how prescriptive to make them. In our view, a data security rule should have a comprehensive definition of personal information that includes online accounts and biometric data; require companies to implement, maintain, and keep up-to-date reasonable security protections and a reasonable security program appropriate to the nature of the information, to protect the information (and any such device) from unauthorized access, destruction, use, modification, or disclosure, with administrative, physical, and technical safeguards; and retention limits. The goal should be to provide companies with adequate direction without being so prescriptive that it is overly burdensome and outdated within a few years.

Some security provisions within privacy legislation are barely one line long, essentially restating the FTC’s *de facto* reasonableness standard.¹⁴⁵ The advantage of such a standard is flexibility over time and lack of burden on the FTC to revise guidance in light of changing technology. On the other hand, especially in light of the Equifax data breach, policymakers have sought to provide companies with more specific guidance as to what constitutes reasonable security. For example, the New York Department of Financial Services (NYDFS) recently adopted stringent data security requirements for financial institutions, including annual penetration testing and bi-annual vulnerability assessments, limits on access privileges, and a requirement to designate a chief information security officer who is responsible for the company’s security program.¹⁴⁶ The FTC has recently updated its Safeguards Rule with more specific security requirements, consistent with the NYDFS regulation, including placing limits on

¹⁴³ Andrea Arias, *The NIST Cybersecurity Framework and the FTC*, Fed. Trade Comm’n Business Blog (Aug. 31, 2016), <https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc>.

¹⁴⁴ *Federal Trade Commission 2020 Privacy and Data Security Update*, Fed. Trade Comm’n at 3-4 (2021), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-2020-privacy-data-security-update/20210524_privacy_and_data_security_annual_update.pdf.

¹⁴⁵ VA SB 1392 § 59.1-574(A)(3) (2021), <https://lis.virginia.gov/cgi-bin/legp604.exe?211+ful+SB1392ES1+pdf>.

¹⁴⁶ 23 CRR-NY § 500.0 et seq., <https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I5be30d2007f811e79d43a037eefd0011>.

internal access to data, new encryption requirements, and a requirement to establish a chief security officer.¹⁴⁷

E. Access, portability, correction, and deletion

Privacy frameworks often include provisions giving consumers the right to access, delete, and correct data related to them in the possession of companies. Access rights give accountability and transparency into corporate practices, while correction and deletion rights give consumers some degree of control over data held by companies. Access, correction, and deletion rights have been a core element of European privacy law dating back to the Data Protection Directive, and have been reinforced by the enactment of the Global Data Protection Regulation. Recently enacted state statutes — the CCPA, VCDPA, and CPA — all include access and deletion provisions, and upon adoption of new California provisions under Proposition 24, all will provide a right of correction. (Privacy legislation adopted in Nevada did not include any of these elements — only a weak opt out of data sales.)¹⁴⁸

To justify mandating data access under its unfairness authority, the FTC could make the plausible case that not knowing what data companies have about them puts consumers at risk of data exposure, and prevents them from making informed choices among market participants. As discussed above, collection and retention of consumer data leaves consumers vulnerable to data breaches and misuse of information by employees, who can use their privileged access to sensitive information to manipulate users.¹⁴⁹ Providing access to that data gives consumers more control over such data — depending on what the consumer finds, they might want to delete, correct, or request to opt out; move their business elsewhere; or potentially report concerns to regulators. Without these access rights, consumers are unable to effectively make decisions about their data in the marketplace.

Existing state privacy laws also typically nod to data portability in their access provisions. For example, the CCPA requires businesses to provide electronic data “in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance.”¹⁵⁰ Such provisions are important in giving consumers further control over their data, and greater ability to make choices in the marketplace over their preferred platforms. If the FTC can make a case that access rights forestall injuries stemming from not knowing where data about them is stored, it can also make the case that such data needs to be provided in a commonly-used and accessible format.

The other elements of unfairness are easier to demonstrate for mandating access rights: any injury resulting from not knowing what data is stored about them is certainly unavoidable by

¹⁴⁷ *FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches*, Fed. Trade Comm’n (Oct. 27, 2021), <https://www.ftc.gov/news-events/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial>.

¹⁴⁸ NRS 603A.345, <https://www.leg.state.nv.us/nrs/nrs-603a.html>.

¹⁴⁹ Adrian Chen, *GCreep: Google Engineer Stalked Teens, Spied on Chats*, Gawker (Sept. 14, 2010) <http://gawker.com/5637234/gcreep-googleengineer-stalked-teens-spied-on-chats>.

¹⁵⁰ Cal. Civ. Code § 1798.100(d).

consumers, as consumers are otherwise ignorant or potential risk and not empowered to take action. As for countervailing benefits, there are costs associated with providing data access, though those costs are incrementally less for each additional data subject making a request. There also may be costs associated with providing access to derived inferences as well — in that they may cast insight on proprietary algorithms that could be co-opted by others — however, those costs likely do not outweigh the significant value in giving consumers transparency into how companies are classifying and targeting them, especially if such ad targeting implicates job or housing opportunities.

Most of the harms covered by the rules proposed by this paper should not face significant challenge on the premise that the harms are not “prevalent” (as is required by Section 18). In response to privacy law in Europe and states like California, companies have had to develop systems to comply with data access requests. If as a matter of course most companies offer access to those same systems to residents of other states, then a case could be made that deprivation of data access is not, in fact, prevalent. The FTC could conduct an informal inquiry into this empirical question prior to initiating the rulemaking process.

In some cases, the case for correction may be more difficult than the case for access or deletion where there are no clear consequences related to the incorrect information. Receiving untargeted marketing does not seem like a compelling injury. If the data is internal, there are no clear reputational losses, though the data could still potentially embarrass someone if it were later breached or disclosed. FCRA grants correction rights for data that could impact credit and employment,¹⁵¹ and it would be appropriate to extend correction rights, at the very least, to all scenarios where the data could lead to significant legal effects. The Supreme Court adopted a skeptical view of the harms associated with inaccurate data in cases such as *Spokeo*¹⁵² and *Transunion*,¹⁵³ though the test for Article III standing is different from the test for unfairness, and the fact patterns in both those cases were somewhat idiosyncratic.

Finally, the FTC would have a strong case to mandate deletion rights for non-necessary data sets as part of an unfairness privacy rulemaking. As discussed *supra*, getting rid of old data that serves no useful purpose should be properly considered as part of a company’s data security obligations.¹⁵⁴ For other data that still retains some potential benefit, consumers still are at risk to data exposure or misuse so long as it remains saved. If a user wishes to delete information associated with their account or profile, in many cases it will be difficult to make the argument that there is a countervailing benefit associated with retaining the data against her wishes. Certainly some data should be exempted from deletion rights as is the case under CCPA and other privacy laws — consumers for example are not entitled to delete the fact that

¹⁵¹ 15 U.S.C. § 1681i.

¹⁵² *Spokeo, Inc. v. Robins*, 578 U.S. 330 (2016).

¹⁵³ *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021).

¹⁵⁴ Compl., *FTC v. SkyMed International, Inc.*, No. 1923140 at ¶ 12(e) (Dec. 16, 2020), https://www.ftc.gov/system/files/documents/cases/skymed_-_complaint.pdf.

they owe a merchant.¹⁵⁵ But for many if not most data sets, the FTC can reasonably argue that failure to respond to deletion requests constitutes an unfair business practice.

F. Prohibition on the use of dark patterns

Finally, any privacy rulemaking could be accompanied by regulations specifically prohibiting the use of “dark patterns” to subvert consumer choice and autonomy. In response to GDPR and the ePrivacy Directive, many companies have resorted to cookie consent interfaces that strongly steer users to granting blanket consent to tracking and that make turning off certain tracking considerably more difficult. While the approaches outlined in this paper are designed to minimize the role of consent and user choice, there is no way to wholly remove individual autonomy from any privacy framework — not should there be. If secondary uses are prohibited, a company may make a pitch for using data for a different primary purpose. If a user globally opts out, a company may be able to ask for an exception. Guardrails must be implemented to ensure that such prompts do not overwhelm or confuse users as an end run around the protections of a Data Minimization Rule.

There is increased precedent on the state level for prohibitions on the use of dark patterns — a prohibition in the CCPA regulations on the use of dark patterns in opt outs;¹⁵⁶ a prohibition in CCPA as amended by Proposition 24, on the use of dark patterns in obtaining consent to opt back into the disclosure of their information,¹⁵⁷ in the Colorado Privacy Act,¹⁵⁸ and in California’s new Genetic Information Privacy Act.¹⁵⁹ The measures use similar language, prohibiting interfaces or processes designed with the substantial effect of subverting or impairing user choice. While this is an important first step, to be effective a rulemaking would likely need to be more prescriptive, specifying how privacy disclosures and user interfaces should look. There may be some cost to innovation, but standardization and narrower options would better serve consumers in the long run.

VI. Judicial Review of FTC Unfairness Rules

Federal Trade Commission unfair trade practice rules promulgated under Section 5 of the FTC Act are subject to judicial review in the D.C. Circuit.¹⁶⁰ The Magnuson-Moss Act empowers the FTC to enforce its trade regulation rules.¹⁶¹ The Mag-Moss rulemaking process contains procedural requirements that are greater than the notice-and-comment requirements of

¹⁵⁵ See, for example, significant exemptions in the CCPA’s right to delete, including to “Otherwise use the consumer’s personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information” Cal. Civ. Code §1798.105(d)(9).

¹⁵⁶ Cal. Code Regs tit. 11 § 999.315(h).

¹⁵⁷ Cal. Civ. Code §1798.140(h).

¹⁵⁸ CO S. 21-190 (2021) § 6-1-1303(5)(c), https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_rer.pdf.

¹⁵⁹ CA SB 41 (2021) § 2(b)(6), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202120220SB41.

¹⁶⁰ 15 U.S.C. § 57a(e); See *generally Am. Fin. Servs. Ass’n v. F.T.C.*, 767 F.2d 957 (D.C. Cir. 1985).

¹⁶¹ 15 U.S.C. § 57b(a)(1).

the Administrative Procedure Act (“APA”).¹⁶² First, the agency must publish an advanced notice of proposed rulemaking describing the topic area for rulemaking, Commission objectives, and regulatory options.¹⁶³ The public is then invited to comment on the initial notice.¹⁶⁴ If the FTC finds that the unfair and deceptive practices covered by the proposed rulemaking are “prevalent,” it then submits notice to Congress¹⁶⁵ and then must publish a more detailed notice of proposed rulemaking “stating with particularity the text of the proposed rule, including any alternatives.”¹⁶⁶ Then, the agency must “conduct an informal hearing at which any interested person can present his position orally or by documentary submission or both, subject to such Commission rules as may tend to avoid unnecessary costs and delay.”¹⁶⁷ If the FTC decides that it “must resolve disputed issues of material fact necessary to fair decisionmaking on the record as a whole,” Section 18 “entitles interested persons to offer such rebuttal submissions or to conduct (or to have the Commission conduct) such cross-examination of witnesses as the Commission deems appropriate and necessary for a full and true disclosure of facts pertinent to the disputed issues.”¹⁶⁸ Finally, the FTC publishes the final rule, along with a statement justifying the rule along with an economic analysis of its effects.¹⁶⁹

In reviewing a trade regulation rule promulgated by the FTC, an appellate court’s role is to “determine if the Commission’s finding is supported by substantial evidence on the record as a whole[.]” and not “to reweigh the evidence de novo to determine how we would have resolved the matter.”¹⁷⁰ There will likely not be a successful challenge to the proposed rule on the grounds of an insufficient rulemaking process, such as the FTC blocking the introduction of evidence because the extensive rulemaking process will provide the FTC with substantial evidence and provide interested parties the opportunity to submit input.

A. Deference to Agency Interpretations

A party can challenge an FTC-promulgated rule under Mag-Moss or the APA.¹⁷¹ A court may set aside a Mag-Moss rule if it “finds that the Commission’s action is not supported by substantial evidence in the rulemaking record” or if the court finds that the FTC “precluded disclosure of disputed material facts which was necessary for fair determination by the Commission of the rulemaking proceeding taken as a whole” by refusing or limiting the petitioner’s cross-examination or rebuttal submissions.¹⁷² The rulemaking record requires “the rule, its statement of basis and purpose, the transcript required by subsection (c)(5), any written submissions, and any other information which the Commission considers relevant to such

¹⁶² 5 U.S.C §§ 556–57.

¹⁶³ 15 U.S.C. § 57a(b)(2)(A)(1).

¹⁶⁴ 15 U.S.C. § 57a(b)(2)(A)(2).

¹⁶⁵ 15 U.S.C. § 57a(b)(2)(C).

¹⁶⁶ 15 U.S.C. § 57a(b)(1).

¹⁶⁷ *Ass’n of Nat. Advertisers, Inc. v. F.T.C.*, 617 F.2d 611, 614 (D.C. Cir. 1979) (citing 15 U.S.C. § 57a(c)).

¹⁶⁸ *Id.* at 614–15 (citing 15 U.S.C. § 57a(c)).

¹⁶⁹ 15 U.S.C. § 57a(d)(1).

¹⁷⁰ *Thompson Med. Co. v. F.T.C.*, 791 F.2d 189, 196 (D.C. Cir. 1986).

¹⁷¹ See 15 U.S.C. § 57a(e)(3); see also 5 U.S.C. § 706(2).

¹⁷² 15 U.S.C. § 57a(e)(3)(A).

rule.”¹⁷³ Any privacy rule promulgated and challenged under Mag-Moss will thus survive judicial scrutiny so long as the FTC’s rulemaking record supports the FTC’s determinations and the FTC provides sufficient cross-examination and rebuttal submission opportunities.

“Judicial review of an administrative agency’s decision is authorized by the APA.”¹⁷⁴ The APA provides that a court “may only set aside agency action that is ‘arbitrary, capricious, an abuse of discretion or otherwise not in accordance with law.’”¹⁷⁵ The D.C. Circuit has discussed the arbitrary and capricious standard, opining that the “arbitrary and capricious review requires us to consider whether the FTC action is supported by reasoned decisionmaking,”¹⁷⁶ “whether the agency ‘relied on factors which Congress [did] not intend[] it to consider,’”¹⁷⁷ and “whether the Rule was promulgated in ‘observance of procedure required by law[.]’”¹⁷⁸ The FTC has satisfied the arbitrary and capricious standard when its decision is based “upon consideration of the relevant factors” and is “adequately explained in the administrative record to allow judicial review.”¹⁷⁹ Under the FTC’s rulemaking procedure, the proposed trade regulation rule would have to be supported by reasoned decisionmaking demonstrated in the formal rulemaking process as is required by the APA, and the FTC would articulate a connection between facts and conclusions. The proposed rule would rely on the FTC’s mandate to protect consumers from injuries under §45(n) and could not rely on factors that Congress did not intend for it to consider. The proposed Data Minimization Rule would not be considered arbitrary or capricious because it would be based in reason and supported by evidence provided in the notice and comments period of the rulemaking process.

When an agency interprets an ambiguous statute, their interpretation will be given deference unless it is impermissible. In *New York State Bar Association v. Federal Trade Commission*, the D.C. District Court stated, “A challenge to an agency’s interpretation of a statute that it administers is subject to deferential review under *Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837, 104 S.Ct. 2778, 81 L.Ed.2d 694 (1984)[.]”¹⁸⁰ The *Chevron* test is applicable to APA challenges under 5 U.S.C. § 706(2)(C).¹⁸¹ “Under the well known *Chevron* test... the Court must first examine ‘whether Congress has directly spoken to the precise question at issue.’”¹⁸² Further, the Court notes, “It is fair to assume generally that Congress contemplates administrative action with the effect of law when it provides for a relatively formal administrative procedure tending to foster the fairness and deliberation that

¹⁷³ 15 U.S.C. § 57a(e)(1)(B).

¹⁷⁴ *Mueller v. England*, 404 F. Supp. 2d 51, 55 (D.D.C. 2005) (citing 5 U.S.C. §§ 701–706).

¹⁷⁵ *Id.* (citing 5 U.S.C. § 706(2)(A)).

¹⁷⁶ *Pharm. Rsch. & Mfrs. of Am. v. F.T.C.*, 790 F.3d 198, 204 (D.C. Cir. 2015) (citing *Allentown Mack Sales & Serv., Inc. v. NLRB*, 522 U.S. 359, 374, 118 S.Ct. 818, 139 L.Ed.2d 797 (1998)).

¹⁷⁷ *Id.* (quoting *Motor Vehicle Mfrs. Ass’n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983)).

¹⁷⁸ *Id.* (quoting 5 U.S.C. § 706(2)(D)).

¹⁷⁹ *Dr. Pepper/Seven-Up Companies, Inc. v. F.T.C.*, 991 F.2d 859, 864 (D.C. Cir. 1993).

¹⁸⁰ *New York State Bar Ass’n v. F.T.C.*, 276 F. Supp. 2d 110, 115 (D.D.C. 2003).

¹⁸¹ *Id.* at 117.

¹⁸² *Id.* (quoting *Chevron, U.S.A., Inc. v. Nat. Res. Def. Council, Inc.*, 467 U.S. 837, 842-43 (1984)).

should underlie a pronouncement of such force.”¹⁸³ Next, if the statute is ambiguous or silent with respect to a particular provision, “the question for the court is whether the agency’s answer is based on a permissible construction of the statute.”¹⁸⁴ The FTC’s rulemaking process, which includes notice and comment opportunities, provides a formal administrative procedure. A trade rule regulation promulgated by the FTC under 5 U.S.C. § 45 authority will therefore be granted *Chevron* deference by courts if there is an ambiguity under 5 U.S.C. § 45. With respect to § 45, “substantial injury,” “reasonably avoidable,” and “countervailing benefits to consumers or competition” may be ambiguous as applied to online behavioral advertising.

The flexible standard of the FTC’s unfairness authority will allow the FTC to promulgate privacy rules because courts will give substantial deference to the FTC’s factual conclusions and legal interpretations. A legal challenge to an unfairness rule promulgated by the FTC will focus on the three-part test in the statute. As stated previously, an act or practice is unfair when it “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.”¹⁸⁵ As detailed earlier, privacy harms are substantial injuries and the FTC should use its authorities to address these harms under its unfairness authority. The unfairness standard is not rigid and Congress envisioned that the FTC would “develop[] and refin[e] its unfair practice criteria on a progressive, incremental basis.”¹⁸⁶ This standard, coupled with the procedural requirements of the Mag-Moss rulemaking process, show that so long as the FTC determines that the online surveillance of internet users is a substantial injury that consumers cannot reasonably avoid without countervailing benefits to consumers or competition, and follows the procedural requirements of the Mag-Moss rulemaking process, the rule will withstand a judicial challenge. There is no question that Congress has clearly delegated rulemaking authority to the FTC that encompasses broad scale commercial regulations with vast economic and political significance¹⁸⁷ and that the FTC has exercised those powers effectively over more than one hundred years.

B. Privacy Rules Can Be Crafted to Withstand First Amendment Scrutiny

Agency actions that restrict or penalize speech are potentially subject to challenge under the First Amendment.¹⁸⁸ The level of scrutiny applied to a law or regulation subject to a First Amendment challenge depends on the type of activity restricted and the impact of the restriction on protected speech. For example, restrictions that only have “indirect impacts on speech” are

¹⁸³ *United States v. Mead Corp.*, 533 U.S. 218, 230, (2001) (“Cf. *Smiley v. Citibank (South Dakota), N. A.*, 517 U.S. 735, 741, (1996) (APA notice and comment ‘designed to assure due deliberation’)).

¹⁸⁴ *Chevron, U.S.A., Inc. v. Nat. Res. Def. Council, Inc.*, 467 U.S. 837, 843 (1984).

¹⁸⁵ 15 U.S.C. § 45(n).

¹⁸⁶ *Am. Fin. Servs. Ass’n v. F.T.C.*, 767 F.2d 957, 978 (D.C. Cir. 1985).

¹⁸⁷ The Supreme Court has recently raised questions about whether such “major questions” can be addressed through administrative rulemaking absent a clear statement from Congress. See *Alabama Ass’n of Realtors v. HHS*, 594 U.S. ___, ___, (slip op. at 6), 141 S. Ct. 2485, 2489 (2021). But here the FTC’s authority to promulgate unfair trade practices rules was expressly endorsed by Congress when the unfairness policy statement was codified in the Federal Trade Commission Act Amendments of 1994, Pub. L. 103-312, 108 Stat. 1691, 1695 (1994) (codified at 15 U.S.C. § 45(n)).

¹⁸⁸ *Matal v. Tam*, 137 S. Ct. 1744, 1763–64 (2017).

subject to rational basis review.¹⁸⁹ Even regulations that directly restrict commercial speech are only subject to “relaxed” or “intermediate scrutiny” under *Central Hudson*,¹⁹⁰ which provides that the speech must “at least concern lawful activity and not be misleading; the government interest [must be] substantial; the regulation must directly advance the governmental interest asserted, and the regulation must not be more extensive than is necessary to serve the interest.”¹⁹¹

Courts have held that the government’s interest in protecting privacy is substantial.¹⁹² Courts have repeatedly upheld statutes and regulations that aim to protect informational privacy interests.¹⁹³ Indeed, courts have rejected challenges to the Fair Credit Reporting Act and Gramm-Leach-Bliley Act privacy requirements on the grounds that businesses seeking to sell “information about individual consumers and their credit performance” are given “reduced constitutional [speech] protection” under the private commercial speech doctrine.¹⁹⁴ The D.C. Circuit has also upheld the application of opt-in rules to limit downstream uses of personal information.¹⁹⁵ When considering whether the restriction is “no more broad or no more expansive than necessary to serve [the government’s] substantial interests,” the “only condition is that the regulation is proportionate to the interests sought to be advanced.”¹⁹⁶

VII. Conclusion

The pervasive collection and use of personal data online for secondary purposes causes substantial harm to consumers. The FTC should promulgate a Section 5 unfair trade practices rule to prohibit these widespread and harmful surveillance practices. The Commission has broad authority under Section 5 to address these issues and there are several different ways that they could craft them. We believe that the most effective rule would be a blanket prohibition on most secondary use and third party disclosure with narrow exceptions. This would ensure that consumers are not subjected to unwanted surveillance and unfair data practices.

¹⁸⁹ *Barr v. Am. Ass’n of Political Consultants, Inc.*, 140 S. Ct. 2335, 2349 (2020) (Breyer, J., concurring in the judgment with respect to severability and dissenting in part). See *Glickman v. Wileman Bros. & Elliott, Inc.*, 521 U.S. 457, 469–70 (1997).

¹⁹⁰ *Central Hudson Gas & Elec. Corp. v. Pub. Svc. Comm’n of N.Y.*, 447 U.S. 557 (1980).

¹⁹¹ *Nat’l Cable & Telecomm. Ass’n v. FCC*, 555 F.3d 996 (D.C. Cir. 2009) (internal quotation marks omitted).

¹⁹² *Trans Union Corp v. FTC* (“*Trans Union I*”), 245 F.3d 809, 818 (D.C. Cir. 2001).

¹⁹³ See, e.g., *Nat’l Cable & Telecommunications Ass’n v. F.C.C.*, 555 F.3d 996, 1002 (2009) (upholding the Telecommunications Act privacy rules); *Mainstream Mktg. Servs. Inc. v. FTC*, 358 F.3d 1228, 1246 (10th Cir. 2004) (upholding the Do Not Call Registry rules); *Nat’l Fed. of the Blind v. FTC*, 420 F.3d 321 (4th Cir. 2005) (same); *Trans Union LLC v. FTC* (“*Trans Union III*”), 295 F.3d 42 (D.C. Cir. 2002) (upholding the Gramm-Leach-Bliley Act privacy protections); *Trans Union I*, 245 F.3d at 818–19 (upholding the Fair Credit Reporting Act prohibition on selling target market lists).

¹⁹⁴ *Trans Union I*, 245 F.3d at 818 (quoting *Dun & Bradstreet, Inc. v. Greenmass Builders, Inc.*, 472 U.S. 729 762 n.8 (1985)).

¹⁹⁵ *Trans Union Corp. v. FTC* (“*Trans Union II*”), 267 F.3d 1138, 1143 (D.C. Cir. 2001); *Nat’l Cable & Telecommunications Ass’n v. F.C.C.*, 555 F.3d 996, 1001–02 (2009).

¹⁹⁶ *Nat’l Cable & Telecommunications Ass’n v. F.C.C.*, 555 F.3d 996, 1002 (2009).

Organization Descriptions

Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to 6 million members across the U.S.

EPIC is an independent, nonprofit organization that has been focusing public attention on emerging privacy and civil liberties issues since 1994. EPIC works at the intersection of policy, advocacy, and litigation to protect privacy, freedom of expression, and democratic values in the information age. EPIC files briefs in cutting edge privacy cases, files comments and petitions with federal and state regulatory agencies, and provides expert advice to policymakers and lawmakers.

Model State Privacy Act



FEBRUARY, 2021

INTRODUCTION

Over the last thirty years, companies have dramatically expanded their data collection practices as they have found new ways to monetize consumers' private information, but there are few federal requirements to keep that data private and secure. This lack of legal protections is particularly frustrating because privacy is a basic human right, enshrined in American jurisprudence and in nearly a dozen state constitutions.¹ While there are federal laws that provide certain protections for financial² and some health data,³ there is no comprehensive federal privacy law granting consumers baseline privacy and security protections, covering tech giants like Google, Amazon, and Facebook. The Federal Trade Commission (FTC) has taken action against companies for privacy and security violations under its authority to police unfair and deceptive acts and practices,⁴ but it is vastly underpowered and under-resourced.⁵ California has adopted a landmark privacy law, the California Consumer Privacy Act (CCPA), but consumers have struggled to exercise their new privacy rights.⁶

Consumers shouldn't bear the burden of securing their own privacy. This model bill prohibits companies from engaging in the most privacy-invasive behaviors. The data minimization provision limits companies' collection, use, and disclosure of data to what is reasonably necessary to operate the service. In contrast, existing privacy laws typically require consumers to either opt in or opt out of the disclosure of their data. Both are better than the FTC's "notice-and-choice" regulatory approach, which directs companies to outline their privacy practices in a disclosure.⁷ But neither is ideal. While opt in may be preferable to opt out, particularly in the absence of a global opt-out option, companies have been able to force consumers to consent to more sharing than they intended through the use of dark patterns—deceptive interfaces that subvert user intent.⁸ In response to Europe's recent GDPR privacy law, many websites forced users through confusing consent dialogs to ostensibly obtain consent to share and collect data

¹ National Conference of State Legislatures, Privacy Protections in State Constitutions (May 11, 2020), <https://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx>.

² Gramm-Leach-Bliley Act, 113 Stat. 1338.

³ Health Insurance Portability and Accountability Act, 110 Stat. 1936.

⁴ Fed. Trade Comm'n, Privacy and Security Enforcement (last visited May 19, 2020), <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement>.

⁵ Tony Romm, *The Agency in Charge of Policing Facebook and Google is 103 Years Old. Can it Modernize?* WASH. POST (May 4, 2018), <https://www.washingtonpost.com/news/the-switch/wp/2018/05/04/can-facebook-and-googles-new-federal-watchdogs-regulate-tech/>.

⁶ Maureen Mahoney, *California Consumer Privacy Act: Are Consumers' Digital Rights Protected?* CONSUMER REPORTS DIGITAL LAB (Oct. 1, 2020), http://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf. California voters have recently ratified the California Privacy Rights Act (CPRA), which refines and strengthens the CCPA. Most provisions will become operative on January 1, 2023.

⁷ Florencia Marotta-Wurgler, *Does "Notice and Choice" Disclosure Regulation Work? An Empirical Study of Privacy Policies* at 2-3 (Apr. 2015), <https://www.law.umich.edu/centersandprograms/lawandeconomics/workshops/Documents/Paper13.Marotta-Wurgler.Does%20Notice%20and%20Choice%20Disclosure%20Work.pdf>.

⁸ Harry Brignull, *Dark Patterns: Inside the Interfaces Designed to Trick You*, THE VERGE (Aug. 29, 2013), <https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you>.

for any number of undisclosed purposes.⁹ Consumers shouldn't be asked to opt in to harmful data sharing; it should simply be restricted.

Consumer Reports proposes this model legislation to ensure that companies are required to honor consumers' privacy. This model law uses the CCPA as a baseline,¹⁰ and provides additional protections to ensure that consumers' privacy rights are respected by default—in other words, without the consumer having to take action. The model bill provides eight key protections:

- Data minimization and a broad prohibition on secondary data sharing;
- Opt out of first-party advertising;
- Right to delete;
- Right to access and data portability;
- Right to correct;
- Data security;
- Non-discrimination; and
- Strong enforcement.

In the absence of comprehensive consumer privacy protections on the federal level, momentum for privacy and data security laws has moved to the states. The CCPA, which went into effect on January 1, 2020, is one of the first comprehensive laws to protect consumers' online privacy.¹¹ The CCPA advances consumer protections in several important ways—increased transparency, and the right to access, delete, and opt out of the sale of information to third parties. But while it is a good start, the CCPA is not strong enough to fully protect consumer data. The CCPA provides few limits on companies' collection of data—which inherently threatens consumer privacy. The unchecked collection and sharing of data—even if it has nothing to do with the service requested by the consumer—has allowed companies like Google and Facebook to grow into behemoths with the ability to draw unparalleled insights into a consumer's activities, associations, and preferences—and even to predict these behaviors. Once collected, even under the CCPA, there are few limits on what companies can do with the data.

The CCPA also puts a lot of responsibility on the consumer to figure out every company that collects information about them and opt out—which is too burdensome for consumers. Consumer Reports has found that consumers experience significant difficulty exercising their rights under the CCPA. In our recent study, hundreds of volunteers tested the opt-out provision of the CCPA, by submitting DNS requests to companies listed on the data broker registry. 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. Consumers were often forced to wade through confusing and intimidating disclosures to opt out. About 14% of the time, burdensome or broken DNS processes prevented consumers from exercising their rights under the CCPA.¹² In the absence of default privacy protections, the new

⁹ *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy*, NORWEGIAN CONSUMER COUNCIL (Jun. 27, 2018), <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>.

¹⁰ Cal. Civ. Code § 1798.100 et seq.

¹¹ *Id.* at § 1798.198.

¹² *California Consumer Privacy Act: Are Consumers' Digital Rights Protected?*, *supra* note 6.

Global Privacy Control, a proposed standard to allow consumers to send a global “Do Not Sell” signal, could help make the CCPA more workable for consumers¹³ (CCPA regulations require companies to honor these signals;¹⁴ CPRA adds this requirement to the statute).¹⁵ The CCPA’s authorized agent provisions, which allow consumers to delegate third parties to submit requests on their behalf, also help provide a practical option for consumers seeking to submit requests to multiple companies.¹⁶

Additionally, some adtech platforms and publishers, including Google and Facebook, have exploited ambiguities in the CCPA to not honor consumer requests to stop the sale of their information to third parties.¹⁷ The recently-ratified California Privacy Rights Act will help close up loopholes that companies have exploited to continue to deliver targeted advertising outside of the opt out—though those provisions will not go into effect until 2023.¹⁸

Some states have been moving in the wrong direction following passage of CCPA. Several states have pursued legislation that is weaker than the CCPA. For example, in 2019, an industry-favored privacy bill, SB 5376, nearly passed the Washington State legislature, over the objections of privacy advocates.¹⁹ The 2019 bill—based on a risk assessment model that would have essentially given companies the choice of whether or not to comply—unfortunately has been replicated in other states, such as Illinois,²⁰ Minnesota,²¹ and Arizona.²² (A much-improved Washington Privacy Act also failed to make it across the finish line in 2020).²³ In 2019, Nevada passed a bill giving consumers a limited right to opt out of the sale of their data to third parties—but the new law is riddled with exemptions, and due to its narrow definition of sale, does not completely cover data used for online tracking.²⁴ Weak privacy legislation could be worse than no privacy legislation at all, if it does nothing to rein in existing data use practices and hinders efforts to pass effective legislation in other states or on the federal level.

That’s why it’s crucial that states pass privacy legislation that protects consumers’ privacy by default. Below, we outline the key provisions for strong legislation:

¹³ Press release, *Announcing Global Privacy Control: Making it Easy for Consumers to Exercise Their Privacy Rights*, Global Privacy Control (Oct. 7, 2020), <https://globalprivacycontrol.org/press-release/20201007.html>.

¹⁴ Cal. Code Regs. tit. 11 § 999.315(c) (2020).

¹⁵ Cal. Civ. Code § 1798.135(e).

¹⁶ Consumer Reports has begun to explore submitting CCPA requests on behalf of consumers. See Maureen Mahoney, Ginny Fahs, and Don Marti, *The State of Authorized Agent Opt Outs Under the California Consumer Privacy Act*, CONSUMER REPORTS DIGITAL LAB (Feb. 2021), https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_AuthorizedAgentCCPA_022021_VF_.pdf.

¹⁷ Maureen Mahoney, *Many Companies Are Not Taking the California Consumer Privacy Act Seriously—The Attorney General Needs to Act* (Jan. 9, 2020), <https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb>.

¹⁸ California Privacy Rights Act (2020), https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf.

¹⁹ Letter from Consumer Reports et al. to The Honorable Christine Rolfes (Feb. 21, 2019), <https://advocacy.consumerreports.org/wp-content/uploads/2019/02/SB-5376-Privacy-Coalition-Letter-Oppose.pdf>; Letter from Consumer Reports et al. to The Honorable Zach Hugins (March 25, 2019), <https://advocacy.consumerreports.org/wp-content/uploads/2019/03/Privacy-Coalition-Letter-Opposing-ITED-v.-4.pdf>.

²⁰ SB 2263 (2019).

²¹ HF 3936 (2020).

²² HB 2729 (2019).

²³ Maureen Mahoney, *Washington State Fails to Advance Game-Changing Privacy Law*, MORNING CONSULT (Mar. 16, 2020), <https://morningconsult.com/opinions/washington-state-fails-to-advance-game-changing-privacy-law/>.

²⁴ NRS 603A.345, <https://www.leg.state.nv.us/NRS/NRS-603A.html>.

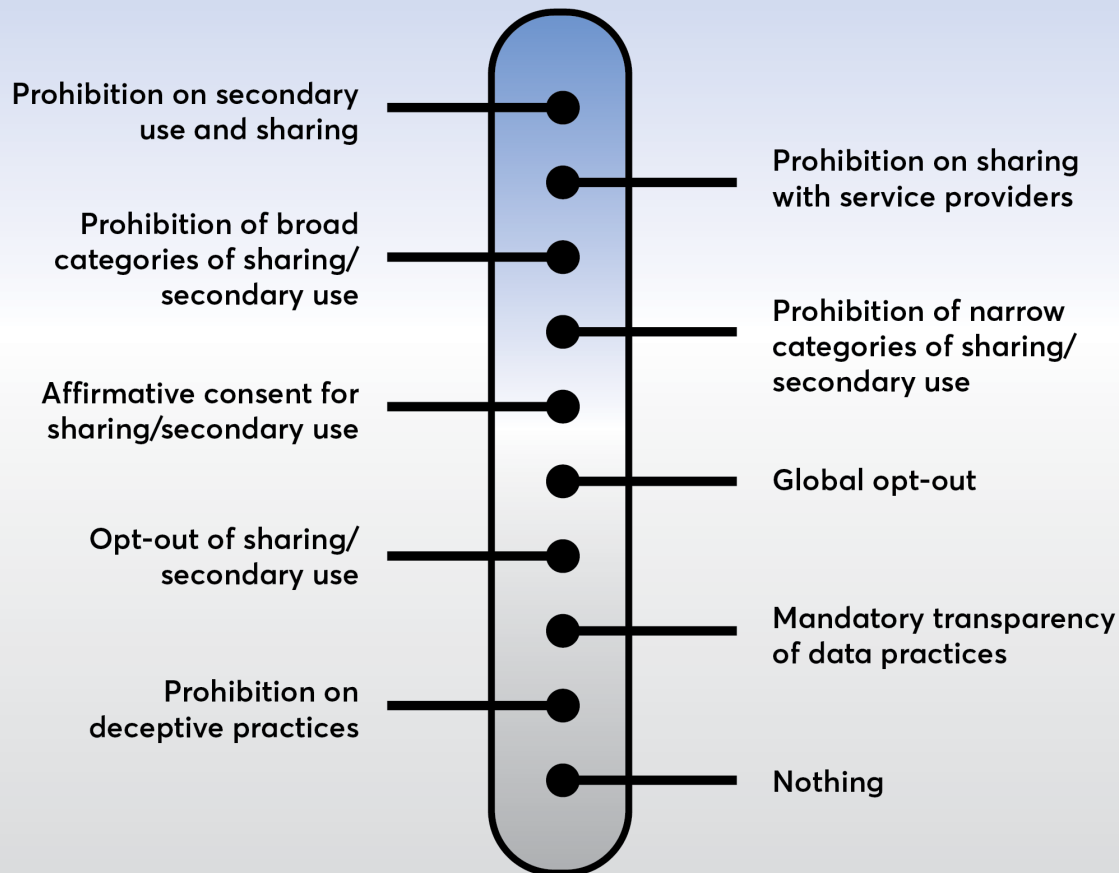
Data minimization and a broad prohibition on secondary data sharing: Privacy laws must set limits on the data that companies can collect and share. Consumers should be able to use an online service or app safely without having to take any action, such as opting in or opting out. This model bill helps ensure privacy by default by requiring data minimization in Section 2, 103(a)-(b), in other words, limiting data collection and sharing to what is reasonably necessary to provide the service requested by the consumer, with some exceptions for operational purposes. Falling outside of the limits of what is reasonably necessary is the sale of data to third parties, which is contrary to consumer expectations and is not needed to provide the service.

A strong default prohibition on data sharing is preferable to an opt-out based regime which relies on users to hunt down and navigate divergent opt-out processes for potentially hundreds of different companies. We do not characterize this framework as an “opt-in” approach either, as secondary data sharing is simply prohibited. While consumers are always free to share data with whomever they like, a privacy law should not encourage companies to coerce consumers into giving permission for additional tracking or sharing, such as by denying consumers access to the site content without agreement to the information-sharing terms, as many companies have done in response to the Global Data Protection Regulation (GDPR) in Europe. If companies want to collect personal data, it should only be as functionally necessary for the specific product a consumer has requested, not for monetization. Privacy law should also prohibit discrimination or differential treatment against consumers who do not agree to share data for a separate unrelated product. If a consumer affirmatively wants to fill out a survey or allow advertisers to monitor cross-site and -app behavior to recommend ads, that is their prerogative. But too often manipulative and confusing consent flows lead users into granting permission to unexpected and unwanted data collection or sharing. Existing consumer protection law prohibits deceptive interfaces, but a privacy statute could more clearly prohibit abusive “dark patterns” that subvert user autonomy.

Section 3(m) lists permitted secondary uses that a company can reasonably do without permission from the consumer: this includes fixing errors, performing internal research (based on first-party data) to improve its own product, and providing customized content or advertising. In other words, this bill permits a fair amount of first-party uses of the data so that consumers can continue to receive the services that they would normally expect—such as having sites recommend products that they might like—without being pummeled with opt-in notices. Consent fatigue is a real concern—if consumers begin to expect to have to opt in to simply use the service, they will be less likely to make a distinction between reasonable and harmful uses of data.²⁵ The bill also takes the burden of managing privacy and data collection off of the consumer and puts it, appropriately, onto the company.

²⁵ Neil M. Richards and Woodrow Hartzog, *The Pathologies of Digital Consent* at 1497-8, WASHINGTON UNIVERSITY LAW REVIEW (2019), <https://ssrn.com/abstract=3370433>.

Range of possible policy options to rein in data sharing



Opt out of first-party advertising: However, some consumers might be uncomfortable with companies tracking their purchases and offering them suggestions about what they might like. That's why we have provided an opt out for first-party use of data for advertising purposes in Section 2, 103(c). This will ensure that consumers who are more sensitive to first-party advertising can exercise their privacy preferences, without running the risk of consent fatigue.

Right to delete: Consistent with the data minimization principle, consumers should be able to delete data when it is no longer needed. This will help reduce the risk of unwanted disclosure, including through a data breach. For example, the Capital One breach of 2019 included the disclosure of data from credit applications that were over ten years old.²⁶ The right to delete provision in this bill tracks the CCPA, which is designed to allow businesses to continue to retain

²⁶ Capital One, Information on the Capital One Cyberincident (Sept. 23, 2019), <https://www.capitalone.com/facts2019/>.

data if it is needed to continue to provide the service, for research purposes, and for recall and warranty notifications.

Right to access and data portability: Consumers deserve to know the specific information that companies have on file. This model bill gives consumers the ability to access the specific pieces of data collected about them, as well as the specific third parties to whom their information was disclosed—which will make it easier for consumers to exercise their privacy preferences with respect to those companies. It is more expansive than the CCPA, which provides only the categories of third parties to whom the data is sold. This bill also ensures data portability, in other words, it requires companies to provide data in a format that could be easily transferred to a competing service, helping to improve competition among online services. This draft improves upon the CCPA by giving consumers the right to direct the company to transfer that information to another entity so that the consumer does not have to download and port the information themselves.

Right to correct: Personal information is often used to make important decisions about consumers, such as with respect to employment and housing—and data brokers' files often include incorrect information.²⁷ Consumers should have the right to ensure that the information is accurate. The Fair Credit Reporting Act,²⁸ the GDPR,²⁹ and the California Privacy Rights Act³⁰ all include a right to correct, suggesting that correction rights are increasingly considered one of the basic digital privacy rights.

Non-discrimination: This model state law includes a provision to ensure that companies can't charge consumers more for exercising their privacy rights. Unfortunately, ambiguity in CCPA's text could allow for programs that monetize data by selling personal information about customer habits to third-party data brokers. Consumers could be forced to choose between affordable necessities and their own rights, and retailers can continue to profit off of business models that exploit consumers' privacy without meaningful consumer choice. This model bill cuts off exploitative programs that could separate consumers into privacy haves and have-nots, and clarifies that legitimate loyalty programs, which reward consumers for repeated patronage, are supported by this bill. This bill also ensures that consumers' personal information (like browsing history) can't be used to deny them economic opportunities and benefits.

Data security: This bill ensures that companies are required to protect all information that is reasonably linkable to a consumer. Companies should be required to keep behavioral data, search history, and shopping history secure, as it can reveal more about consumers than they might want to share with others: their sexual preferences, health issues, and political activities. Over 20 states require businesses to keep data secure, but those requirements typically cover only a limited set of personal information (such as banking and other financial information that could lead to identity theft).³¹

²⁷ Persis Yu, *Big Data: A Big Disappointment for Scoring Consumer Credit Risk*, NAT'L CONSUMER LAW CTR. at 15 (Mar. 2014), <https://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf>.

²⁸ 15 U.S.C. § 1681.

²⁹ European Parliament and Council of European Union (2016) *Regulation (EU) 2016/679*, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>.

³⁰ California Privacy Rights Act, *supra* note 18.

³¹ National Conference of State Legislatures, *Data Security Laws: Private Sector* (May 29, 2019), <https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx>.

Strong enforcement: Finally, the CCPA's weak enforcement provisions have been corrected in this model law by adding a private right of action, removing the requirement that the AG provide individual compliance advice to companies, and removing the right to cure (the guidance requirement and right to cure in the CCPA also will be removed from the law when the California Privacy Rights Act becomes operative in 2023). Strong enforcement is essential to make sure that companies comply. The California AG has the resources to bring only an estimated three cases a year for privacy violations, which provides companies with little incentive to comply, given that their chances of getting caught are minimal.³² The right to cure provision is particularly problematic, as it essentially constitutes a get-out-of-jail-free card for any company that is caught violating the law, provided they can fix their behavior in 30 days. (And given the nature of privacy violations, it's unclear how to "cure" the inappropriate disclosure of a consumer's personal information). In Europe, clearly illegal data sharing practices have continued unabated, despite the GDPR. Regulators as yet appear unwilling to truly hold companies accountable. For example, the UK regulator found that RTB behaviors—the buying and selling of consumer data to sell space on sites for targeted advertising—violates the consent requirement of the GDPR, but still hasn't penalized any companies for continuing to engage in the behavior without consumer consent.³³ While the issue is not without debate, we believe consumer rights are most protected by providing for a private right of action to create appropriate incentives for compliance.

Finally, this is an evolving document that we will update as more information becomes available.

³² Yuri Nagano, *California Attorney General Plans Few Privacy Law Enforcement Actions, Telling Consumers to Take Violators to Court*, SAN FRANCISCO PUBLIC PRESS (May 15, 2019), <https://sfpublicpress.org/news/2019-05/california-attorney-general-plans-few-privacy-law-enforcements-telling-consumers-to-tak>.

³³ Simon McDougall, *Blog: Adtech - The Reform of Real Time Bidding Has Started and Will Continue*, ICO (Jan. 17, 2020), <https://ico.org.uk/about-the-ico/news-and-events/blog-adtech-the-reform-of-real-time-bidding-has-started/>.

MODEL STATE PRIVACY ACT

Section 1. Short title. This Act may be cited as the Consumer Privacy Act.

Section 2. Requirements. The following is added to the code of statutes:

100. Transparency about the collection, use, retention, and sharing of personal information.³⁴

(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.³⁵

(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.

³⁴ Intel, Ethical and Innovative Data Use Act of 2019, Section 4(f), (May 23, 2019), <https://usprivacybill.intel.com/wp-content/uploads/IntelPrivacyBill-05-25-19.pdf>. This bifurcated notice—which requires both an easy-to-read, consumer-facing section to explain to consumers how to exercise their rights; and a second, longer section, intended for regulators and privacy testing organizations, that explains the large business's data use practices, so they can be held accountable for failure to comply—is adapted from Intel's 2019 model privacy bill.

³⁵ *Id.* at Section 4(f)(3)(B).

103. 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.³⁶ 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.³⁷

104. Prohibition of dark patterns.

(a) It shall be unlawful for any company to design, modify, or manipulate a user interface with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice, as further defined by regulation.³⁸

105. Deletion of personal information.

(a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected.

(b) A business that collects personal information about consumers shall disclose, pursuant to the notice requirements of subsection 130, the consumer's right to request the deletion of the consumer's personal information.

³⁶ In this model law, data minimization puts real limits on the company by allowing only the collection and sharing of data needed to provide the service requested by the consumer. While the concept of data minimization is included in the GDPR, the GDPR's formulation is too weak, allowing data collection and sharing this is "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed." Companies could still list any purposes they would like into the policy to collect whatever they want—taking advantage of the fact that consumers don't typically read privacy policies.

³⁷ This subsection adds protections to the CCPA—data minimization—that are similar to CA AB 3119 (2020), which would limit collection and sharing to what is reasonably necessary to operate the service, with exemptions for operational purposes. This model bill improves upon AB 3119 since it does not require the consumer to opt-in to data sharing that is necessary to operate the service. The goal is to prevent consumers from being barraged with unnecessary consent dialogues, and to ensure that consumers can both use the service and have their privacy protected.

³⁸ This definition of "dark patterns" is adapted from S. 1084 (2019), The DETOUR Act, <https://www.congress.gov/bill/116th-congress/senate-bill/1084/text>. Subverting consumer intent online has become a real problem, and it's important to address. A 2019 Princeton University study of 11,000 shopping sites found more than 1,800 examples of dark patterns, many of which clearly crossed the line into illegal deception. See Mathur, Acar, Friedman, Lucherini, Mayer, Chetty, and Narayanan, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, CONSUMERPROC. ACM HUM.-COMPUT. INTERACT. (2019), <https://webtransparency.cs.princeton.edu/dark-patterns/>.

(c) A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.

(d) If a consumer submits a deletion request to a service provider that has collected, used, processed, or retained the consumer's personal information in its role as a service provider, then the service provider shall direct the consumer to the business where the consumer can submit their deletion request.

(e) A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:

(1) Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or otherwise perform a contract between the business and the consumer.³⁹

(2) Detect or respond to security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity.

(3) Debug to identify and repair errors that impair existing intended functionality.

(4) Exercise constitutionally-protected speech, or ensure the right of another consumer to exercise his or her right to constitutionally-protected speech, including speech conducted through use of a business.

(5) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the business's deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

(6) Comply with a legal obligation.

110. Access to and portability of retained personal information.

(a) If a business collects personal information about a consumer, the consumer shall have the right to ask the business for the following information, and the business shall have the duty to provide it, promptly and free of charge, upon receipt of a verifiable request:

(1) The specific pieces of personal information that the business retains about that consumer.

(2) Its purpose for collecting the personal information.

(b) When a business receives a verifiable consumer request from a consumer for the specific pieces of their personal information, the business shall disclose that information in an electronic, portable, machine-readable, and readily-useable format or formats to the consumer, or to another business of the consumer's designation. The Attorney General shall issue regulations to implement this subsection.

115. Access to disclosures of personal information.

(a) If a business discloses personal information about a consumer to a third party or service provider, the consumer shall have the right to ask the business for the specific third parties or service providers to whom the personal information was disclosed, and the business

³⁹ This provision was added to the CCPA by AB 1146 (2019), to ensure that the CCPA does not interfere with consumer notification in the event of a recall or to take advantage of a warranty.

shall have the duty to provide it, promptly and free of charge, upon receipt of a verifiable request.⁴⁰

120. Right to correct inaccurate personal information.⁴¹

(a) A consumer shall have the right to require a business that maintains inaccurate personal information about the consumer to correct such inaccurate personal information.

(b) A business that collects personal information about consumers shall disclose, pursuant to subsection 130, the consumer's right to request correction of inaccurate personal information.

(c) A business that receives a verifiable consumer request to correct inaccurate information shall use commercially reasonable efforts to correct the inaccurate personal information, as directed by the consumer, pursuant to subsection 130.

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

(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.⁴²

126. Discrimination in economic opportunities.⁴³

(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:

⁴⁰ This subsection expands upon the CCPA by requiring companies to provide specific third parties to whom the information was sold, rather than just the categories of companies, so consumers can more easily exercise their rights with respect to those companies.

⁴¹ This subsection is adapted from CPRA § 1798.106.

⁴² This subsection removes from the CCPA the existing § 1798.125(e) that could allow companies to charge consumers more for exercising their privacy rights. In its place is a provision making it clear that bona fide loyalty programs, that reward consumers for repeated patronage, are allowed and even encouraged, as long as these companies are prohibited from selling data to third parties. It is similar to consensus language in the Washington Privacy Act (2021), Sec. 107(v)(7), <http://lawfilesex.leg.wa.gov/biennium/2021-22/Pdf/Bills/Senate%20Bills/5062-S2.pdf?q=20210221185931>.

⁴³ This subsection is drawn from *The Online Civil Rights and Privacy Act of 2019*, FREE PRESS ACTION AND THE LAWYERS' COMMITTEE FOR CIVIL RIGHTS UNDER LAW, Section 3(a) (Mar. 11, 2019), https://www.freepress.net/sites/default/files/2019-03/online_civil_rights_and_privacy_act_of_2019.pdf.

(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.

127. Discrimination in public accommodations.⁴⁴

(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.

128. 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.

130. Business implementation of duties.

(a) A business shall:

(1) (A) Make available to consumers two or more designated methods for submitting requests permitted by this title, including, at a minimum, a telephone number. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address or online portal for submitting requests for information required to be disclosed pursuant to subsections

⁴⁴ *Id.* at Section 3(b). This subsection is drawn from Free Press Action and the Lawyers' Committee for Civil Rights Under Law's Online Civil Rights and Privacy Act of 2019.

110 and 115, or for requests for deletion or correction pursuant to subsections 105 and 120, respectively.⁴⁵

(B) If the business maintains an internet website, make the internet website available to consumers to submit requests for information required to be disclosed pursuant to subsections 110 and 115, or for requests for deletion or correction pursuant to subsections 105 and 120, respectively.

(2) Disclose and deliver the required information to a consumer free of charge, or correct inaccurate personal information, or delete a consumer's personal information, based on the consumer's request, within 45 days of receiving a verifiable consumer request. The business shall promptly take steps to determine whether the request is a verifiable consumer request from the identified consumer. The time period may be extended once by 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. It shall be delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option, if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, but shall not require the consumer to create an account with the business in order to make a verifiable request.

(3) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in this Act, and how to direct consumers to exercise their rights in this Act.

(4) Limit the use of any personal information collected from the consumer in connection with the business's verification of the consumer's request solely for the purposes of verification, and not further disclose the personal information or retain it longer than necessary for the purposes of verification.

(b) A business is not obligated to provide the information required by subsections 110 and 115 to the same consumer more than twice in a 12-month period.

(c) A service provider shall not be required to comply with a verifiable consumer request pursuant to subsections 110, 115, and 120 to the extent that the service provider has collected personal information about the consumer in its role as a service provider. A service provider shall provide assistance to a business with which it has a contractual relationship with respect to the business's response to a verifiable consumer request, including but not limited to by providing to the business the consumer's personal information in the service provider's possession, which the service provider obtained as a result of providing services to the business, and by correcting inaccurate information. A service provider that collects personal information on behalf of a business shall be required to assist the business in complying with the requirements of subsection 100.⁴⁶

Section 3. Definitions.

For purposes of this title:

(a) "Aggregate consumer information" means information that relates to a group of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified.

⁴⁵ This incorporates amendments to the CCPA made by AB 1564 (2019).

⁴⁶ This clarification of the role of service providers is added by CPRA § 1798.130(a)(3)(A).

(b) “Biometric information” means an individual’s physiological, biological or behavioral characteristics or an electronic representation of such, including an individual’s deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(c) “Business” means:

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that collects consumers’ personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers’ personal information, that does business in the State of [XX], and that satisfies one or more of the following thresholds:

(A) As of January 1 of the calendar year, had annual gross revenues in excess of fifty million dollars (\$50,000,000) in the preceding calendar year, as adjusted pursuant to Section 8.

(B) Alone or in combination, annually buys, receives for the business’ commercial purposes, shares, or discloses for commercial purposes, alone or in combination, the personal information of [100,000] or more consumers, households, or devices.⁴⁷

(C) Derives 50 percent or more of its annual revenues from sharing consumers’ personal information.

(2) Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business and with whom the business shares consumers’ personal information. “Control” or “controlled” means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. “Common branding” means a shared name, servicemark, or trademark, such that the average consumer would understand that two or more entities are commonly owned.

(3) A joint venture or partnership composed of businesses in which each business has at least a 40 percent interest. For purposes of this title, the joint venture or partnership and each business that composes the joint venture or partnership shall separately be considered a single business, except that personal information in the possession of each business and disclosed to the joint venture or partnership shall not be shared with the other business.

(e) “Collects,” “collected,” or “collection” means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer’s behavior.

(f) “Commercial purposes” means to advance a person’s commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. “Commercial purposes” do not include for the purpose of

⁴⁷ CPRA raises one of the CCPA’s thresholds: from a company that receives or shares the data of 50,000 consumers, households, or devices per year to one that receives or shares the data of 100,000 consumers, households, or devices per year. Since “consumer” refers to a resident of the state, these numbers will not be appropriate for states with much smaller populations, and we recommend adopting a threshold that is roughly proportionate.

engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.

(g) “Consumer” means a natural person who is a [XX] resident. It does not include an employee or contractor of a business acting in their role as an employee or contractor.

(h) “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.⁴⁸

(i) “Designated methods for submitting requests” means a mailing address, email address, Internet Web page, Internet Web portal, telephone number, or other applicable contact information, whereby consumers may submit a request under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 8.

(j) “Device” means any physical object that is capable of connecting to the Internet, directly or indirectly, or to another device.

(k) “Health insurance information” means a consumer’s insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the consumer, or any information in the consumer’s application and claims history, including any appeals records, if the information is linked or reasonably linkable to a consumer or household, including via a device, by a business or service provider.

(l) “Intentionally interacts” means when the consumer intends to interact with a person via one or more deliberate interactions, such as visiting the person’s website or purchasing a good or service from the person. Hovering over, muting, pausing, or closing a given piece of content, or using a communications service to interact with a third-party website, does not constitute a consumer’s intent to interact with a person.

(m) “Large business” is a business that, alone or in combination, buys, receives for the business’s commercial purposes, sells, or shares for commercial purposes the personal information of [10,000,000] or more consumers in a calendar year.⁴⁹

(n) “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

⁴⁸ This definition is similar to that in CPRA and tracks the Federal Trade Commission’s definition of deidentified: that a company cannot reidentify the information, even if they wanted to. See, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, FED. TRADE COMM’N at 21 (2012), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

⁴⁹ This definition of “large business” for bifurcated notice obligations reflects the one included in the California Attorney General’s CCPA regulations, § 999.317(g). Since “consumer” refers to a resident of the state, these numbers likely will not be appropriate for states with much smaller populations than California, and we recommend adopting a threshold that is roughly proportionate.

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.

(o) “Person” means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

(p) (1) “Personal information” means information that identifies or could reasonably be linked, directly or indirectly, with a particular consumer, household, or consumer device.⁵⁰

(2) “Personal information” does not include publicly available information. For the purposes of this paragraph, “publicly available” means information that is lawfully made available from federal, state, or local government records. “Personal information” does not include consumer information that is deidentified or aggregate consumer information.

(q)(1) “Place of public accommodation” includes all businesses of any kind, whether for-profit or not for-profit, that offer goods or services of any kind to the general public, whether for a charge or not for a charge. This includes businesses that offer goods or services through the Internet or any other medium of communications, regardless of whether or not they operate from a physical location.⁵¹

(2) “Place of public accommodation” does not include a tax-exempt religious entity, a distinctly private club, or a distinctly private online discussion forum. A club or online discussion forum shall be deemed distinctly private if (1) Its primary purpose is expressive association; (2) It is membership-based and has no more than 1000 members; and (3) It does not regularly receive payment directly or indirectly on behalf of non-members for dues, fees, use of physical or online facilities, or goods or services of any kind, for the furtherance of trade or business.⁵²

(r) “Processing” means any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means.

(s) “Service” or “services” means work, labor, and services, including services furnished in connection with the production, sale or repair of goods.

(s) “Service provider” means a person that processes personal information on behalf of a business and to which the business discloses a consumer’s personal information pursuant to a written or electronic contract, provided that (1) the contract prohibits the person from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, including a prohibition on retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business; and (2) the service provider does not combine the personal information which the service provider receives from or on behalf of the business with personal information which the service provider receives from or on behalf of another person or persons, or collects from its own interaction with consumers.⁵³

⁵⁰ This definition of personal information is similar to the CCPA, in that it covers information reasonably linkable to a consumer, both directly or indirectly. It’s important to have a broad definition of personal information to ensure that targeted advertising is covered by the law: information disclosed for targeted advertising purposes cannot always be associated with an individual consumer. However, unlike the CCPA, this definition does not include examples of categories of personal information, because a list could have the unintended effect of limiting the information covered by the law.

⁵¹ From David Brody and Sean Bickford, *Discriminatory Denial of Service: Applying State Public Accommodations Laws to Online Commerce*, LAWYERS’ COMMITTEE FOR CIVIL RIGHTS UNDER LAW at 7 (Jan. 2020), <https://lawyerscommittee.org/wp-content/uploads/2019/12/Online-Public-Accommodations-Report.pdf>.

⁵² *Id.*

⁵³ The service provider exemption improves upon the CCPA’s and CPRA’s by tightly limiting use of the information and preventing service providers from combining information received from multiple companies. Without these

(t) “Share” means renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to a third party for monetary or other valuable consideration, or otherwise for a commercial purpose.⁵⁴

For purposes of this title, a business does not share personal information when:

(1) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with one or more third parties, provided the third party or parties do not also share the personal information, unless that disclosure would be consistent with the provisions of this title.

(2) The business discloses the personal information of a consumer with a service provider and the business has provided notice that the information is being used or disclosed in its terms and conditions consistent with subsection 100.

(3) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or disclosed consistently with this title. A third party may not materially alter how it uses or discloses the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection.

(u) “Third party” means a person who is not any of the following:

(1) The business with whom the consumer intentionally interacts and that collects personal information from the consumer as part of the consumer’s current interaction with the business under this title.

(2) A service provider to whom the business discloses a consumer’s personal information pursuant to a written contract, which includes a certification made by the person receiving the personal information that the person understands the restrictions under the Consumer Privacy Act and will comply with them.

(v) “Verifiable consumer request” means a request that is made by a consumer, by a consumer on behalf of the consumer’s minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer’s behalf, and that the business can reasonably verify.⁵⁵ A business is not obligated to provide any personal information to a consumer pursuant to subsections 110 and 115, to delete personal information pursuant to subsection 105, or to correct inaccurate personal information pursuant to subsection 120, if the business cannot verify that the consumer making the request is the consumer about whom the business has collected personal information or is a person authorized by the consumer to act on such consumer’s behalf.⁵⁶

protections, service providers (such as Salesforce) could build huge databases of customer data, allowing them to develop even more sensitive insights into consumers’ behavior.

⁵⁴ This definition is similar to the CCPA’s definition of sale, except it adds a final clause, “or otherwise for a commercial purpose,” to ensure that transfers of data for targeted advertising purposes are covered (this loophole is addressed by CPRA). Some incorrectly claim that because money isn’t necessarily exchanged for data, data transfers for targeted advertising purposes aren’t a sale under the CCPA—therefore, consumers don’t have the right to opt out. See, Tim Peterson, *‘We’re Not Going to Play Around’: Ad Industry Grapples with California’s Ambiguous Privacy Law*, DIGIDAY (Dec. 9, 2019), <https://digiday.com/marketing/not-going-play-around-ad-industry-grapples-californias-ambiguous-privacy-law/>.

⁵⁵ This “authorized agent” provision mirrors language in the CCPA that gives consumers the right to delegate to third parties the ability to submit requests on their behalf, providing a practical option for submitting requests to multiple companies.

⁵⁶ It’s appropriate to require identity verification for access, correction, and deletion requests, however, opt outs should not require verification, since that would exempt information that can’t be associated with an identifiable consumer.

Section 4. Exceptions.

(a) The obligations imposed on businesses by this title shall not restrict a business's or service provider's ability to:

(1) Comply with federal, state, or local laws.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

(3) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.

(4) Exercise or defend legal claims.

(5) Collect, use, retain, share, or disclose consumer information that is deidentified or in the aggregate derived from personal information.

(6) Collect or share a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of [XX]. For purposes of this title, commercial conduct takes place wholly outside of [XX] if the business collected that information while the consumer was outside of [XX], no part of the sharing of the consumer's personal information occurred in [XX], and no personal information collected while the consumer was in [XX] is shared. This paragraph shall not permit a business from storing, including on a device, personal information about a consumer when the consumer is in [XX] and then collecting that personal information when the consumer and stored personal information is outside of [XX].

(b) Nothing in this title shall require a business to violate an evidentiary privilege under [XX] law or federal law or prevent a business from providing the personal information of a consumer who is covered by an evidentiary privilege under [XX] law as part of a privileged communication.

(c) (1) This title shall not apply to any of the following:

(A) Protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5).

(B) A covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A) of this section.

(C) Personal information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration.

(2) For purposes of this subdivision, the definitions of "medical information" and "provider of health care" in Section 56.05 shall apply and the definitions of "business associate," "covered entity," and "protected health information" in Section 160.103 of Title 45 of the Code of Federal Regulations shall apply.

(d) This title shall not apply to activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal

characteristics, or mode of living by a consumer reporting agency, as defined by subdivision (f) of Section 1681a of Title 15 of the United States Code, by a furnisher of information, as set forth in Section 1681s-2 of Title 15 of the United States Code, who provides information for use in a consumer report, as defined in subdivision (d) of Section 1681a of Title 15 of the United States Code, and by a user of a consumer report as set forth in Section 1681b of Title 15 of the United States Code. This paragraph shall only apply to the extent that such activity involving the collection, maintenance, disclosure, sale, communication, or use of such information by that agency, furnisher, or user is subject to regulation under the Fair Credit Reporting Act, Section 1681 et seq., Title 15 of the United States Code and the information is not collected, maintained, disclosed, sold, communicated, or used except as authorized by the Fair Credit Reporting Act.⁵⁷

(e) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102) or the [XX state financial privacy law], and implementing regulations, if it is inconsistent with that act, and only to the extent of the inconsistency.⁵⁸

(f) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.), if it is in conflict with that act.

(g) Notwithstanding a business' obligations to respond to and honor consumer rights requests pursuant to this title:

(1) A time period for a business to respond to any verifiable consumer request may be extended by up to a total of 90 additional days where necessary, taking into account the complexity and number of the requests. The business shall inform the consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay.

(2) If the business does not take action on the request of the consumer, the business shall inform the consumer, without delay and at the latest within the time period permitted of response by this section, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business.

(3) If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. The business shall bear the burden of demonstrating that any verifiable consumer request is manifestly unfounded or excessive.

(h) A business that discloses personal information to a service provider in compliance with this title shall select as service providers entities that are capable of adhering to the restrictions set forth in this title, and enforce compliance in adhering to these restrictions, through effective enforceable contractual obligations and regular evaluation of compliance.⁵⁹ A service provider shall not be liable under this title for the obligations of a business for which it provides

⁵⁷ Since consumer reporting agencies are incompletely covered by FCRA (some also sell information for non-FCRA covered purposes, such as for marketing or advertising), it's important that the FCRA carveout is carefully tailored only to FCRA-covered activities. See, Steven Melendez and Alex Pasternack, *Here Are the Data Brokers Quietly Buying and Selling Your Personal Information*, FAST COMPANY (Mar. 2, 2019), <https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information>.

⁵⁸ Too many state privacy bills inappropriately exempt information covered by the Gramm-Leach-Bliley Act (GLBA). GLBA is weak legislation that primarily provides an opt out of disclosure to third parties and does not provide access or deletion rights. It would be inappropriate to treat sensitive financial data less strictly than other data. Moreover, GLBA explicitly allows for stronger state laws. See GLBA (Sec. 507), which clarifies that states can pass stronger laws. <https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf>.

⁵⁹ This model act adds new oversight responsibilities to companies' existing CCPA requirements to ensure that their service providers are complying with the law.

services as set forth in this title, provided that the service provider shall be liable for its own violations of this title.

(i) This title shall not be construed to require a business to:

(1) Comply with a verifiable consumer request to access, delete, or correct personal information pursuant to subsections 105, 110, 115, or 120 if all of the following are true:

(A) (i) The business is not reasonably capable of linking or associating the request with the personal information, or

(ii) It would be unreasonably burdensome for the business to link or associate the request with the personal information;

(B) The business does not use the information to recognize or respond to the specific consumer who is the subject of the personal information or link or associate the personal information with other personal information about the same specific consumer.

(C) The business does not share the personal information to any third party, or otherwise voluntarily disclose the personal information to any third party other than a service provider except as otherwise permitted in this subsection.

(2) Maintain information in identifiable, linkable or associable form, or to collect, obtain, retain, or access any data or technology, in order to be capable of linking or associating a verifiable consumer request with personal information.⁶⁰

(j) The rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other consumers.

(k) Nothing herein shall apply to the publication of newsworthy information to the public, or to the collection or editing of information for that purpose.

Section 5. Consumer's private right of action.

(a) A consumer who has suffered a violation of this Act may bring a lawsuit against the business that violated this Act. A violation of this Act shall be deemed to constitute an injury in fact to the consumer who has suffered the violation, and the consumer need not suffer a loss of money or property as a result of the violation in order to bring an action for a violation of this Act.

(b) A consumer who prevails in such a lawsuit shall obtain the following remedies:

(1) Damages in an amount not greater than seven hundred and fifty (\$750) per consumer per incident or actual damages, whichever is greater.

(2) Injunctive or declaratory relief, as the court deems proper.

(3) Reasonable attorney fees and costs.

(4) Any other relief the court deems proper.

(c) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

(d) Actions pursuant to this section may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible and the behavior underlying the violations was unintentional, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual

⁶⁰ This paragraph adds new guidance to companies for compliance with the CCPA: the goal is to ensure that companies are not encouraged to reidentify information kept in a bona fide deidentified form in order to respond to consumer requests.

statutory damages or class-wide statutory damages may be initiated against the business. A cure shall not be possible for violations of sections 103, 104, 105, 110, 115, 120, 125, 126, 127, and 128. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement.⁶¹

(e) A consumer bringing an action shall notify the Attorney General within 30 days that the action has been filed.

Section 6. Enforcement.

(a) The State Attorney General, a County District Attorney, or a City Corporation Counsel may bring a civil action, in the name of the people of the state, against any business, service provider, or other person that violated this Act.

(b) Any person, business, or service provider that violates this title may be liable for a civil penalty of up to seven thousand five hundred dollars (\$7,500) for each intentional violation and of up to two thousand five hundred dollars (\$2,500) for each unintentional violation.

Section 7. Construction. This title is intended to further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information. The provisions of this title are not limited to information collected electronically or over the Internet, but apply to the collection and sharing of all personal information collected by a business from consumers. Wherever possible, law relating to consumers' personal information should be construed to harmonize with the provisions of this title, but in the event of a conflict between other laws and the provisions of this title, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.

Section 8. Attorney General regulations.

(a) The Attorney General has the ability to issue regulations including, but not limited to, the following areas:

(1) Detailing and updating as needed the types of information that are "personal information," the definition of "deidentified," "intentionally interacts," and "dark patterns," in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.

(2) Establishing 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.

(3) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights.

(4) Adjusting the monetary threshold in Section 3(c)(1)(A) in January of every odd-numbered year to reflect any increase in the Consumer Price Index.

(5) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to

⁶¹ A limited right to cure could make sense in the context of a private right of action; however, the right to cure is inappropriate in administrative enforcement, because it could provide incentives for companies to break the law. The right to cure in administrative enforcement was removed from the CCPA by Proposition 24.

consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings.

(6) Establishing rules and procedures to further the purposes of subsections 105, 110, 115, and 120 and to facilitate a consumer's or the consumer's authorized agent's ability to obtain personal information, delete personal information, or correct inaccurate personal information pursuant to subsection 130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business' determination that a request for information received by a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business' authentication of the consumer's identity.

(7) Establishing rules and procedures for the following:

(A) To facilitate and govern the submission of a request by a consumer or the consumer's authorized agent to opt out of the use of their personal information to personalize advertising pursuant to Section 103(c).

(B) To govern business compliance with a consumer's opt-out request.

(C) For the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt out of the use of their personal information to personalize advertising.

(8) Establishing rules and procedures to govern business compliance with 100(d), to provide information in an electronic, portable, machine-readable, and readily-useable format or formats to the consumer, or to another business of the consumer's choice.

(b) The Attorney General may update the foregoing regulations, and adopt additional regulations, as necessary to further the purposes of this title.

(c) Before adopting any regulations, the Attorney General shall solicit broad public participation concerning those regulations.

Section 9. Intermediate transactions. If a series of steps or transactions were component parts of a single transaction intended from the beginning to be taken with the intention of avoiding the reach of this title, a court shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title.⁶²

Section 10. Non-waiver. Any provision of a contract or agreement of any kind, including an arbitration agreement, that purports to waive or limit in any way rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable.

Section 11. Construction. This title shall be liberally construed to effectuate its purposes.

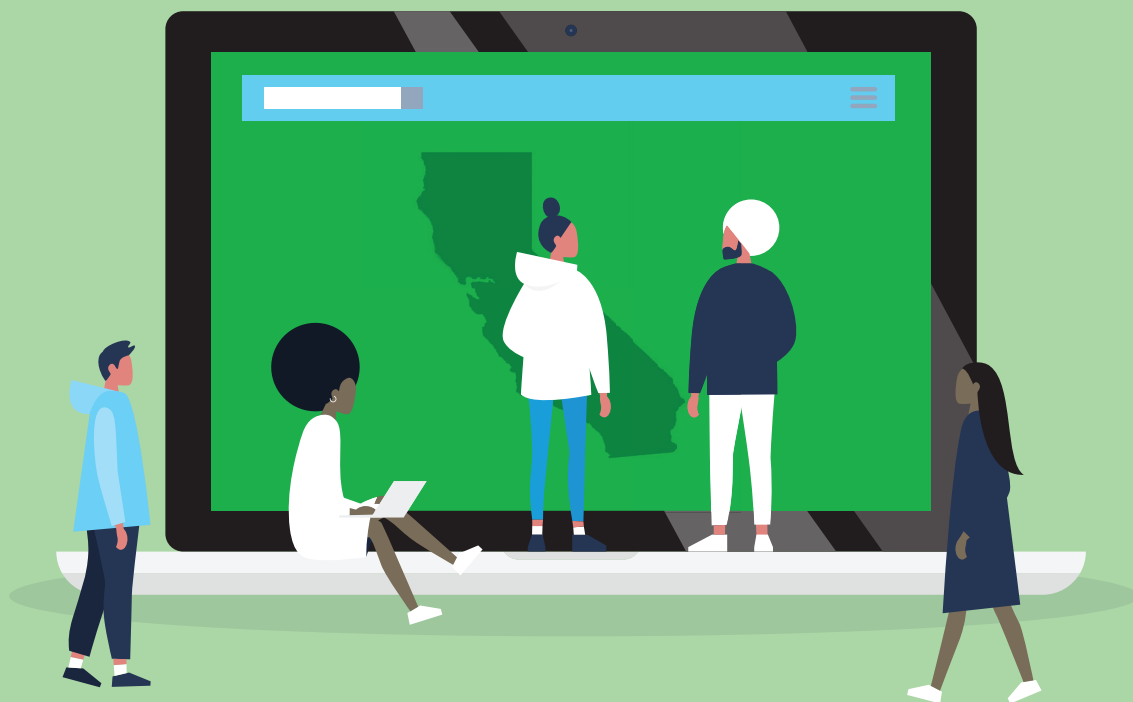
Section 12. Effective date. This title shall be operative one year after it is enacted.

Section 13. Severability.

(a) The provisions of this bill are severable. If any provision of this bill or its application is held invalid, that invalidity shall not affect other provisions or applications that can be given effect without the invalid provision or application.

⁶² This provision is adapted from CPRA § 1798.190 to help prevent non-compliance.

Please contact **Justin Brookman** (justin.brookman@consumer.org) or **Maureen Mahoney** (maureen.mahoney@consumer.org) for more information.



California Consumer Privacy Act: Are Consumers' Digital Rights Protected?

MAUREEN MAHONEY

OCTOBER 1, 2020

Table of Contents

Acknowledgments	3
Executive Summary	4
Introduction	6
Companies' Responsibilities Under the CCPA	8
Methodology	10
Findings	13
Policy Recommendations	44
Conclusion	48
Appendix	49

Acknowledgments

This report is the result of a team effort. Thanks especially to Ben Moskowitz and Leah Fischman for shepherding us through this project, and to Justin Brookman, who provided invaluable assistance throughout. Devney Hamilton, Tom Smyth, and Jill Dimond at Sassafras Tech Collective deserve much of the credit for their work in devising the research study, building the testing tool, and analyzing the results. Kimberly Fountain, Alan Smith, and Daniela Nunez helped us recruit volunteers to participate in the study. Kaveh Waddell made countless contributions and Jennifer Bertsch offered crucial troubleshooting. Karen Jaffe, Camille Calman, Heath Grayson, David Friedman, and Cyrus Rassool improved the report through their review and support. Tim LaPalme and the creative team at Consumer Reports designed the report and helped us present the results more clearly. Finally, our deepest gratitude to the volunteer testers, without whom we would not have been able to conduct this study.

Executive Summary

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 (DNS) 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.¹ As part of the study, 543 California residents made DNS requests to 234 data brokers listed in the California Attorney General's data broker registry. Participants reported their experiences via survey.*

Findings

- 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.
 - Follow-up research primarily focused on the sites in which all three testers did not find the link revealed that at least 24 companies on the data broker registry do not have the required DNS link on their homepage.
 - 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.

¹ Cal. Civ. Code § 1798.135(a)(1).

* On May 13, 2021, the Executive Summary was updated to note that requests were sent to a total of 234 data brokers, not 214.

- 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.*

Policy recommendations

- The Attorney General should vigorously enforce the CCPA to address noncompliance.
- To make it easier to exercise privacy preferences, consumers should have access to browser privacy signals that allow them to opt out of all data sales in one step.
- The AG should more clearly prohibit dark patterns, which are user interfaces that subvert consumer intent, and design a uniform opt-out button. This will make it easier for consumers to locate the DNS link on individual sites.
- The AG should require companies to notify consumers when their opt-out requests have been completed, so that consumers can know that their information is no longer being sold.
- The legislature or AG should clarify the CCPA's definitions of "sale" and "service provider" to more clearly cover data broker information sharing.
- Privacy should be protected by default. Rather than place the burden on consumers to exercise privacy rights, the law should require reasonable data

*On May 13, 2021, the Findings were updated to clarify that the follow-up research that revealed that at least 24 data brokers did not have a DNS link was primarily focused on, but not limited to, the sites in which all three testers failed to find a DNS link.

minimization, which limits the collection, sharing, retention, and use to what is reasonably necessary to operate the service.

Introduction

California consumers have new rights to access, delete, and stop the sale of their information under the landmark California Consumer Privacy Act, one of the first—and the most sweeping—online privacy laws in the country.² However, as the CCPA went into effect in January 2020, it was unclear whether the CCPA would be effective for consumers. Though the CCPA was signed into law in June 2018, many companies spent most of the 2019 legislative session working to weaken the CCPA.³ Early surveys suggested that some companies were dragging their feet in getting ready for the CCPA.⁴ And some companies, including some of the biggest such as Facebook and Google, declared that their data-sharing practices did not fall under the CCPA.⁵ We suspected that this disregard among the biggest and most high-profile entities would filter down to many other participants in the online data markets, and decided to further explore companies' compliance with the CCPA.

The CCPA's opt-out model is inherently flawed; it places substantial responsibility on consumers to identify the companies that collect and sell their information, and to submit requests to access it, delete it, or stop its sale. Even when companies are making a good-faith effort to comply, the process can quickly become unmanageable for consumers who want to opt out of data sale by hundreds if not thousands of different companies. Given that relatively few consumers even know about the CCPA,⁶

² Cal. Civ. Code § 1798 et seq.; Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (Jun. 28, 2018), <https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html>.

³ Press Release, Consumer Reports et al., Privacy Groups Praise CA Legislators for Upholding Privacy Law Against Industry Pressure (Sept. 13, 2019), https://advocacy.consumerreports.org/press_release/joint-news-release-privacy-groups-praise-ca-legislators-for-upholding-privacy-law-against-industry-pressure/.

⁴ *Ready or Not, Here it Comes: How Prepared Are Organizations for the California Consumer Privacy Act?* IAPP AND ONETRUST at 4 (Apr. 30, 2019), https://iapp.org/media/pdf/resource_center/IAPPOneTrustSurvey_How_prepared_for_CCPA.pdf (showing that “[M]ost organizations are more unprepared than ready to implement what has been heralded as the most comprehensive privacy law in the U.S. ever.”)

⁵ Maureen Mahoney, *Many Companies Are Not Taking the California Consumer Privacy Act Seriously—The Attorney General Needs to Act*, MEDIUM (Jan. 9, 2020), <https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb>

⁶ *Report: Nearly Half of U.S.-Based Employees Unfamiliar with California Consumer Privacy Act (CCPA)*, MEDIAPRO (Apr. 30, 2019), <https://www.mediapro.com/blog/2019-eye-on-privacy-report-mediapro/>.

participation is likely fairly low. Anecdotally, those that are aware of the CCPA and have tried to exercise their new privacy rights have struggled to do so.⁷ Through this study we sought to get better insight into the challenges faced by consumers trying to exercise their rights under the CCPA's opt-out model.

This study also seeks to influence the regulations implementing the CCPA, to help ensure that they are working for consumers. The CCPA tasks the California Attorney General's office with developing these regulations, which help flesh out some of the responsibilities of companies in responding to consumer requests.⁸ For example, with respect to opt outs, the regulations clarify how long the companies have to respond to opt-out requests⁹ and outline the notices that need to be provided to consumers.¹⁰ On August 14, 2020, the AG regulations went into effect.¹¹ The CCPA directs the AG to develop regulations as needed to implement the CCPA, consistent with its privacy intent,¹² and the AG has signaled that they plan to continue to consider a number of issues with respect to opt outs.¹³

The AG is also tasked with enforcing the CCPA, and this study is also intended to help point out instances of potential noncompliance. Despite efforts of industry to push back the date of enforcement,¹⁴ the AG has had the authority to begin enforcement since July 1, 2020.¹⁵ Already, the AG's staff has notified companies of potential violations of the CCPA.¹⁶

⁷ Geoffrey Fowler, *Don't Sell My Data! We Finally Have a Law for That*, WASH. POST (Feb. 19, 2020), <https://www.washingtonpost.com/technology/2020/02/06/ccpa-faq/>.

⁸ Cal. Civ. Code § 1798.185(a).

⁹ Cal. Code Regs. tit. 11 § 999.315(e) (2020).

¹⁰ *Id.* at § 999.304-308.

¹¹ State of California Department of Justice, CCPA Regulations (last visited Aug. 15, 2020), <https://www.oag.ca.gov/privacy/ccpa/regs>.

¹² Cal. Civ. Code § 1798.185(b)(2).

¹³ Cathy Cosgrove, *Important Commentary from Calif. OAG in Proposed CCPA Regulations Package*, IAPP (Jul. 27, 2020), <https://iapp.org/news/a/important-commentary-from-calif-oag-in-proposed-ccpa-regulations-package/>.

¹⁴ See, e.g. Andrew Blustein, *Ad Industry Calls for Delayed Enforcement of CCPA*, THE DRUM (Jan. 29, 2020), <https://www.thedrum.com/news/2020/01/29/ad-industry-calls-delayed-enforcement-ccpa>; Association of National Advertisers, *ANA and Others Ask for CCPA Enforcement Extension* (Mar. 18, 2020), <https://www.ana.net/blogs/show/id/rr-blog-2020-03-ANA-and-Others-Asks-for-CCPA-Enforcement-Extension>.

¹⁵ Cal. Civ. Code § 1798.185(c).

¹⁶ Cosgrove, *Important Commentary*, *supra* note 13; Malia Rogers, David Stauss, *CCPA Update: AG's Office Confirms CCPA Enforcement Has Begun*, JD SUPRA (Jul. 14, 2020), <https://www.jdsupra.com/legalnews/ccpa-update-ag-s-office-confirms-ccpa-55113/>.

Our study revealed flaws in how companies are complying with CCPA and with the CCPA itself. Many companies are engaging in behavior that almost certainly violates the CCPA. But even if companies were complying completely in good faith, the CCPA makes it incredibly difficult for individuals to meaningfully exercise control over the sale of their personal information. Indeed, the conceit that consumers should have to individually opt out of data sale from each of the hundreds of companies listed on the California data broker registry—let alone the hundreds or thousands of other companies that may sell consumers' personal information—in order to protect their privacy is absurd. Over half of the survey participants expressed frustration with the opt-out process, and nearly half were not even aware if their requests were honored by the recipient. The Attorney General should aggressively enforce the current law to remediate widespread noncompliant behavior, but it is incumbent upon the legislature to upgrade the CCPA framework to protect privacy by default without relying upon overburdened consumers to understand complex data flows and navigate heterogeneous privacy controls.

Companies' responsibilities under the CCPA

Under the CCPA, companies that sell personal information (PI) to third parties must honor consumers' requests to opt out of the sale of their PI.¹⁷ The CCPA has a broad definition of personal information, which includes any data that is reasonably capable of being associated with an individual or household—everything from Social Security numbers, to biometric information, or even browsing history. This also covers browsing history or data on a shared computer (in other words, not data that can be exclusively tied to a single individual)¹⁸—further highlighting that opt outs need not be verified to a particular individual. The CCPA's definition of sale covers any transfer of data for valuable consideration,¹⁹ intended to capture data that is shared with third parties for behavioral advertising purposes.²⁰

¹⁷ Cal. Civ. Code § 1798.120(a).

¹⁸ *Id.* at § 1798.140(o)(1).

¹⁹ *Id.* at § 1798.140(t)(1).

²⁰ California Senate Judiciary Committee, SB 753 Bill Analysis at 10 (Apr. 22, 2019), https://leginfo.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201920200SB753. The analysis excerpts a letter from the sponsors of AB 375, Californians for Consumer Privacy, opposing SB 753, legislation proposed in 2019 that would explicitly exempt cross-context targeted advertising from the CCPA: "SB 753 proposes to amend the definition of 'sell' in Civil Code Section 1798.140 in a manner that will break down th[is] silo effect As a result, even if a consumer opts-out of the sale of their data, this proposal would allow an advertiser to combine, share and proliferate data throughout the advertising

The CCPA places certain responsibilities on these companies to facilitate the opt outs. They are required to provide a “clear and conspicuous link” on their homepage so that consumers can exercise their opt-out rights.²¹ The CCPA pointedly creates a separate process for exercising opt-out rights than it does for submitting access and deletion requests—the latter requires verification to ensure that the data that is being accessed or deleted belongs to the correct person.²² In contrast, for opt outs, verification is not required.²³ Importantly, companies may not use the information provided by the opting out consumer for any other purpose.²⁴ The CCPA also directs the AG to design and implement a “Do Not Sell” button to make it easier for consumers to opt out.²⁵

The AG's regulations outline additional requirements. Companies must post a prominent link labeled “Do Not Sell My Personal Information,” which must lead the consumer to the required interactive form to opt out.²⁶ (The AG declined to finalize a design to serve as an opt-out button.)²⁷ CCPA regulations clarify that “A request to opt-out need not be a verifiable consumer request. If a business, however, has a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent, the business may deny the request[,]” and the company, if it declines a request for that reason, is required to notify the consumer and provide an explanation.²⁸ Companies must honor consumers' requests to opt out within 15 business days²⁹ (in contrast to 45 days for deletion and access requests).³⁰

economy. The proposed language will essentially eliminate the silo effect that would occur pursuant to the CCPA, which allows for targeted advertising but prevents the proliferation of a consumer's data throughout the economy.”

²¹ Cal. Civ. Code § 1798.135(a)(1).

²² *Id.* at § 1798.140(y).

²³ *Id.* at § 1798.135.

²⁴ *Id.* at § 1798.135(a)(6).

²⁵ *Id.* at § 1798.185(a)(4)(C).

²⁶ Cal. Code Regs. tit. 11 § 999.315(a) (2020).

²⁷ State of California Department of Justice, Final Statement of Reasons at 15 (June 1, 2020), <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor.pdf> [hereinafter FSOR].

²⁸ *Id.* at § 999.315(g).

²⁹ *Id.* at § 999.315(e).

³⁰ Cal. Civ. Code § 1798.130(a)(2).

Methodology

In this section, we describe our sample, the research exercise, survey, and method of analysis.

Selecting Companies to Study

To select the companies to study, we used the new California data broker registry,³¹ which lists companies that sell California consumers' personal information to third parties, but do not have a direct relationship with the consumer.³² Reining in data brokers—which profit from consumers' information but typically do not have a direct relationship with them—was a primary purpose of the CCPA. Through the opt out of sale, the authors of the CCPA sought to dry up the pool of customer information available on the open market, disincentivize data purchases, and make data brokering a less attractive business model.³³

The data broker registry was created in order to help consumers exercise their rights under the CCPA with respect to these companies. Companies that sell the personal information of California consumers but don't have a relationship with the consumer are required to register with the California Attorney General each year.³⁴ The AG maintains the site, which includes the name of the company, a description, and a link to the company's website, where the consumer can exercise their CCPA rights.³⁵ The data broker registry is particularly important because many consumers do not even know which data brokers are collecting their data, or how to contact them. Without the data broker registry, exercising CCPA rights with respect to these companies would be near impossible.

For many consumers, data brokers exemplify some of the worst aspects of the ad-supported internet model, giving participants in the study a strong incentive to opt out of the sale of their information. Nearly everything a consumer does in the online or even physical world can be collected, processed, and sold by data brokers. This could

³¹ State of California Department of Justice, Data Broker Registry (last visited August 10, 2020), <https://oag.ca.gov/data-brokers> [hereinafter DATA BROKER REGISTRY].

³² Cal. Civ. Code § 1798.99.80(d).

³³ Nicholas Confessore, *The Unlikely Activists Who Took on Silicon Valley—And Won*, N.Y. TIMES (Aug. 14, 2018), <https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html>.

³⁴ DATA BROKER REGISTRY, *supra* note 31.

³⁵ *Id.*

include location data picked up from apps, purchase history, browsing history—all combined to better understand and predict consumer behavior, and to guide future purchases. Data brokers can purchase information from a variety of sources, both online and offline, including court records and other public documents. The inferences drawn can be startlingly detailed and reveal more about a consumer than they might realize. Consumers can be segmented by race, income, age, or other factors.³⁶ The information collected can even provide insight whether a consumer is subject to certain diseases, such as diabetes, or other insights into health status.³⁷ All of this data might be used for marketing, or it could be used to assess consumers' eligibility for certain opportunities, either due to loopholes in consumer protection statutes such as the Fair Credit Reporting Act, or because of a lack of transparency and enforcement.³⁸

Sampling

We randomly sampled from all of the 234 brokers in California's data broker registry as of April 2020. In the final analysis, we included three sample requests for each of 214 brokers, totaling 642 DNS requests made by 403 different participants. Though we did not have enough testers to ensure that every company on the data broker registry received three tests, a sample of 214 of 234 companies in the database is more than sufficient to represent the different types of processes for all companies. In our initial investigation into DNS requests, in which we submitted our own opt-out requests, we found that three requests were generally enough to uncover the different processes and pitfalls for each company. However, in order to analyze and generalize success rates of DNS requests depending on different processes, a follow-up study should be conducted toward this end. In cases in which testers submitted more than three sample requests for a company, we randomly selected three to analyze.

Participants were not representative of the general population of California. As this initial study was designed to understand the landscape of different data brokers and their DNS request processes, we decided to use a convenience sample. Participants were

³⁶ *Data Brokers: A Call for Transparency and Accountability*, FED. TRADE COMM'N at 24 (May 2014), <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.

³⁷ *Id.* at 25.

³⁸ *Big Data, A Big Disappointment for Scoring Consumer Credit Risk*, NAT'L CONSUMER LAW CTR. at 26 (Mar. 2014), <https://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf>; *Spokeo to Pay \$800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA*, FED. TRADE COMM'N (June 12, 2012), <https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed>.

recruited through CR's existing membership base, promotion by partner organizations, and through social media outreach. Participation was limited to California residents. Therefore, participants were likely better informed about the CCPA and digital privacy rights than the general population. The study was conducted in English, excluding those not fluent in English. Participation in the study was not compensated.

Research Exercise

In the study exercise, participants were randomly assigned a data broker from the registry using custom software, and were emailed with instructions to attempt making a DNS request to that data broker. Participants could, and many did, test more than one data broker. On average, participants performed 1.8 test requests. For each request, the participant was given a link to the data broker's website and its email address. They were instructed to look for a "Do Not Sell My Personal Info" (or similar) link on the broker's site and to follow the instructions they found there, or to send an email to the email address listed in the data broker registration if they did not find the link. Participants then reported their experience with the DNS process via survey immediately after their first session working on the request. Participants were prompted by email to fill out follow-up surveys at one week and 21 days (approximately 15 business days) to report on any subsequent steps they had taken or any updates on the status of their request they had received from the data broker. (See Appendix, Section A for a diagram of the participant experience of the exercise).

Survey Design

The survey aimed to capture a description of a participant's experience in making a DNS request. We approached the design of this study as exploratory to understand the DNS process and as a result, asked mixed qualitative and quantitative questions. The survey branched to ask relevant questions based on what the participant had reported thus far. These questions involved mostly optional multi-select questions, with some open-ended questions. Because the survey included optional questions, not all samples have answers to every question. We omitted from the analysis samples in which there was not enough applicable information for the analysis question. Participants were encouraged to use optional "other" choices with open-ended text. We also offered participants the ability to send in explanatory screenshots. Where participants flagged particularly egregious behaviors, we followed up by having a contractor collect screenshots, or we followed up ourselves to collect screenshots.

Data Analysis

We used both quantitative and qualitative methods for analysis. To answer the questions of time spent and ability to find the DNS request link, we aggregated the responses. To understand the result of request processes, we relied on answers to both open-ended text questions and multi-select questions related to status in order to code and tally the results.

For open response text, we used a qualitative thematic analysis approach where we read the text and coded inductively for themes.

Limitations

This was an exploratory study designed to uncover different DNS processes. As such, our results are not experimental and cannot conclusively establish the efficacy of these DNS processes. Some questions in the survey were meant to capture the participants' experiences, such as "Did the [broker] confirm that they are not selling your data?" For example, a confirmation email could have been sent to the consumer's junk mail folder—so the consumer may not have been aware of the confirmation, even if the company had sent one. Also, consumers may not have understood brokers' privacy interfaces, and conflated DNS requests with other rights; for example, some consumers may have submitted access or deletion requests when they meant to submit opt-out requests. That said, given that the CCPA is designed to protect consumers, consumers' experiences have value in evaluating the CCPA. In addition, because of our convenience sample, it is likely that the broader population may generally drop off from these processes earlier (or not engage at all) due to constraints such as time or lack of technology skill.

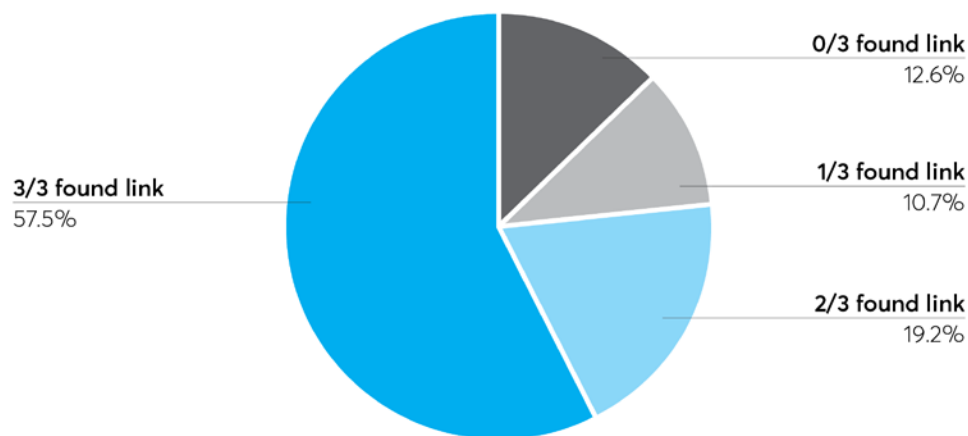
Findings

CCPA opt outs should be simple, quick, and easy. However, we found that many companies failed to meet straightforward guidelines—posing significant challenges to consumers seeking to opt out of the sale of their information. Below, we explore the challenges consumers faced in opting out of the sale of their information from data brokers.

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 often found it difficult to opt out of the sale of their information, in large part because opt-out links either weren't visible on the homepage or weren't there at all. Nearly half the time, at least one of three of our testers failed to find the link, even though they were expressly directed to look for it. This suggests that either the link wasn't included on the homepage, or that it was not listed in a “clear and conspicuous” manner, both of which are CCPA requirements.

Brokers by number of testers who found DNS link



Companies on the California data broker registry by definition sell customer PI to third parties and should have a Do Not Sell link on their homepage in order to comply with the CCPA. Under California law, every data broker is required to register with the California Attorney General so that their contact information can be placed on the registry.³⁹ A data broker is defined as a “business that knowingly collects *and sells* to third parties the personal information of a consumer with whom the business does not have a direct relationship.”⁴⁰ [emphasis added] The definitions of “sell,” “third parties,”

³⁹ Cal. Civ. Code §1798.99.82.

⁴⁰ *Id.* at § 1798.99.80(d).

and “personal information” all mirror those of the CCPA, which helps to ensure that the registry effectively aids consumers in exercising their CCPA rights with respect to these entities.⁴¹

While it is true that some data brokers may enjoy certain exemptions from AB 1202, companies selling customer information still are obligated to put up Do Not Sell links. In response to requests to the AG during the rulemaking process to “Amend [the CCPA rules] to explain that businesses must provide notice of consumer rights under the CCPA only where such consumer rights may be exercised with respect to personal information held by such business. Consumer confusion could result from explanation of a certain right under the CCPA when the business is not required to honor that right because of one or more exemptions[,]” the AG responded that “CCPA-mandated disclosures are required even if the business is not required to comply with the consumers’ exercise of their rights.”⁴²

The homepage means the first, or landing, page of a website. It is not sufficient to place a link to a privacy policy on the first page, that leads to the DNS link—the link on the homepage must be labeled “Do Not Sell My Personal Information.”⁴³ The CCPA clarifies that “homepage” indeed means “the introductory page of an internet website and any internet web page where personal information is collected.”⁴⁴ The AG further explains that a link to a privacy policy is not sufficient to constitute a Do Not Sell link: “The CCPA requires that consumers be given a notice at collection, notice of right to opt out, and notice of financial incentive. These requirements are separate and apart from the CCPA’s requirements for the disclosures in a privacy policy.”⁴⁵

The CCPA does note that a company need not include “the required links and text on the homepage that the business makes available to the public generally[,]” if it establishes “a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for

⁴¹ *Id.* at § 1798.99.80(e)-(g).

⁴² State of California Department of Justice, Final Statement of Reasons, Appendix A, Response #264 (June 1, 2020), <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor-appendix-a.pdf> [hereinafter “FSOR Appendix”].

⁴³ Cal. Civ. Code § 1798.135(a)(1).

⁴⁴ *Id.* at § 1798.140(l).

⁴⁵ FSOR Appendix, *supra* note 42, Response #105.

California consumers and not the homepage made available to the public generally.”⁴⁶ We limited our outreach to participants who had previously told us they were California residents, though we cannot say for sure that they were in California at the time they completed our survey. Occasionally California employees supplemented survey responses by capturing additional screenshots, sometimes from within California, sometimes without. Technically, the CCPA gives rights to Californians even when they are not physically present within the state, though it is possible that data brokers treat users differently based on approximate geolocation derived from their IP address.⁴⁷

If testers are unable to find a DNS link on the homepage even if it is there, that suggests that it may not be placed in a “clear and conspicuous” manner, as required by the CCPA. If testers that have been provided instructions and are looking for an opt-out link in order to complete a survey are unable to find a link, it is less likely that the average consumer, who may not even know about the CCPA, would find it.

Testers that did not find an opt-out link but continued with the opt-out process anyway often faced serious challenges in exercising their opt-out rights. We instructed these testers to email the data broker to proceed with the opt-out request. This considerably slowed down the opt-out process, as a consumer had to wait for a representative to respond in order to proceed. And often, the agent provided confusing instructions or was otherwise unable to help the consumer with the opt-out request. For example, we received multiple complaints about Infinite Media. Infinite Media did not have a “Do Not Sell” link on its homepage (see Appendix, Section B for a screenshot). Further, its representative puzzled testers by responding to their opt-out emails with confusing questions—such as whether they had received any marketing communications from the company—in order to proceed with the opt out.

I am with Infinite Media/ Mailinglists.com and have been forwarded your request below. We are a list brokerage company and do not compile any data. We do purchase consumer data on behalf of some of our clients and we do work with a large business compiler and purchase data from them as well. Can you tell me if you received something to your home or business address? If home address I will need your full address info. If business, then please send your company name and address. Also do you work from home? Lastly who was it that you received the mail piece, telemarketing call or email from? I need to know the

⁴⁶ Cal. Civ. Code § 1798.135(b).

⁴⁷ Cal. Civ. Code § 1798.140(g).

name of the company that contacted you so I can track back where the data came from and contact the appropriate list company and have you removed from their data file so they don't resell your name any longer.

Given the number of unsolicited communications that consumers receive, it was difficult for the testers to answer and frustrated their efforts to opt out. One consumer reached out to us after receiving the message: "I don't know how to reply - since I have not received any marketing item from them, ca[n]'t give them the name of outfit/person they're asking about. Our landline does get an annoying amount of robocalls and telemarketing calls but I can't tell who/what they're from...."

The agent's confusing response itself is a potential CCPA violation, as the CCPA requires companies to "[e]nsure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Section 1798.120 [regarding the right to opt out] and this section and how to direct consumers to exercise their rights under those sections."⁴⁸ Instead of directing consumers to the interactive form to opt out, the agent confused and frustrated consumers seeking to exercise their CCPA opt-out rights by asking them questions that they could not answer.

At least 24 companies on the data broker registry do not have a DNS link anywhere on their homepages.

Follow-up research primarily focused on the sites in which all three testers did not find the link revealed that at least 24 companies do not have the required DNS link on their homepage (see Appendix, Section B for screenshots).^{49*} For example, some companies provide information about CCPA opt-out rights within its privacy policy or other document, but offer no indication of those rights on the homepage. Since consumers typically don't read privacy policies,⁵⁰ this means that unless a consumer is familiar with the CCPA or

⁴⁸ Cal. Civ. Code § 1798.135(a)(3).

⁴⁹ These companies are: Admarketplace.com, Big Brook Media, Inc., Blue Hill Marketing Solutions, Comscore, Inc., Electronic Voice Services, Inc., Enformion, Exponential Interactive, Gale, GrayHair Software, LLC, Infinite Media Concepts Inc, JZ Marketing, Inc., LeadsMarket.com LLC, Lender Feed LC, On Hold-America, Inc. DBA KYC Data, Outbrain, PacificEast Research Inc., Paynet, Inc., PossibleNow Data Services, Inc, RealSource Inc., Social Catfish, Spectrum Mailing Lists, SRAX, Inc., USADATA, Inc., and zeotap GmbH.

* On May 13, 2021, the report was updated to clarify that this follow-up research was primarily focused on, but not limited to, the sites in which all three testers failed to find a DNS link.

⁵⁰ Brooke Axier et al., *Americans' Attitudes and Experiences with Privacy Policies and Laws*, PEW RESEARCH CTR. (Nov. 15, 2019),

is specifically looking for a way to opt out, they likely won't be able to take advantage of the DNS right.

For example, the data broker Outbrain doesn't have a "Do Not Sell My Personal Information" link on its homepage. The consumer can click on the "Privacy Policy" link at the bottom of the page, which sends the consumer through at least six different steps in order to opt out of the sale of their information on that device. (The consumer can cut out several steps by clicking on "Interest-Based Ads" on the homepage.) If a consumer would like to opt out on their phone, they would have to go through another process. And if the consumer clears their cookies, they would need to opt out again. As one consumer told us, "It was not simple and required reading the 'fine print.'" Below, we show the opt-out process through screenshots (See pages 20-21):

STEP 1 The "Privacy Policy" link takes the consumer to the "Privacy Center." Consumers can click on panel 6, "California Privacy Rights," **STEP 2.**

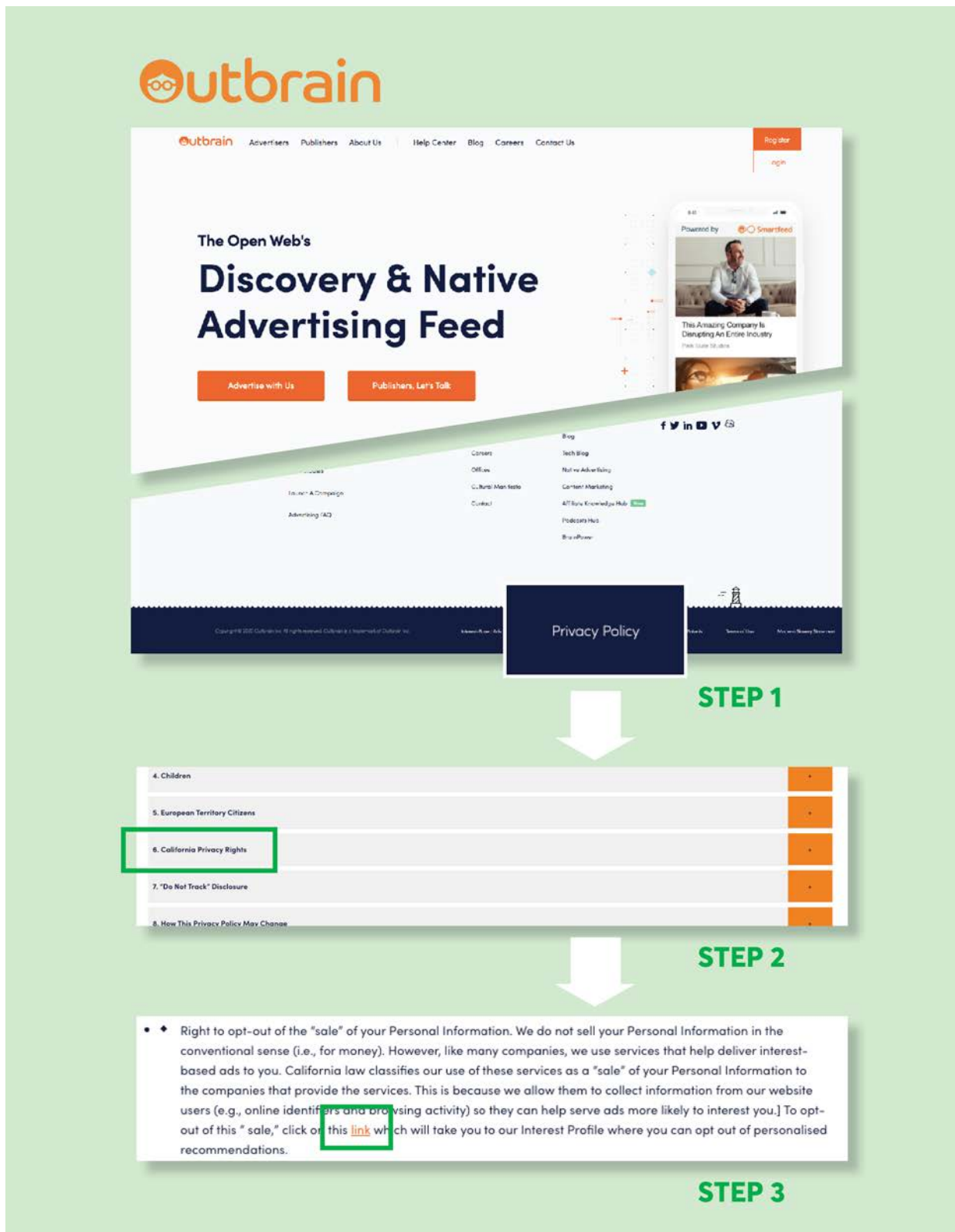
Clicking on "California Privacy Rights" opens up a text box **STEP 3**, that includes a bullet on the "Right to opt-out of the 'sale' of your Personal Information." That section includes a very small hyperlink to "opt out of personalised recommendations."

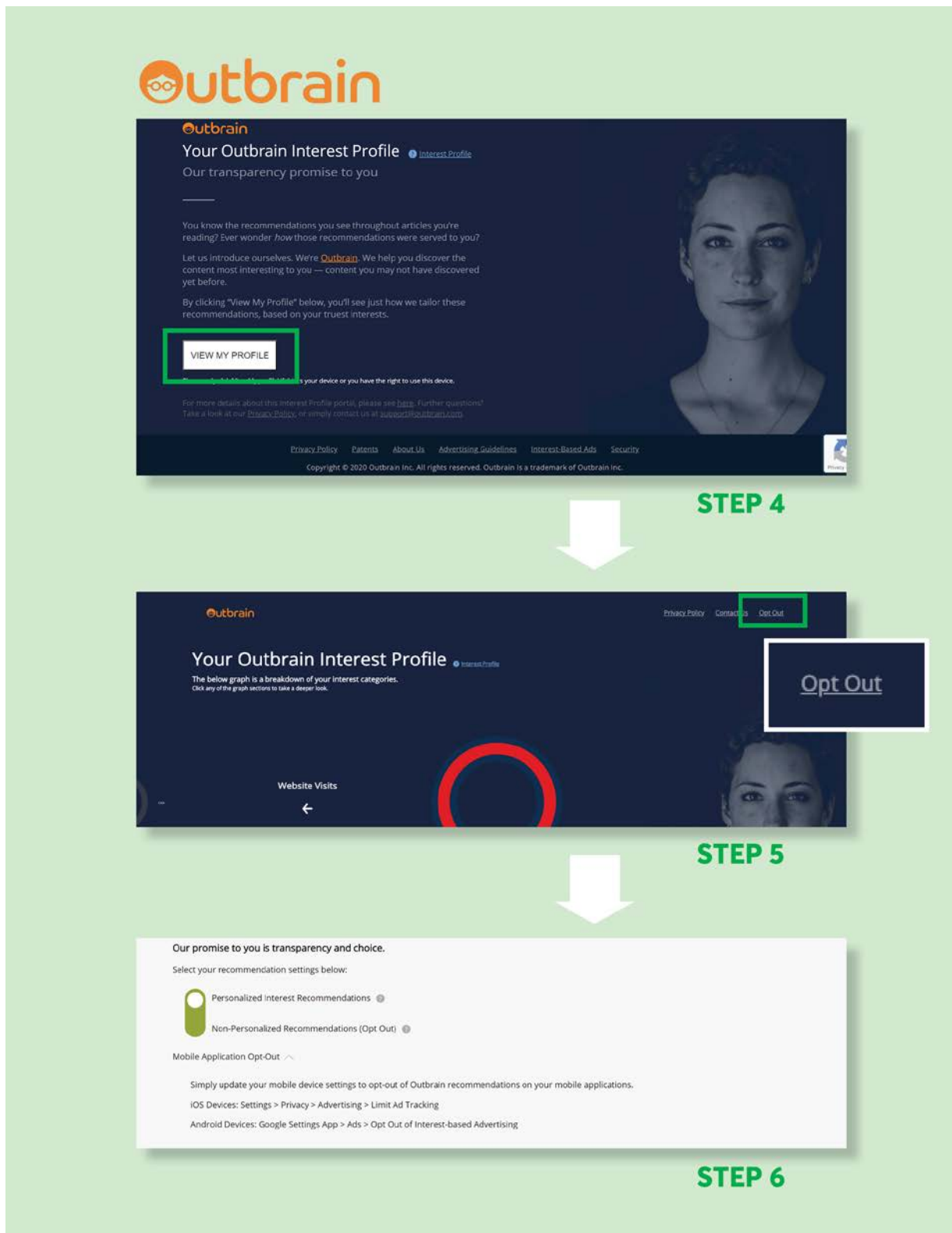
Clicking on that link takes the consumer to another to a page titled "Your Outbrain Interest Profile," **STEP 4.** (The consumer can also reach this page by clicking on "Interest-Based Ads" on the homepage.)

The consumer can then click on "View My Profile," which takes them to a new page that provides a breakdown of interest categories. In the upper right-hand corner, there is a small, gray-on-black link to "Opt Out," **STEP 5.**

This finally takes the consumer to a page where they can move a toggle to "opt out" of interest-based advertising, **STEP 6**, though it is unclear whether turning off personalized recommendations is the same as opting out of the sale of your data under the CCPA. One tester remarked on the confusion, "There were many links embedded in the Outbrain Privacy Center page. I had to expand each section and read the text and review the links to determine if they were the one I wanted. I am not sure I selected "DO not Sell" but I did opt out of personalized advertising."

<https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/> (Showing that only 9% of adults read the privacy policy before accepting the terms and conditions, and 36% never do.).





Even those steps don't opt consumers out for all devices. There are separate instructions for opting out on a mobile device, and for bulk opting out of ad targeting through a voluntary industry rubric (though again, it isn't clear if this is the same as stopping sale under the CCPA).

Instead of leaving consumers to navigate through multiple steps to opt out, Outbrain should have included a link that says "Do Not Sell My Personal Information" on the homepage, and then immediately taken the consumer to a page with the toggle to opt out. The AG's regulations require companies to provide "two or more designated methods for submitting requests to opt out, including an *interactive form* accessible via a clear and conspicuous link titled "Do Not Sell My Personal Information," on the business's website or mobile application."⁵¹ (emphasis added). This suggests that the opt out is intended to involve nothing more than filling out a short form, one that is quickly and easily accessed from the homepage.

For an additional five companies, all three testers were unable to find the DNS link, suggesting that they may not be listed in a "clear and conspicuous" manner as required by the CCPA.

All three testers were unable to find the DNS link for an additional five companies (see Appendix, Section C for screenshots).⁵² For example, all three testers failed to find the Do Not Sell link for the data broker Freckle I.O.T. Ltd./PlacelQ. First, the website <https://freckleiot.com/>, which is listed on the data broker registry, automatically redirects to <https://www.placeiq.com/>, where consumers are confronted with a dark pattern banner at the bottom of the screen that only offers the option to "Allow Cookies" (the banner also states that "scrolling the page" or "continuing to browse otherwise" constitutes consent to place cookies on the user's device.) If the user does not click "Allow," the banner stays up, and it obscures the "CCPA & Do Not Sell" link (for more on mandating cookie acceptance as a condition of opting out, see *infra*, p. 30).

⁵¹ Cal. Code Regs. tit. 11 § 999.315(a) (2020).

⁵² These companies are: AcademixDirect, Inc., Fifty Technology Ltd, Freckle I.O.T. Ltd./PlacelQ, Marketing Information Specialists, Inc., and Media Source Solutions. Two of the companies in which all three testers could not find the DNS link did not appear to have a functioning website at all: Elmira Industries, Inc. and Email Marketing Services, Inc.

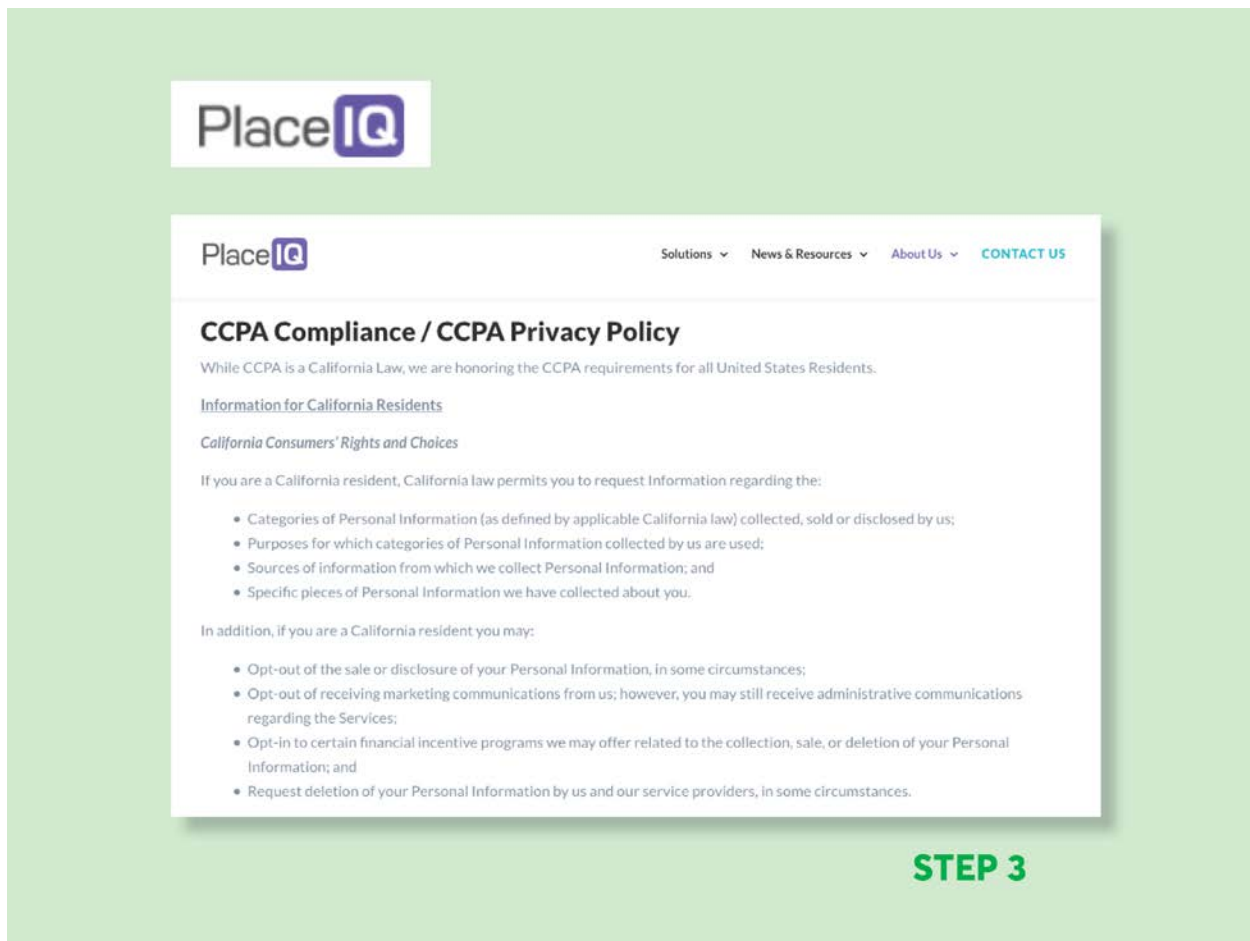
California Consumer Privacy Act: Are Consumers' Digital Rights Protected?

The diagram illustrates the process of accessing the California Consumer Privacy Act (CCPA) options on the PlaceIQ website. It is divided into two main steps:

STEP 1: A callout box labeled "Allow cookies" points to the "Allow cookies" button on the website's cookie banner.

STEP 2: A callout box labeled "Consumer Options: Privacy Policy, CCPA & Do Not Sell" points to the "CCPA & Do Not Sell" link in the "Consumer Options" section of the website's footer.

The website screenshot shows the PlaceIQ logo, navigation links (Solutions, News & Resources, About Us, CONTACT US), a COVID-19 research announcement, a company history section, partner logos (Oracle Data Cloud, Experian, comscore, Marketing Evolution), a cookie banner, and a footer with contact information, privacy partners (NAES, MMA, IAB, DPAA), news & insights, solutions, and company information. The "Consumer Options" section in the footer is highlighted, showing links to the Privacy Policy and CCPA & Do Not Sell.



After clicking “Allow Cookies,” revealing the full homepage, then, the user must scroll all the way down to the bottom of the homepage to get to the CCPA & Do Not Sell link (also note that the link is not labeled “Do Not Sell My Personal Information” as required by the CCPA).

Since users must accept cookies to remove the pop up and reveal the link, and the link was buried at the very bottom of the page, it is not surprising that none of the consumers testing the site were able to find the opt-out link, even though they were looking for it. This shows how confusing user interfaces can interfere with consumers' efforts to exercise their privacy preferences, and how important it is for companies to follow CCPA guidance with respect to “clear and conspicuous” links. Without an effective mechanism to opt out, consumers are unable to take advantage of their rights under the law.

Some DNS processes involved multiple, complicated steps to opt out, including downloading third-party software, raising serious questions about the workability of the CCPA for consumers.


While companies might need to collect some information from consumers in order to identify consumer records—for example, data brokers typically sell records by email⁵³—some companies asked for information that was difficult to obtain, or required consumers to undergo onerous processes in order to opt out. There were a variety of formats for making DNS requests such as instructions to download a third-party app, instructions to send an email, or no instruction or clearly visible opt-out link at all (we instructed our participants to send an email to the email address in the registry if they could not find the opt-out link).

The most common type of DNS process involved filling out a form with basic contact information such as name, email, address, and phone number. However, several companies, such as those tracking location data, asked consumers to provide an advertising ID and download a third-party app to obtain it. This was confusing and labor intensive for many testers.

Companies that defaulted to pushing consumers to install an app to obtain the ID discouraged some consumers from opting out—downloading a separate app to their phone was a step too far. One tester of data broker Freckle I.O.T./PlacelQ reported, “Too technically challenging and installing an app on your phone shouldn't be required.” The consumer further notes that the Freckle I.O.T./PlacelQ opt-out process would be impossible for consumers without a mobile phone. “The process also could not be completed on a computer, so anyone without a smartphone would not be able to complete the request this way.” In nearly half (8 out of 20) of cases, consumers declined to provide an advertising or customer ID.

Other consumers found themselves unable to submit opt-out requests because the company required an IP address. For example, four testers reported that they could not complete their request to Megaphone LLC because they were asked to provide their IP address. In this case, it was likely that testers declined to proceed further because they could not figure out how to obtain their IP address. The screenshot on page 25 shows that Megaphone's opt-out form includes a required question, “What is your IP address?”

⁵³ For example, TowerData claims that clients can obtain “data on 80% of U.S. email addresses.” TowerData (last visited Sept. 13, 2020), <http://intelligence.towerdata.com/>.




Megaphone


Advertisers Publishers

About Press Log in Contact us

Modern podcast technology for publishers and advertisers.



I'm an



I'm a

☐ Do not sell my personal information

By using this site, you agree to the use of cookies by Megaphone and our partners to provide the best experience, analyze site use and assist in our marketing efforts. [Privacy Policy](#)

Close

☐ Do not sell my personal information

E

C

STEP 1

CCPA Request

California residents may use this form to submit a request to opt out of the "sale" of their personal information to third parties.

The only personal information that Megaphone collects is a user's IP address and user agent, which is information about the user's device, browser, and platform of origin. We require California residents to submit their IP address and the platform from which they download podcasts because, without that information, we have no way to act on their requests.

* Name


* Email address

* What is your IP address?

* What is your user agent?

- Select -

☐ I'm not a robot


reCAPTCHA
Privacy Terms

SUBMIT

STEP 2

Some data brokers asked consumers to submit information that they were reluctant to provide, such as a photo of their government ID.

Some companies asked consumers to verify their identities or residence, for example by providing their government ID number, an image of their government ID, or a “selfie.” Testers reported that a few asked knowledge-based authentication questions, such as previous addresses or a home where someone has made a payment.

The histogram on page 27 shows the relative frequency of types of information testers were asked for and steps they were asked to take as part of their DNS request.⁵⁴

⁵⁴ All requests are combined in this analysis (rather than broken down by broker), reflecting the overall experience of making DNS requests under the CCPA. For reporting what is asked of testers in the process, we used the answers to multi-select questions about what information testers were asked for and/or refrained from providing, and multi-select questions about actions they were asked to take and/or refrained from taking. As some of the action options were redundant of the information options, we combined a non-repeat subset of the action options with the information options. We also used text answers in these parts of the survey in qualitative analysis about the variety of DNS processes.

DNS Request Processes*



A company needs some personal information in order to process a “Do Not Sell” request—if a data broker sells records linked to email addresses, it needs to know the email address about which it is no longer allowed to sell information. Nevertheless,

* On May 13, 2021, this chart was corrected to note that the number of requests to send or receive email were 209, not 204; and that several consumers were asked to “Provide a selfie,” not “Provide a profile.”

companies are not allowed to mandate identity verification to process a DNS request under CCPA, and requesting sensitive information provided friction and led many consumers to abandon their efforts to opt out. See, for example, the Melissa Corporation, which requested consumers to provide “verification of California residency and consumer’s identity.”

The screenshot shows a web form for the Melissa Corporation. At the top is the Melissa logo. Below it is a section titled "California Consumer Privacy Act Notice (Show Details...)" with three checkboxes: "Right to Know", "Right to Opt-Out of Sale of Personal Information", and "Right to Delete". Below this is a section titled "Please provide the information that you want to inquire." with various input fields: "First Name:", "Last name:", "Phone:", "Mobile Phone:", "Email:", "Address:", "Address2:", "City", "State:" (a dropdown menu showing "CA"), and "ZIP/Postal Code:". Below these fields is a section titled "*Attach verification of California residency and consumer's identity (Supported files: .pdf, .jpg, .jpeg, .gif, .bmp, .png, .tif)". This section contains three "Choose File" buttons, each followed by the text "No file chosen". A green rectangular box highlights this entire section. At the bottom of the form is a blue "Submit" button.

The CCPA only covers California consumers,⁵⁵ and the statute and implementing regulations are ambiguous on how companies may require consumers to prove they are

⁵⁵ Cal. Civ. Code § 1798.140(g).

covered by the law. However, asking for proof of residence added difficulty to the opt-out process, especially as other companies achieved this objective by requesting the consumer's name, address, and email.

West Publishing Corporation, part of Thomson Reuters, also asked consumers to submit to identity verification to complete the opt-out process. As shown in the screenshot below, the site requires consumers to submit a photo of their government ID and a selfie, as well as their phone number. Once the phone number is submitted, the site sends a text to help facilitate the capture of these documents through the user's mobile phone.

The screenshot shows a web form for identity verification. At the top, there is a logo for 'the answer company THOMSON REUTERS'. Below this, a text block explains the need for identity verification and states that data will be deleted after the transaction is completed. The form contains three main sections: 'Drivers License *' with a status of 'Incomplete', 'Facial Similarity Snapshot *' with a status of 'Incomplete', and 'Mobile phone *' with a text input field containing '(201) 555-0123' and a US flag icon. A green button labeled 'Continue on Mobile' is at the bottom.

While these requests might be appropriate in the case of an access or deletion request, where identity verification is important to make sure that data is not being accessed or

deleted without the consumer's consent, in the case of an opt out, it frustrates consumers' objectives to stop the sale of their personal information and does not provide additional privacy protection.

Some data brokers led consumers to abandon opt outs by forcing them to accept cookies.

As the CCPA went into effect in January 2020, some California consumers noticed that when they visited websites, they were asked to opt in to the use of cookies—and expressed confusion about what they were being asked to do. These notices have been common in Europe in response to the e-Privacy Directive, and more recently the Global Data Protection Regulation, though privacy advocates have been deeply critical of the practice: companies often use dubious dark patterns to nudge users to click “OK,” providing the veneer, but not the reality of, knowing consent.⁵⁶ The expansion of cookie banners in California was borne out in our study. Sixty-six of the 214 brokers had at least one consumer report a request or mandate to accept cookies as part of the DNS process. In some cases, for example if a company only tracks online using cookies, it may be reasonable for a site to set a non-unique opt-out cookie to allow the opt out to persist across multiple sessions. But the examples we saw were confusing to consumers, and did not clearly convey that a cookie was going to be placed for the limited purpose of enabling the opt out of cross-site data selling. And, as previously noted, sometimes the cookie consent banners obscured links to opt-out processes on a company's home page (see discussion of Freckle I.O.T./PlacelQ's interface, *supra* p. 21-22, and *infra* p. 31).

When visiting the website of the data broker Chartable to opt out of the sale of information, visitors are required to accept cookies. Chartable explains that the cookies are used to “serve tailored ads.” The only option is to “Accept Cookies,” and it asserts that by browsing the site users are agreeing to its terms of service and privacy policy.

⁵⁶ *Most Cookie Banners are Annoying and Deceptive. This Is Not Consent*, PRIVACY INTERNATIONAL (last visited Aug. 28, 2020), <https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent>.



For nine brokers, at least one tester reported refraining from accepting cookies as part of the process. In five of these cases, testers reported that they stopped their request because they felt uncomfortable or did not understand next steps. For example, a Freckle I.O.T./PlacelQ tester described how accepting cookies was implicitly required for making a DNS request:

Their text-box asking to Allow Cookies covers the bottom 20% of the screen and won't go away unless, I assume, you tick the box to Allow. Therefore, I cannot see all my options. Also, I am accessing their site on a PC and they want me to download an app to my phone. Very difficult or impossible to see how to stop them from selling my data.

Another tester reported that the company they tested, Deloitte Consulting, had “two request types—‘Cookie Based’ and ‘Non-Cookie Based’” and that they were “skeptical that most people will be able to decode the techno-babble description of each type.”

Consumers were often forced to wade through confusing and intimidating disclosures to opt out.

While our survey did not include direct questions about communications with data brokers, in some cases consumers proactively reported finding language surrounding the DNS request link and process excessively verbose and hard to understand. For example, one tester reported of the data broker US Data Corporation, “There is a long, legalistic and technical explanation of how and why tracking occurs, not for the faint of heart.” Another said of Oracle America, “The directions for opting out were in the middle of a wordy document written in small, tight font.” Another found the legal language used by Adrea Rubin Marketing intimidating: “they seemed to want to make the process longer and unnecessarily legalese-y, even a bit scary--under threat of perjury.”

Another data broker, ACBJ, placed a “Your California Privacy Rights” link at the bottom of their homepage (rather than a “Do Not Sell My Personal Information” link), which led to their privacy and cookie policy.⁵⁷ Once on the policy page, the consumer is forced to search in their browser for the phrase “Do Not Sell My Personal Information” or scroll and scan ten sections of the privacy policy to find the paragraph with a “Do Not Sell My Personal Information” link, or follow two additional links to navigate from the privacy policy table of contents to the “Do Not Sell My Personal Information” link. Upon clicking the “Do Not Sell My Personal Information” link, the consumer is shown a pop-up with a page of additional legal information, and then has to scroll down to a toggle that finally allows them to request their data not be sold.

Some consumers spent nearly an hour, if not more, to complete a request.

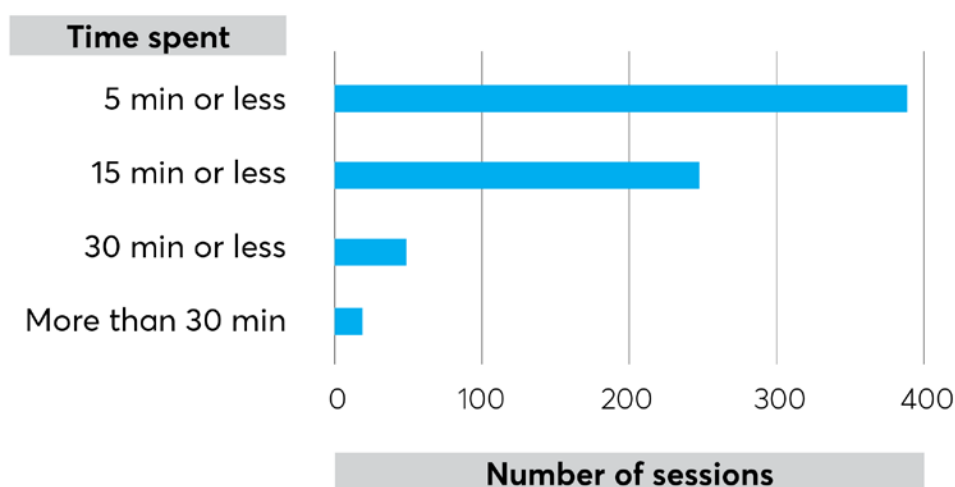
We also asked consumers about how long they spent to complete a request, and to not include the time spent filling out the survey. While the vast majority of consumers spent less than 15 minutes at a time on requests—and the most common amount of time was less than 5 minutes—some consumers reported that they nearly an hour or more than an hour opting out. A consumer working on the Jun Group reported that they were required to obtain their advertising ID to opt out: “Obtaining my Advertising Identifier was very time consuming and I am not sure how it is used.” The consumer testing Accuity reported: “They make it so hard to even find anything related to my information collected or subscribing or op-out that I had to read through so much boring yet infuriating do to what they collect and every one the will give it to for a price. We, as

⁵⁷ ACBJ (last visited Aug. 10, 2020), <https://acbj.com/privacy#X>.

Americans shouldn't have to do this to keep our information out of advertising collectors.”

Even spending five minutes on a single opt-out request could prevent consumers from exercising their CCPA rights. A consumer would have to make hundreds of such requests to be opted out of all data brokers potentially selling their data—not to mention all of the other companies with which the consumer has a relationship.

Sessions By Time Spent



At least 14% of the time, burdensome or broken DNS processes prevented consumers from exercising their rights under the CCPA.

Participants reported giving up in 7% of tests.⁵⁸ They reported being unable to proceed with their request in another 7% of tests.⁵⁹ These 14% of cases represent a DNS process clearly failing to support a consumer's CCPA rights.

⁵⁸ Example responses coded as “giving up” include: “Dead ended, as I am not going to send the info requested” and “Gave up because too frustrating. . . ”

⁵⁹ Example responses coded as “unable to proceed” include “the website is currently waiting for me to provide my IDFA number but I'm not sure how to adjust my settings to allow the new app permissions to retrieve;” “I could not Submit my form after several tries;” and “It looks like I did not email them after

The overwhelming reason for a consumer to refrain from part of a DNS request process, or give up all together, was not feeling comfortable providing information requested. Out of the 68 reports that the tester chose not to provide information they were asked for as part of the process, 59 said it was because they were not comfortable doing so. For example, nearly all consumers declined to provide a photo in order to process their opt-out requests. Out of 7 instances in which consumers reported that they were asked to provide a photo selfie, in 6 the consumer declined.

Consumers told us that they were just as averse to providing government IDs. One tester of Searchbug reported: "I hated having to send an image of my Driver License. I thoroughly regret having done so. It feels like an invasion of privacy to have to do that, just so I can take steps to PROTECT my privacy. Feels wrong and dirty." Even consumers that ended up providing the drivers' license ended up confused by the company's follow-up response. One tester of Hexasoft Development Sdn. Bhd. responded: "After sending them a copy of my California driver license to satisfy their residency verification, I got an email back which simply stated that '[w]e will update the ranges in the future release.' I have no idea what that means." Out of 17 reports of being asked for an image of a government ID, in 10 the consumer chose not to. Out of 40 reports of being asked to provide a government ID number, in 13 the consumer refrained from providing it.

The data broker X-Mode used data submitted as part of a DNS request to deliver a marketing email, a practice that is prohibited by the CCPA.

X-Mode, a data broker that sells location data, used customer data provided to opt out in order to send a marketing email, in violation of the CCPA. Study participants voiced concerns about handing over additional personal information to data brokers in order to protect their privacy, and it was disappointing to discover that their concerns were warranted. Consumers are particularly sensitive about receiving additional marketing messages. One consumer, for example, shared with us that they began receiving more unsolicited robocalls after submitting the opt-out request. Reflecting these concerns, the CCPA specifically prohibits companies from using data collected to honor an opt-out request for any other purpose.⁶⁰

getting nowhere calling the number on their website that was supposed to handle requests and had no idea what I was talking about."

⁶⁰ Cal. Civ. Code § 1798.135(a)(6).

But X-Mode ignored that requirement. X-Mode is a data broker that pays apps—such as weather and navigation apps—to collect location data from devices that have installed the software.⁶¹ X-Mode makes money by selling insights drawn from that data to advertisers. For example, the Chief Marketing Officer of X-Mode explained, “If I walked by a McDonald’s but walk into a Starbucks, my device knows with the XDK that I passed a McDonald’s but I actually went into Starbucks.”⁶² X-Mode also sells personal information to third party applications and websites.⁶³ And it has also shared anonymized location data with officials in order to help track compliance with stay-at-home orders during the COVID-19 crisis.⁶⁴ Because it sells such sensitive information, X-Mode should be particularly careful to protect the anonymity of consumer data and respect consumers’ privacy preferences.

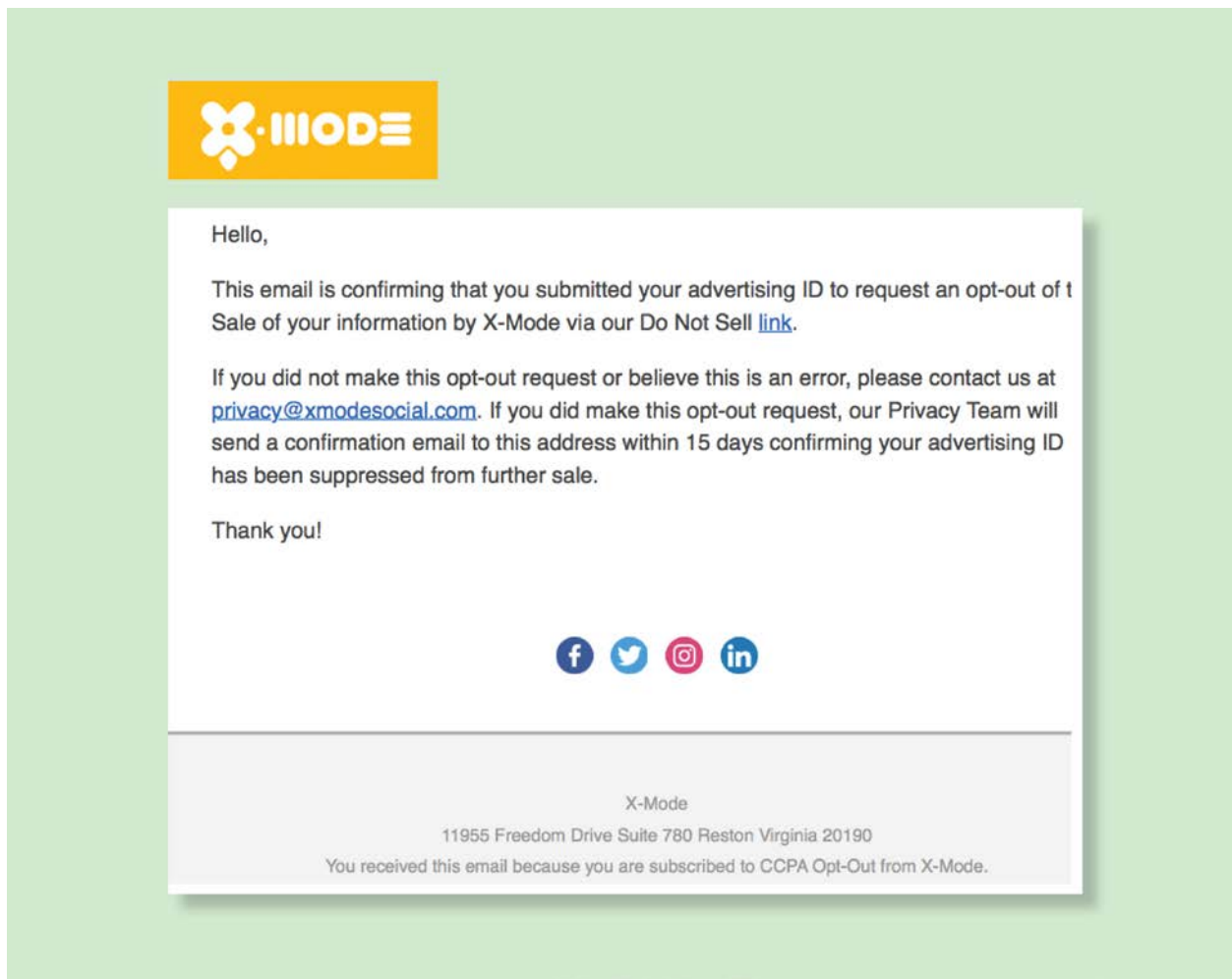
After submitting the opt-out request in April 2020, the author received the following email confirming that she had been placed on an “CCPA Opt-out” mailing list:

⁶¹ Sam Schechner et al., *Tech Firms Are Spying on You. In a Pandemic, Governments Say That’s OK*, WALL ST. J. (June 15, 2020), <https://www.wsj.com/articles/once-pariahs-location-tracking-firms-pitch-themselves-as-covid-sleuths-11592236894>.

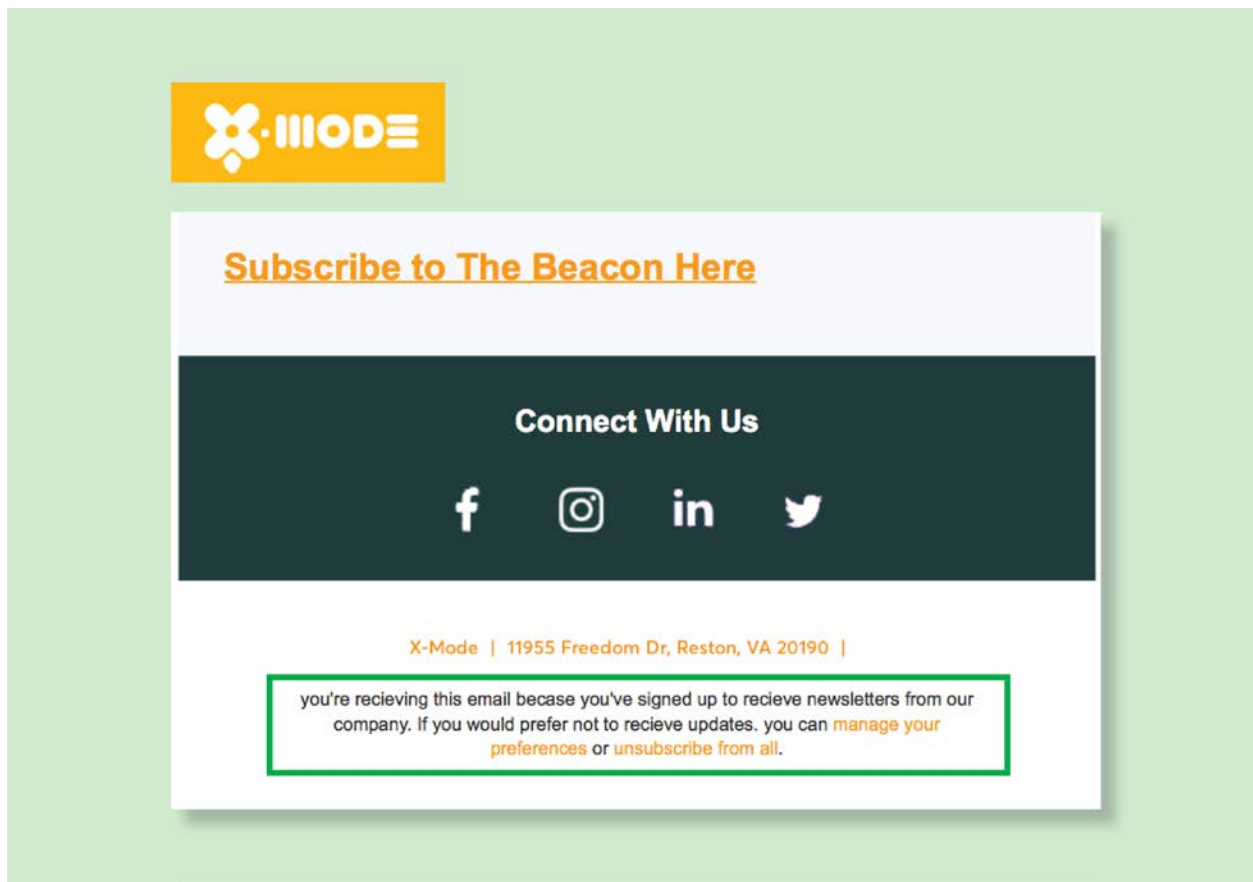
⁶² Jake Ellenburg, quoted in Karuga Koinange, *How Drunk Mode, An App for the Inebriated, Became Data Location Company X-Mode Social*, TECHNICALLY (Feb. 27, 2020), <https://technical.ly/dc/2020/02/27/how-drunk-mode-app-became-data-location-company-x-mode-social/>.

⁶³ ZenLabs LLC, Privacy Policy (last visited Aug. 28, 2020), <http://www.zenlabsfitness.com/privacy-policy/>.

⁶⁴ Schechner et al., *Tech Firms Are Spying on You*, *supra* note 61.



The following month, the author received an email inviting her to subscribe to X-Mode's newsletter in order to keep up with the business. The fine print explained that the email was sent "because you've signed up to receive newsletters from our company[,]" with the option to unsubscribe.

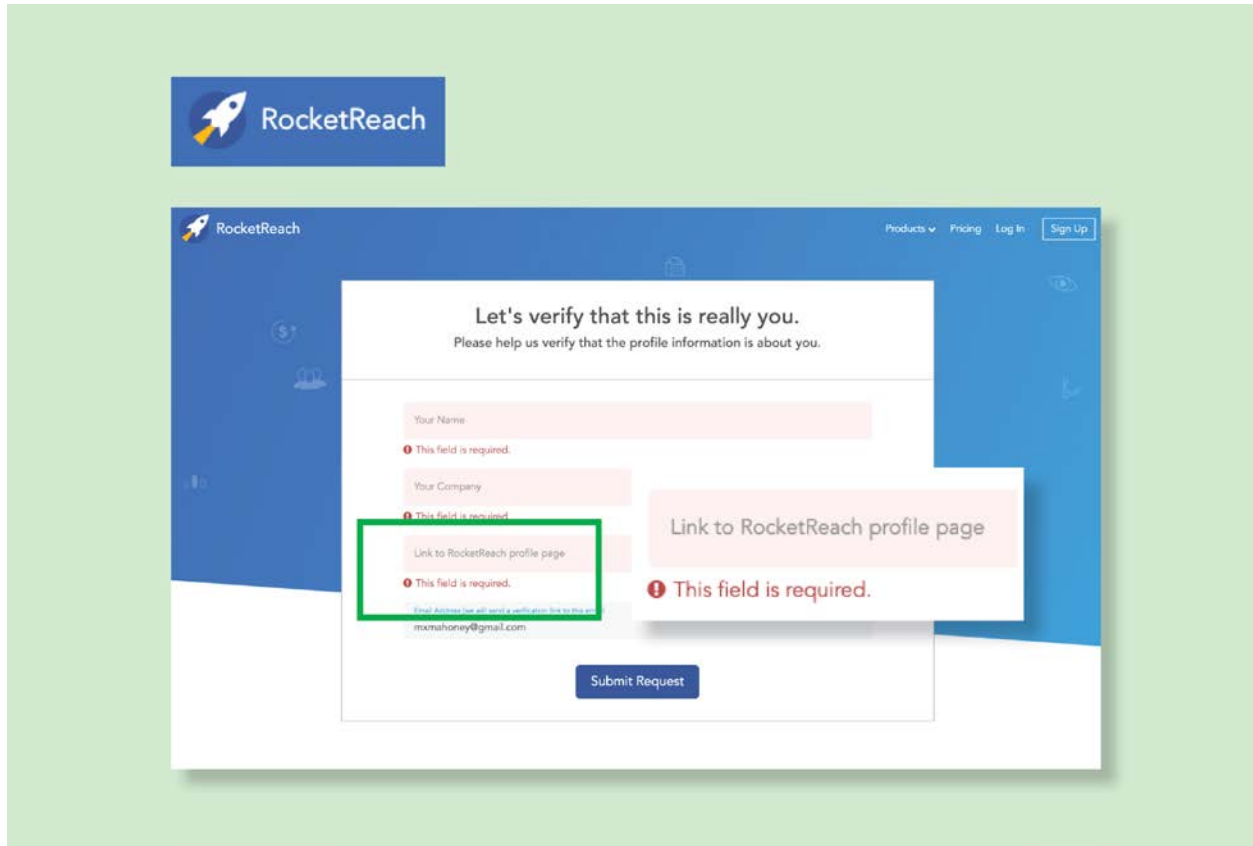


Since the only interaction that the author has had with X-Mode was to opt out—by definition, data brokers do not have relationships with consumers—the only way that she could have “signed up” was through opting out of the sale of her information. This behavior violates the CCPA’s prohibition on reuse of data provided for exercising data rights, and it could have a chilling effect on consumers exercising their rights with respect to other companies, as they are understandably worried about subjecting themselves to even more messages.

The data broker RocketReach requires the user to set up an account to opt out, which is prohibited by the CCPA.

RocketReach, a company that helps users find the contact information of potential business leads, requires users to list their RocketReach account in order to opt out of the sale of their information, even though the CCPA explicitly prohibits requiring

consumers to set up an account to opt out.⁶⁵ The homepage includes a link that reads “Do Not Sell My Info,” which then takes the consumer to a page that requires them to list their name, company, link to RocketReach profile, and email. If the user enters only name and email, the site does not let the user proceed further.



This frustrated testers, one of whom said, “I cannot determine whether they hold any of my information because they require a company and RocketReach account profile in order to honor the do not sell request.”

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

Neither the CCPA nor the implementing regulations require companies to notify consumers when their opt-out request has been honored, and this left consumers

⁶⁵ Cal. Civ. Code § 1798.135(a)(1).

confused about whether the company was still selling their information. Only in 18% of requests did participants report a clear confirmation from the broker that their data was or would soon not be sold. **In 46% of tests, participants were left waiting or unsure about the status of their DNS request.** In the 131 cases where the consumer was still waiting after one week, 82% were dissatisfied with the process (60% reported being very dissatisfied, and 22% reported being somewhat dissatisfied). The lack of clarity and closure was reflected in consumer comments such as “left me with no understanding of whether or not anything is going to happen” and “While it was an easy process—I will read their privacy policy to see if there is more [I] have to do to verify they are complying with my request. They left me unsure of the next step.”

In looking at how often consumers gave up or were unable to complete requests, we found a wide variety of responses from brokers, and variation in how consumers interpreted those responses. Once a DNS request was submitted, broker responses included:

- no response at all;
- acknowledging the request was received but providing no other information;
- acknowledging the request was received and vague language leaving consumers unsure of what was next;
- saying the request would be implemented in a certain timeframe (ranging from 2 weeks to 90 days);
- asking consumers to provide additional information;
- confirming a different type of request (such as Do Not Contact or Do Not Track);⁶⁶
- telling the consumer that the broker is not subject to the CCPA (even though the company was listed on the California data broker registry);
- telling the consumer that the broker has no data associated with them; and
- acknowledging the request was received and confirming that data will no longer be sold.

Consumers' understanding of these responses varied. For example, among participants reporting that the broker said that their request was received and that it would be

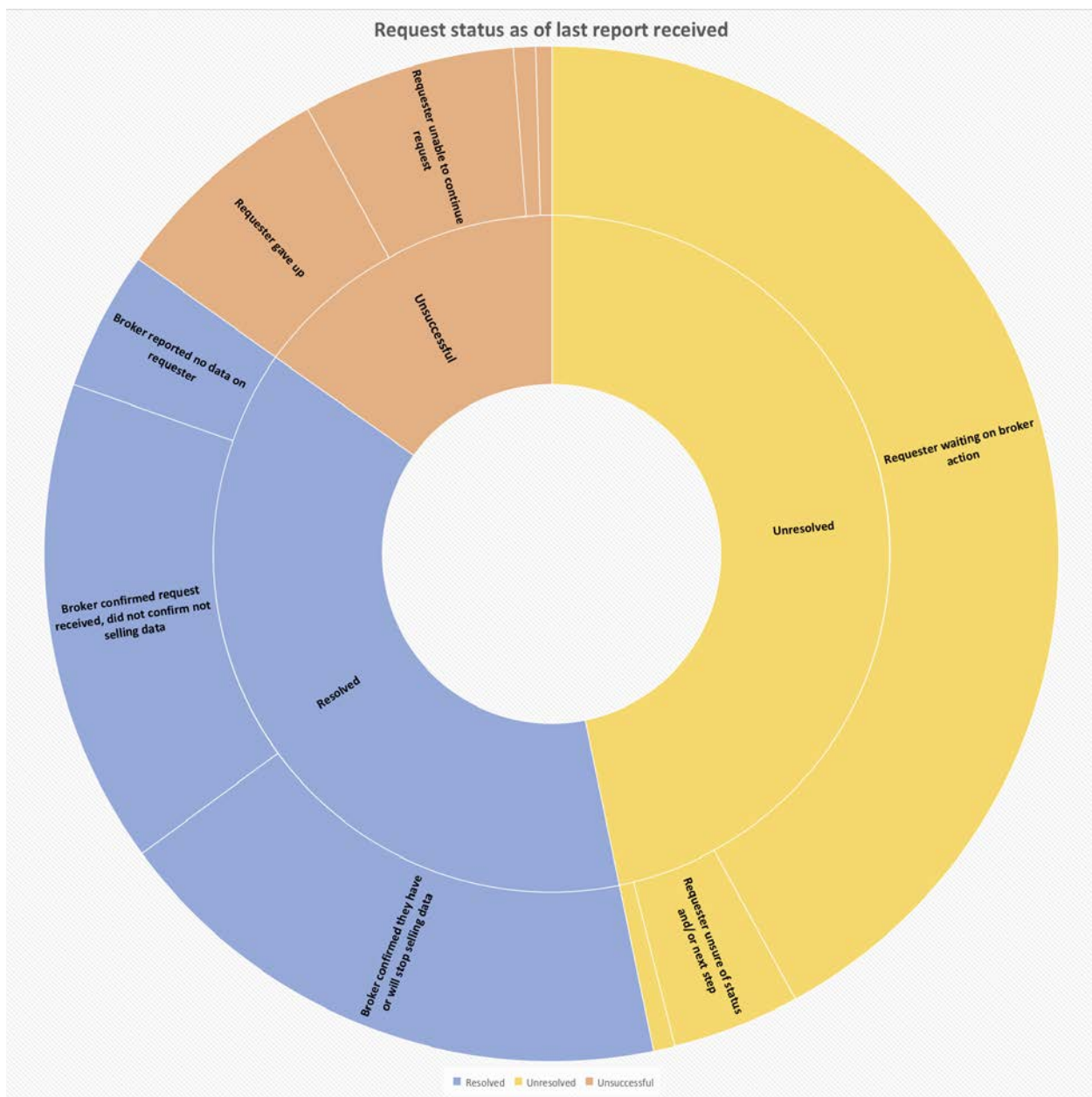
⁶⁶ Testers' references to “Do Not Contact” likely refer to consumers' right to be added to a company's internal “Do Not Call” list under the Telemarketing Sales Rule, 16 CFR § 310.4(b)(1)(iii)(A). Do Not Track refers to a request to stop tracking information about a consumer's activity across multiple sites. California law requires companies that collect personal information to disclose in the privacy policy whether they honor Do Not Track. See Cal. Bus. Prof. Code § 22575(5).

implemented in a certain time frame, some said the broker was honoring their DNS request but most said they were still waiting or unsure of the status of their request.

Below is a chart and visualization of the proportions of requests with different statuses as of the last report for each request:*

Overall Status	Sub Status	Number Requests
Resolved	Broker confirmed they have or will soon stop selling data	107
	Broker confirmed request received, did not confirm not selling data	91
	Broker reported no data on requester	26
Unresolved	Requester waiting on broker action	247
	Requester unsure of status and/or next step	24
	Requester has outstanding follow up	4
Unsuccessful	Requester gave up	42
	Requester unable to continue request	40
	Broker reported not subject to CCPA	4
	Broker confirmed non-DNS request	3

* Some responses did not include enough data to categorize, and were not included in the chart (Note added May 13, 2021).



We took a closer look at requests in which participants were “waiting” as of their last report, and found that many were still waiting for the data broker to respond to them after 21 days. Among the 247 requests in which the consumer was waiting for broker action, 81 were waiting after 21 days, 50 were waiting after at least a week but less than 21 days, and 116 of these were within 2 days of initiating a request. Those 116 represent cases where the broker may follow up later. However, the 81 cases in which consumers were still awaiting broker action after 21 days represent a problem with the

CCPA, in which consumers must choose between giving up and staying engaged for weeks at a time in hopes of receiving a clear confirmation from the broker that their DNS request has been completed. In 17 requests, the tester reported in an open-ended answer that they had had no response at all from the broker. Seven of these reports were after 21 days, and another 4 were after at least one week.

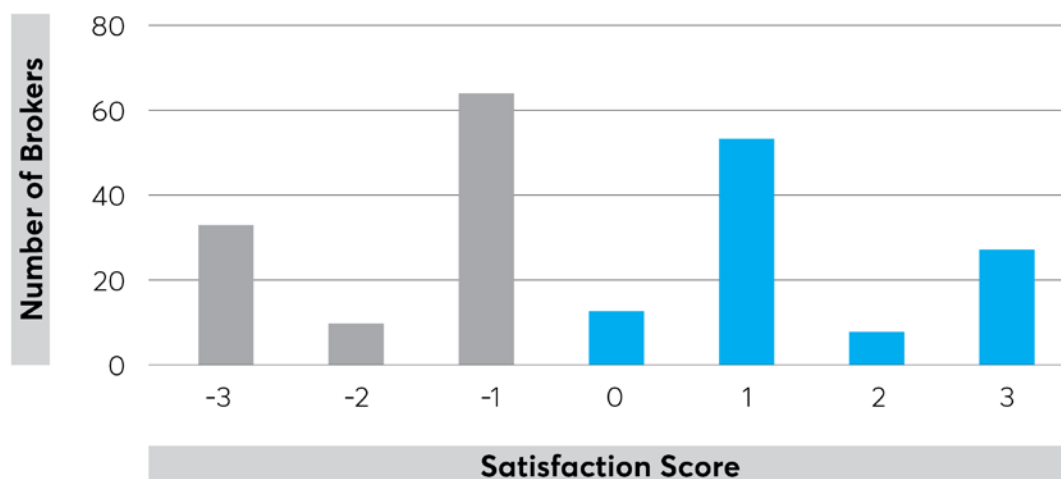
About 52% of the time, the tester was “somewhat dissatisfied” or “very dissatisfied” with opt-out processes.

Overall, testers were more often dissatisfied than satisfied with the DNS processes. The survey asked how satisfied testers were with the process by providing four answers: very satisfied, somewhat satisfied, somewhat dissatisfied, very dissatisfied. The question was optional. Of the testers who answered this question, about 52% of the time, the tester was somewhat or very dissatisfied, and about 47% of the time, the tester was very or somewhat satisfied.⁶⁷

We also assigned each broker a satisfaction score. Some companies had consistent satisfaction, others had consistent dissatisfaction, and most had processes leaving consumers mixed in their satisfaction levels. In the satisfaction score, a broker received a positive point for a “very satisfied” or “somewhat satisfied” answer, and a negative point for a “somewhat dissatisfied” or “very dissatisfied” answer. The number of brokers with each score is plotted on the next page.

⁶⁷ Testers answered this question in 601 tests. Of these tests, in 317 (52%), the respondent was “somewhat dissatisfied” or “very dissatisfied” with the opt-out process, and in 284 (47%) tests, the respondent was “very satisfied” or “somewhat satisfied.” In 41 cases, the tester did not answer the question.

Tester Satisfaction



Some data brokers had quick and easy opt-out processes, showing that companies can make it easier for consumers to opt out. About 47% of the time, the tester was “somewhat satisfied” or “very satisfied” with the opt-out process.

In several cases, consumers reported either a one-step process using an online interface that confirmed their data would no longer be sold, or a prompt and clear confirmation via email from the broker that their data would no longer be sold. For example, one tester of American City Business Journals described the process: “Just had to go to the privacy link at the bottom of the home page. Found the Calif. privacy link then had to scroll to button to turn off ‘sell my info’.” Another shared an email from a DT Client Services, received the same day she submitted her request, that clearly confirmed that they would stop selling her data: “We confirm that we have processed your Request and will not sell your personal information to third parties.” These processes demonstrate an effective standard for implementing DNS requests. Overall, about 47% of the time, the tester was “somewhat satisfied” or “very satisfied” with the opt-out process.

It is also possible for data brokers to post DNS links that are easy to find. For example, for 58% of the brokers, all three testers found the DNS link on the broker’s website, suggesting that these links were posted prominently. Links that were easy to find were

described as “prominent and easy to find,” “at bottom of page, but large,” “bottom of page, bold,” and “prominent at bottom of home page.” Thirty-nine data brokers out of 214 had all three testers report that the DNS link was “very easy” to find. For brokers where three out of three testers found the DNS link, the link was reported “very easy” or “somewhat easy” to find in 65% of cases, and “very difficult” or “somewhat difficult” to find in only 13% of cases.

Policy recommendations

The Attorney General should vigorously enforce the CCPA to address noncompliance.

The AG should use its enforcement authority to address instances of noncompliance, and to incentivize other companies to comply. While the AG is hamstrung by flaws in the enforcement provisions of the privacy requirements, notably the “right to cure” language that lets companies off the hook if they “cure” the problem within 30 days,⁶⁸ taking action will help push companies to get into compliance. Our study showed that a few improvements would go a long way. For example, it was significantly easier to opt out of a data broker site when the company had a link clearly labeled “Do Not Sell My Personal Information” that took consumers directly to the interactive form. Once that element was removed, consumers were often adrift, forced to email customer service staff who may not understand the request, or sent through a maze of sites with confusing disclosures. The AG should make an example of companies that fail to meet these requirements to help bring all of them into compliance.

To make it easier to exercise privacy preferences, consumers should have access to browser privacy signals that allow them to opt out of all data sales with a single step.

At the very least, consumers need access to universal opt-out tools, like browser privacy signals. Requiring consumers to opt out of every company one-by-one simply is not workable. The AG regulations require companies to honor platform-level privacy signals as universal opt outs, if the signal clearly constitutes a “Do Not Sell” command.⁶⁹ At the moment, however, there are no platform signals that we are aware of that clearly indicate a desire to out of the sale of data. Browsers are a logical place to start, though consumers need ways to opt out of advertising on devices other than browsers, such as

⁶⁸ Cal. Civ. Code § 1798.155(b).

⁶⁹ Cal. Code Regs. tit. 11 § 999.315(c) (2020).

TVs and phones. The AG should encourage developers to bring to market these solutions as quickly as possible, and should also set up a registry to help identify the signals that must be honored. This would help bring clarity for businesses and consumers.

The AG should more clearly prohibit dark patterns, which are user interfaces that subvert consumer intent, and design a uniform opt-out button. This will make it easier for consumers to locate the DNS link on individual sites.

Given that many consumers found it difficult to find the Do Not Sell link—it was often labeled with something different, and often buried at the bottom of the page with a bunch of other links—a graphic button would likely have value in ensuring that consumers would take advantage of that privacy protection. The CCPA directs the AG to design an opt-out button: “a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt out of the sale of personal information.”⁷⁰ The AG designed an initial draft, but declined to include a design in the final regulations. According to the AG, the proposed opt-out button was “deleted in response to the various comments received during the public comment period. The OAG has removed this subsection in order to further develop and evaluate a uniform opt-out logo or button for use by all businesses to promote consumer awareness of how to easily opt-out of the sale of personal information.”⁷¹ While the original design came under a fair amount of criticism, a uniform button, regardless of what it ends up looking like, will likely have value for consumers seeking to opt out, and the AG should promulgate one as soon as possible.

This will also help address instances in which companies route consumers through multiple, unnecessary steps in order to opt out. For example, Outbrain (*infra*, p. 18) led consumers through multiple steps to opt out, and on nearly every page the consumer had to hunt to figure out which option would lead them to the next step. And after all that, at least one consumer told us that they were not sure they had even opted out. Given that 7% of our testers gave up on the opt outs out of frustration or concern about sharing additional information, confusing interfaces significantly undermined consumers' ability to opt out.

⁷⁰ Cal. Civ. Code § 1798.185(a)(4)(C).

⁷¹ FSOR, *supra* note 27, at 15.

The AG should require companies to notify consumers when their opt-out request has been honored.

Many consumers had no idea whether or not their opt-out request had been honored. The uncertainty often left consumers dissatisfied with the opt out. Some companies did notify consumers that their requests had been honored, and this information was characteristic of simple, quick, and effective opt-out processes.

Required notification is also important for compliance purposes. For example, the AG regulations require companies to comply with opt outs within 15 business days. Without providing any notification of the opt out completion, there's no way to judge whether or not the company has honored the law and to hold them accountable if not.

The legislature or AG should clarify the definitions of “sale” and “service provider” to more clearly cover data broker information sharing.

In response to the CCPA, many companies have avoided reforming their data practices in response to “Do Not Sell” requests by arguing that data transfers either are not “sales,” or that transferees are “service providers” such that opt-out rights do not apply.⁷² Certainly, while some sharing with true data processors for limited purposes should not be subject to opt-out requests, many companies' interpretation of the CCPA seems to argue that third-party behavioral targeting practices are insulated from consumer choice.⁷³ As such, even if a consumer successfully navigates a DNS request from a data broker, in practice exercising opt-out rights may have little to no practical effect. Policymakers should close these potential loopholes to clarify that, *inter alia*, data broker information sharing for ad targeting is covered by CCPA obligations.

Privacy should be protected by default. Rather than place the burden on consumers to exercise privacy rights, the law should require reasonable data minimization, which limits the collection, sharing, retention, and use to what is reasonably necessary to operate the service.

⁷² Mahoney, *Companies Aren't Taking the CCPA Seriously*, *supra* note 5.

⁷³ IAB CCPA Compliance Framework for Publishers & Technology Companies, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2019), https://www.iab.com/wp-content/uploads/2019/12/IAB_CCPA-Compliance-Framework-for-Publishers-Technology-Companies.pdf; Patience Haggin, *Facebook Won't Change Web Tracking in Response to California Privacy Law*, WALL ST. J. (Dec. 12, 2019), <https://www.wsj.com/articles/facebook-wont-change-web-tracking-in-response-to-california-privacy-law-11576175>.

While our study demonstrates that too many companies do not appear to be complying in good faith with the CCPA, any model that relies upon individuals to affirmatively act to safeguard their privacy will be deeply flawed. Given the challenges posed to businesses and consumers with respect to opting out, a better model is to ensure that privacy is protected without the consumer having to take any additional action. Several consumers who signed up for the study expressed shock that they were expected to opt out of the sale of their information. The thought of having to work their way through the entire data broker registry, which had hundreds of companies, was near unimaginable for these participants. Hard-to-find links, if they're even posted at all, confusing opt-out processes, requiring consumers to submit additional personal information, and above all the fact that there are hundreds of data brokers on the registry alone—all suggest that the responsibility needs to be on the company to protect privacy in the first place, rather than placing all the responsibility on the consumer.

This is a particularly important issue for elderly consumers or others who may have difficulty navigating online, several of whom dropped out of our study because it was so challenging to complete a single opt out. While there may be an easier path forward for some consumers who are able to take advantage of browser privacy signals to opt out universally—those are people who are already fairly tech savvy in the first place. Further, such a system only limits the sale of online data or data collected via a platform; it wouldn't stop the sale of data collected, say, in physical stores.

A better model would simply be to prohibit the sale of personal information as a matter of law, and to mandate that companies only collect, share, use, or retain data as is reasonably necessary to deliver the service a consumer has requested. Consumer Reports has supported legislation to amend the CCPA, AB 3119 (2020), that would require just that; Senator Sherrod Brown has introduced similar legislation, the Data Accountability and Transparency Act of 2020, at the federal level.⁷⁴ While the CCPA and the California data broker registry law are important milestones that improve transparency and individual agency, ultimately a more robust approach will be needed to truly protect Californians' privacy.

⁷⁴ The Data Accountability and Transparency Act of 2020, Discussion Draft, <https://www.banking.senate.gov/imo/media/doc/Brown%20-%20DATA%202020%20Discussion%20Draft.pdf>.

Conclusion

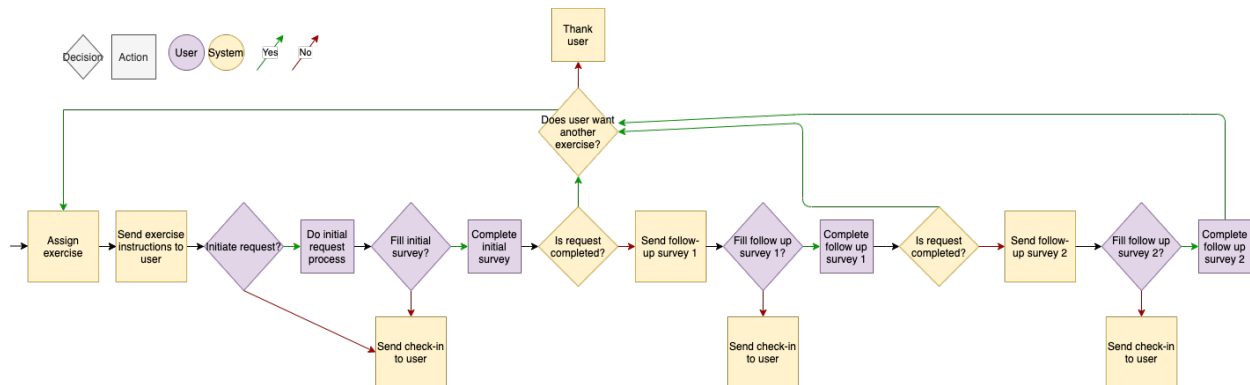
Overall, we found that consumers were too often dissatisfied with CCPA opt-out processes. This study uncovered some cases where the DNS process was short, clear, and satisfactory. It also found that some companies aren't complying with the CCPA, and that consumers were often left frustrated and without confidence that they had successfully exercised their DNS rights. It also reveals that, too often, consumers were unable to make a DNS request or gave up on the process altogether. Policymakers need to adopt crucial reforms in order to ensure that consumers can enjoy their right to privacy under the California Constitution.⁷⁵

⁷⁵ Cal. Cons. § 1.

Appendix

Section A

Below is a diagram of the participant experience of the exercise. Participants were randomly assigned a data broker from the registry using custom software, and were emailed with instructions to attempt making a DNS request to that broker. Participants then reported their experience with the DNS process via survey immediately after their first session working on the request. Participants were prompted by email to fill out follow-up surveys at one week and 21 days (approximately 15 business days) to report on any subsequent steps they had taken or any updates on the status of their request they had received from the data broker.



Section B

Below, we include links to screenshots of the homepages of data brokers that did not have the required “Do Not Sell My Personal Information” links on their homepages.*

[adMarketplace, Inc.](#)
[Big Brook Media, LLC](#)
[Blue Hill Marketing Solutions, Inc.](#)
[Comscore, Inc.](#)
[Electronic Voice Services, Inc.](#)
[Enformion, Inc.](#)
[Exponential Interactive, Inc. doing business as VDX.tv](#)
[Gale](#)
[GrayHair Software, LLC](#)
[Infinite Media Concepts Inc.](#)
[JZ Marketing, Inc.](#)
[LeadsMarket.com LLC](#)
[Lender Feed LC](#)
[On Hold-America, Inc. DBA KYC Data](#)
[Outbrain Inc.](#)
[PacificEast Research Inc.](#)
[Paynet, Inc.](#)
[PossibleNow Data Services, Inc](#)
[RealSource Inc.](#)
[Social Catfish LLC 1, Social Catfish LLC 2](#)
[Spectrum Mailing Lists](#)
[SRAX, Inc.](#)
[USADATA, Inc.](#)
[zeotap GmbH](#)

* On December 3, 2020, we replaced the screenshots for LeadsMarket, Social Catfish, and SRAX to provide a clearer view of the entire homepage.

Section C

An additional five companies had “Do Not Sell” links on their homepages, but all three testers were unable to find the DNS link, suggesting that it may not have been posted in a “clear and conspicuous manner” as required by the CCPA. Below, we include links to screenshots of the homepages of these companies.

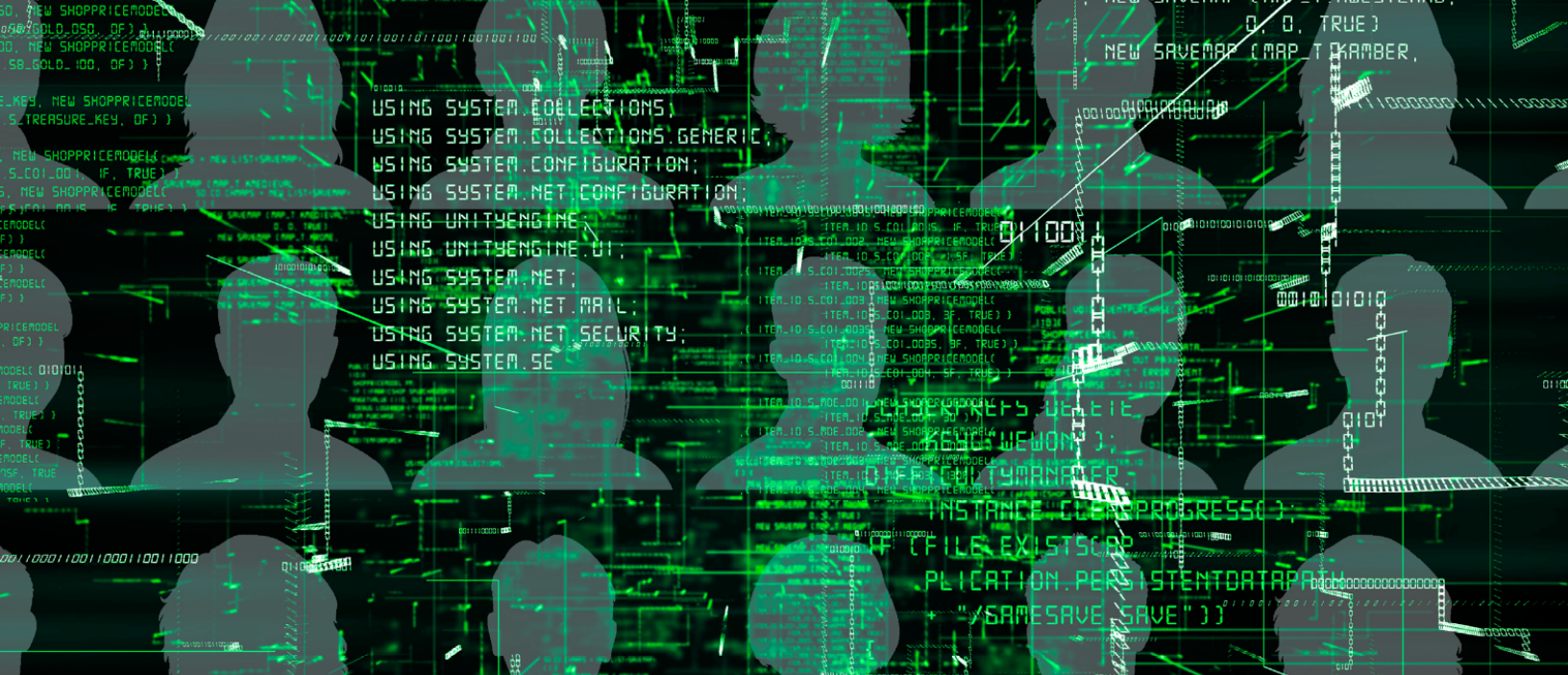
[AcademixDirect, Inc.](#)

[Fifty Technology Ltd.](#)

[Freckle I.O.T. Ltd./PlacelQ](#)

[Marketing Information Specialists, Inc.](#)

[Media Source Solutions](#)



REPORT

Opening Black Boxes: Addressing Legal Barriers to Public Interest Algorithmic Auditing

BY NANDITA SAMPATH
POLICY ANALYST
OCTOBER 2022

Executive Summary

Artificial Intelligence (AI) is being integrated into everyday decision-making in practically every commercial sector in the U.S., from housing to education to the criminal justice system. Landlords have used automated tenant screening reports (which include an algorithmically generated score) to make determinations about potential tenants.¹ The COVID-19 pandemic has led to schools requiring students to download proctoring software to identify cases of cheating during at-home exams.² In the criminal justice system, risk assessments have been used to, among other things, quantify a defendant's future risk of misconduct to determine whether they should be incarcerated before their trial.³ But as AI-enabled decision-making becomes more common, it also has the potential to exacerbate historical societal inequalities if it generates unfair and biased outcomes.

Before we can regulate algorithms effectively, both regulators and the public need to know how they work and arrive at their conclusions and to what extent they perpetuate discrimination and other harms. While federal and state civil rights laws prohibit discrimination based on protected characteristics like race, gender, and skin color in employment, housing, and lending, it can be hard to detect whether certain algorithms lead to discrimination at all. With many algorithms, it can be difficult to determine how they arrive at their final decisions, even for the engineers who design them.⁴ While this paper focuses on identifying discrimination, some companies make unsubstantiated claims about their algorithms, promoting both high accuracy rates and that their algorithms are capable of making certain determinations without external validation.⁵ Furthermore, there are few transparency requirements for businesses to disclose how their algorithms work, the types of data they collect, how each data point is factored into the final decisions, and accuracy or error rates.

Ultimately, our government must be the one to set standards on algorithm testing and auditing, particularly for applications with significant legal effects. However, in the absence of laws that require companies using AI to undergo independent, rigorous third-party audits, public interest researchers can play a vital role in uncovering the harms caused by algorithmic decision-making. This paper will lay out the different types of public interest auditing techniques and then address the legal and practical roadblocks that can impede public interest researchers from performing algorithmic audits. Public interest audits are limited by imperfect access to

¹ Kaveh Waddell, "How Tenant Screening Reports Make It Hard for People to Bounce Back From Tough Times," Consumer Reports, March 11, 2021, <https://www.consumerreports.org/algorithmic-bias/tenant-screening-reports-make-it-hard-to-bounce-back-from-tough-times-a2331058426>.

² Drew Harwell, "Cheating-detection companies made millions during the pandemic. Now students are fighting back," The Washington Post, November 12, 2020, <https://www.washingtonpost.com/technology/2020/11/12/test-monitoring-student-revolt>.

³ Alex Chohlas-Wood, "Understanding risk assessment instruments in criminal justice," Brookings Institution, June 19, 2020, <https://www.brookings.edu/research/understanding-risk-assessment-instruments-in-criminal-justice>.

⁴ Will Knight, "The Dark Secret at the Heart of AI," MIT Technology Review, April 11, 2017, <https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai>; Roman V. Yampolskiy, "Unexplainability and Incomprehensibility of Artificial Intelligence," *Journal of Artificial Intelligence and Consciousness* 7, no. 2 (June 20, 2019), <https://philarchive.org/archive/YAMUAI>.

⁵ Arvind Narayanan, "How to recognize AI snake oil," Princeton University, <https://www.cs.princeton.edu/~arvindn/talks/MIT-STS-AI-snakeoil.pdf>.

algorithms and the underlying data in part because of existing laws designed to limit computer hacking and protect intellectual property. To help remove these obstacles, we recommend policy changes that would balance these legitimate values with the need for research and external accountability. Today, public interest researchers are significantly hindered in performing good faith research to identify sources of algorithmic harm because they are concerned about a potential lawsuit. Policymakers should make targeted changes to the law to address this chilling effect.

Table of Contents

Executive Summary	1
Introduction	3
Problem	4
Case for Public Interest Auditing	5
Why Private Audits Are Not Enough	6
Introduction to Types of Audits	9
1. Code Audit	9
2. Crowdsourced Audit	11
3. Scraping Audit	13
4. Sock Puppet Audit	15
Policy Recommendations	17
1. Access and Publication Mandates	17
2. CFAA and Computer Trespass	18
3. Contract Law	18
4. DMCA	19
5. Copyright	19
6. Civil Rights, Privacy, and Security	20
7. Consumer Protection Law	20
Other Frameworks to Incentivize Public Interest Audits	22
Bug Bounty Programs for Algorithms	22
Whistleblower Protections	23
Conclusion	24

Introduction

Artificial intelligence (AI) and Machine Learning (ML) refer to the use of data to make predictions or classifications about future data points, while an algorithm is simply a set of instructions to make these predictions and classifications. Although there is no consensus over these definitions, both AI and ML generally refer to the types of algorithms used in making these decisions,⁶ and sometimes these terms are used interchangeably. In general, though, data is used to train an algorithm so that it can make more accurate decisions, and the algorithm is only as good as the quality of the data it is fed.

As the use of algorithms and AI become more embedded into daily life, the potential for algorithmic harms like discrimination is alarming. There are minimal regulations and industry standards to guide how algorithms are designed and tested, and how to address any negative impacts, and it is often unclear how existing law applies to these new technologies.⁷ Because many algorithms are quite complex, it is difficult to regulate them appropriately. However, effective audits by public interest researchers can help both the public and regulators understand how algorithms work and their impact on potential discrimination and other harms.

Mandatory, independent, and standardized third-party audits for companies whose algorithms pose significant legal effects are vital for maintaining our civil rights as more processes that affect our lives become automated. This could be done by either government agencies or private companies that have been accredited through a process specified by government agencies that enforce particular laws. For example, the Department of Housing and Urban Development would need to design what an audit should look like to examine algorithms covered under the Fair Housing Act and would need to accredit private auditing companies to carry out these audits, or perform the audits internally.⁸

However, there is a long way to go before this becomes a reality. The U.S. has not yet passed significant AI legislation at the federal level and lags behind governments like the European Union when it comes to enacting technology regulation; and, furthermore, involved federal agencies would likely be limited by funding and staffing issues in order to carry out audits or create an accreditation process effectively. While the burden in the meantime should not fall entirely on public interest researchers to uncover algorithmic harms, they can play a vital role in identifying bias and calling out companies as we push for more government regulation. And lessons learned from public interest audits can potentially be applied once a regulatory regime is in place.

⁶ However, AI is more commonly associated with newer types of algorithms such as neural networks that, while having the potential for high accuracy rates when performing difficult tasks (such as visualizing the surroundings of a self-driving car), are also so complicated that even the engineers that design them cannot fully explain how they work. See: Will Knight, “The Dark Secret at the Heart of AI”; Roman V. Yampolskiy, “Unexplainability and Incomprehensibility of Artificial Intelligence.” ML is often used to refer to older, statistical methods like linear regression models and decision trees, for example, that can more easily be interpretable by engineers and statisticians. These are types of models that can make a prediction or classifications about the output of a system given a particular input.

⁷ Mark MacCarthy, “AI needs more regulation, not less,” Brookings Institution, March 9, 2020, <https://www.brookings.edu/research/ai-needs-more-regulation-not-less>.

⁸ Specific frameworks for what this could look like are out of scope for this paper.

Unfortunately, there are many roadblocks that prevent public interest researchers from performing algorithmic audits. The same laws that were created to promote science and art, and to protect individuals and companies from hacking, are also hindering researchers in performing meaningful audits, for fear of legal recourse. These laws include the Computer Fraud and Abuse Act, copyright law, and contract law. Our conclusion is that these laws need to be clarified and updated so that public interest researchers can perform good faith audits without being concerned about legal repercussions.

Problem

Algorithms are often used in place of human decision-making, and in some cases they are touted as being more objective and thorough than a human decision-maker.⁹ However, an algorithm is only as good as the engineer who designs it and the data it is trained on—human error, including biased data collection methods and the type of algorithm that is chosen by the engineer, can also cause bias. No algorithm will ever be perfect, because a model is a simplified version of real-world events. Most algorithms make mistakes — or are more accurate on certain groups than others¹⁰ — due to these errors during the design process. This can cause real harm when the algorithm is used by a government, school, workplace, or even a landlord.¹¹

While there are some laws that prohibit discrimination based on protected characteristics like race, gender, and skin color in employment, housing, and lending, it is often difficult to identify whether models used in these areas actually contribute to unequal outcomes based on these characteristics. Companies are typically not required to disclose how their algorithms work, how they trained them, what issues they identified with their technology, and what steps they took to mitigate harm.¹² Furthermore, people usually do not know how the algorithm works on others, so it could be difficult for them to even identify whether they were discriminated against (for example, a woman who is rejected for a job by a resume-screening algorithm may not know that it allowed a man of similar experience to pass through).

Algorithmic discrimination is not the only harm associated with AI—social media platforms have been accused by critics of optimizing their algorithms for engagement, which leads to the spread of misinformation, propaganda, and harmful targeted advertisements.¹³ Many companies

⁹ Rebecca Heilweil, “Artificial intelligence will help determine if you get your next job,” Vox, December 12, 2019, <https://www.vox.com/recode/2019/12/12/20993665/artificial-intelligence-ai-job-screen>; Sendhil Mullainathan, “Biased Algorithms Are Easier to Fix Than Biased People,” The New York Times, December 6, 2019, <https://www.nytimes.com/2019/12/06/business/algorithm-bias-fix.html>.

¹⁰ The National Institute of Standards and Technology found that certain facial recognition algorithms were more likely to misidentify Asian and African American faces relative to Caucasians. “Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects,” National Institute of Standards and Technology: News, December 2019, <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>.

¹¹ There are entire books written about these issues, such as *Weapons of Math Destruction* by Cathy O’Neil (Crown Publishing Group, 2016) and *Race After Technology* by Ruha Benjamin (Polity, 2019).

¹² Hannah Bloch-Wehba, “Transparency’s AI Problem,” Knight First Amendment Institute at Columbia University, June 17, 2021, <https://knightcolumbia.org/content/transparencys-ai-problem>.

¹³ Filippo Menczer, “How ‘engagement’ makes you vulnerable to manipulation and misinformation on social media,” The Conversation, September 10, 2021, <https://theconversation.com/how-engagement-makes-you-vulnerable-to-manipulation-and-misinformation-on-social-m>

also promote their AI as being capable of predicting social outcomes or other kinds of “snake oil.” In other words, they make claims about their products that are not backed up by science.¹⁴ Many companies tout their “emotion recognition” algorithms, claiming they can identify how someone is feeling based on their face or other physical characteristics; there are concerns that these algorithms could discriminate based on race and have other harmful implications, and there is no evidence that emotion recognition can be done accurately.¹⁵ Algorithmic discrimination can lead to other egregious, distinct harms—consider hospitals using historical data about patients in an algorithm intended to help decide how to triage patients. One paper found that Black patients were assigned lower-risk scores than white patients, even when they were equally sick; the algorithm used data about patients’ historical healthcare costs to make decisions, and Black patients were routinely spent less on, which the scientists speculated is due to systemic barriers to healthcare access.¹⁶ Oversights like these are a matter of life or death, and we should expect robust standards for these kinds of algorithms.

Ultimately, AI can exacerbate power imbalances between consumers and companies (endless data collection about a consumer can lead to discriminatory pricing for products, or can be used to nudge a consumer to behave a certain way on a platform). AI companies need to be held accountable for AI-enabled harm, and they should be required to make transparent their accuracy rates and testing procedures, or otherwise change their algorithm design and testing procedures when such harms are identified.

Case for Public Interest Auditing

An algorithmic audit can be instrumental in identifying and mitigating algorithmic harm. An audit can help determine whether an algorithm leads to unequal outcomes or harmful effects. It can also identify in what context an algorithm works well, and when it fails. Ultimately, the purpose of an algorithmic audit is highly dependent on the auditor’s goals and the information they have access to in carrying out the audit.

Specifically, we argue that public interest groups, academics, and journalists have a major role to play in identifying algorithmic harms¹⁷ (in the absence of and alongside future government regulation of algorithms) because, unlike private auditing companies hired by the AI companies

[edia-145375](https://www.technologyreview.com/2021/10/04/facebook-whistleblower-reveals-identity-says-company-chooses-profits-over-safety/); Steve Dent, “Facebook whistleblower reveals identity, says company chooses ‘profits over safety,’” October 4, 2021, <https://techcrunch.com/2021/10/04/facebook-whistleblower-reveals-identity-says-company-chooses-profits-over-safety/>.

¹⁴ Arvind Narayanan, “How to recognize AI snake oil,” Princeton University, <https://www.cs.princeton.edu/~arvindn/talks/MIT-STS-AI-snakeoil.pdf>.

¹⁵ Lisa Feldman Barrett et al., “Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements,” *Psychological Science in the Public Interest*, July 17, 2019, https://journals.sagepub.com/doi/10.1177/1529100619832930#_i72.

¹⁶ Heidi Ledford, “Millions Affected by Racial Bias in Health-Care Algorithm,” *Nature* 574 (October 31, 2019): 608-609, <https://media.nature.com/original/magazine-assets/d41586-019-03228-6/d41586-019-03228-6.pdf>.

¹⁷ For example, ProPublica was able to look at outputs of the COMPAS algorithm (which claims to predict a criminal defendant’s likelihood of becoming a recidivist), to determine that the algorithm often predicted Black individuals to be at a higher risk of recidivism than they actually were, and white individuals were often predicted as less risky than they actually were; Jeff Larson, Surya Mattu, Lauren Kirchner and Julia Angwin, “How We Analyzed the COMPAS Recidivism Algorithm,” ProPublica, May 23, 2016, <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm>.

themselves, they typically seek to make available to the public useful information about how algorithms work, and to determine whether these algorithms lead to discriminatory or other harmful outcomes. We define a public interest algorithmic audit as investigatory research into an algorithm intended to discover and inform the public about potential harms caused by the algorithm. They can be performed by academics, public interest groups, journalists, or just concerned citizens. However, these investigators need access to adequate information in order to perform effective audits (which they do not always have).

Why Private Audits Are Not Enough

In contrast, private audits can be ineffective without basic auditing requirements and standards.¹⁸ Because the AI company is the one paying the private, third-party auditor (and generally there are no legal requirements for most AI companies to undergo an audit¹⁹), the AI company can essentially set its own standards for what the audit should entail, which could lead to weak and rather meaningless accountability measures.²⁰ AI companies can determine what types of audits they want to undergo, what specific algorithms they want to be audited, and how much of their information they want to give to auditors (even under a nondisclosure agreement). Companies can also choose which products to audit, keeping secret the ones that are failing while presenting a good public image. It is also likely that different auditing companies will have wildly different techniques in terms of which issues they search for and how they go about identifying them—Auditor A might obtain a significantly different impact assessment of a company's algorithm than Auditor B.

In the absence of auditing transparency requirements, companies that voluntarily undergo audits by private auditing companies can mischaracterize the results in a way that is misleading to the public. Private auditing companies offer auditing services to AI companies. However, because there are few, if any, legal requirements for a third-party audit,²¹ it is not clear that these services will identify or mitigate potential harms.²² A company could use inadequate private

¹⁸ Consider the case of the Arthur Andersen and Enron scandal. The firm Arthur Andersen served as both a consultant and auditor for Enron, which was a conflict of interest, and led to Arthur Andersen being indicted for obstruction of justice after destroying Enron audit information requested by the SEC (which essentially resulted in the downfall of both companies). Ken Brown and Ianthe Jeanne Dugan, "Arthur Andersen's Fall From Grace Is a Sad Tale of Greed and Miscues," *The Wall Street Journal*, June 7, 2002, <https://www.wsj.com/articles/SB1023409436545200>.

¹⁹ Proposed legislation such as the Algorithmic Accountability Act (S.3572 and H.R. 6580) and Washington State's SB 5116 (which failed in March 2022) would require auditing, but there are currently no industry-wide or legal standards to determine the kinds of information companies should provide to auditors about their technology in order for an audit to take place, and even what the audit should address. Because AI applications are diverse and varied, these standards need to be nuanced based on the context of the algorithm. One exception is a New York City law that would require a bias audit be conducted on an automated employment decision tool prior to the use of said tool.

²⁰ Megan Gray, "Understanding and Improving Privacy 'Audits' under FTC Orders," *The Center for Internet and Society: Stanford University*, April 2018, <http://cyberlaw.stanford.edu/files/blogs/white%20paper%204.18.18.pdf>.

²¹ The Federal Trade Commission has put out business guidelines for developing and using AI (<https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms>) that include testing algorithms for bias, making sure decisions are explainable to consumers, and more. While there are not necessarily laws that require testing in a particular way or at all, antidiscrimination law and other laws like Section 5 of the FTC Act could hold companies accountable for failing to identify and mitigate disparate impacts in their algorithms, stated here:

<https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai>.

²² Alfred Ng, "Can Auditing Eliminate Bias from Algorithms?" *The Markup*, February 23, 2021, <https://themarkup.org/ask-the-markup/2021/02/23/can-auditing-eliminate-bias-from-algorithms>.

audits to justify its business practices, rather than to address the potential harms caused by them. HireVue, a video software company that claimed to analyze people's faces during the job interview process, obtained the services of O'Neil Risk Consulting & Algorithmic Auditing (ORCAA) after the company had been widely criticized for allegedly being biased and using debunked pseudoscience to score applicants.²³ However, it was audited only for a narrow hiring test rather than its "candidate evaluation process as a whole."²⁴ HireVue claimed in a press release that the audit was successful, though the audit addressed only a specific issue.²⁵

Finally, companies being audited typically are not required to disclose results of these audits to the public, or to address any problems identified in the audit. The lack of transparency or risk mitigation requirements means companies can tout the fact they have undergone an audit (which can make them look more ethical or responsible as a company) without actually meaningfully addressing the issues identified by the audit.

Public interest audits generally lack the monetary incentives of private audits, and are done to uncover new information and identify potential issues that algorithms pose. Journalists and researchers generally play a part in providing the public with information in regards to issues that companies pose to the public, such as corruption, fraud, and more. And journalists and researchers should be given the same opportunities to do the same with AI companies, which in some cases can pose harm to the public or end-users of an AI application.

For example, researchers at New York University conducted a study called the 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.²⁶ While Facebook has an advertisement database available to the public that it claims contains all political ads shown to users, the Ad Observatory group found that Facebook routinely misses including political ads in this database²⁷ and sometimes fails to disclose who pays for some political ads.²⁸

It is not always seasoned researchers who can identify problems with algorithms. Twitter users noticed in 2020 that Twitter's image-cropping algorithm, which showed a preview of an image on a user's feed, was perhaps biased toward younger, slimmer, and lighter faces.²⁹ Due to the

²³ The company discontinued the use of "visual analysis" from its job interview assessments in early 2020. <https://www.hirevue.com/press-release/hirevue-leads-the-industry-with-commitment-to-transparent-and-ethical-use-of-ai-in-hiring>.

²⁴ Alfred Ng, "Can Auditing Eliminate Bias from Algorithms?"

²⁵ Id.

²⁶ Ultimately, Facebook ended up disabling the researchers' accounts, effectively ending the study. Lois Anne DeLong, "Facebook Disables Ad Observatory; Academicians and Journalists Fire Back," NYU Center for Cybersecurity, August 21, 2021, <https://cyber.nyu.edu/2021/08/21/facebook-disables-ad-observatory-academicians-and-journalists-fire-back>.

²⁷ Nancy Watzman, "The political ads Facebook won't show you," Cybersecurity for Democracy, Medium Blog, May 12, 2021, <https://medium.com/cybersecurity-for-democracy/the-political-ads-facebook-wont-show-you-e0d6181bca25>.

²⁸ Shirin Ghaffary, "People do not trust that Facebook is a healthy ecosystem," Vox, August 6, 2021, <https://www.vox.com/recode/22612151/laura-edelson-facebook-nyu-ad-observatory-social-media-researcher>.

²⁹ Alex Hern, "Student proves Twitter algorithm 'bias' toward lighter, slimmer, younger faces," The Guardian, August 10, 2021,

backlash, Twitter ended up giving more information on how it tests for bias in the image-cropping model, and also gave users more control over how their images were cropped before being published.³⁰

Clearly, public interest researchers can play a big role in identifying and mitigating harm posed by algorithms. However, the type of audit that can be executed and the extent to which a researcher is able to assess a model is highly dependent on the information they have access to. In the next few sections, we will discuss the different types of algorithmic audits, and the practical and legal limitations of each, and suggest policy recommendations to remove barriers to make it easier for researchers to conduct these audits.

<https://www.theguardian.com/technology/2021/aug/10/twitters-image-cropping-algorithm-prefers-younger-slimmer-faces-with-lighter-skin-analysis>.

³⁰ Parag Agrawal and Dantley Davis, “Transparency around image cropping and changes to come,” Twitter Blog, October 1, 2020, https://blog.twitter.com/official/en_us/topics/product/2020/transparency-image-cropping.html.

Introduction to Types of Audits

Public interest groups, academics, and journalists have a major role to play in identifying algorithmic harms, but legal and practical roadblocks often prevent public interest researchers from performing effective AI audits. The same laws that were created to promote science and art, and protect individuals and companies from hacking, are unfortunately also hindering researchers from performing meaningful audits, for fear of legal recourse. These include laws like the Computer Fraud and Abuse Act and copyright law, as well as tort and contract law.

Below, we will describe different types of audits, including code audits, crowdsourced audits, scraping, and sock puppet audits, and their practical and legal limitations for auditing algorithms to identify discrimination or other harms. All of the audit practices described are essential to conducting research on algorithmic discrimination and other harms. The auditor often selects the type of audit based on the availability of information about the system, as well as the resources they have to conduct the audit. Typically, researchers are limited in both access to the necessary information and resources to conduct the audit. Because the purpose of audits is to understand how and when a system works as well as when it fails, researchers need input or output data of a system, adequate staff, and powerful computers to conduct an effective audit.

The audit categories below are fairly generalized—there exist auditing practices that combine any or all of the categories and also practices that are perhaps more nuanced than any of the descriptions below. The categories chosen are derived from Christian Sandvig’s paper on algorithmic audits, but examples and categories have been changed slightly for the purposes of this paper to help distinguish between some of the legal and practical issues that exist between them.³¹

Each type of audit, when carried out by public interest groups, has both practical and legal limitations. We identify the main limitations posed by each audit—and where clear legal barriers exist, we suggest policy solutions to remove them.

1. Code Audit

Description:

The first type of audit is fairly straightforward: A code audit is when an auditor gains access to a company’s source code, which can be the underlying code of any model or algorithm. For example, Twitter made its image-cropping code public after it received backlash about the code’s potential biases.³² The public was able to review the code and test it to identify sources

³¹ Christian Sandvig, Kevin Hamilton, Karrie Karaholios, and Cedric Langbort, “Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms,” International Communication Association, May 22, 2014, <http://www-personal.umich.edu/~csandvig/research/Auditing%20Algorithms%20--%20Sandvig%20--%20ICA%202014%20Data%20and%20Discrimination%20Preconference.pdf>.

³² Kyra Yee, Uthaipon Tantipongpipat, and Shubhanshu Mishra, “Image Cropping on Twitter: Fairness Metrics, their Limitations, and the Importance of Representation, Design, and Agency,” arXiv, September 9, 2021, <https://arxiv.org/pdf/2105.08667.pdf>; Twitter research, Image crop analysis code, GitHub, <https://github.com/twitter-research/image-crop-analysis>.

of bias.³³ Recently, Elon Musk has suggested making Twitter's algorithms open source to increase trust.³⁴

In a code audit, a company can provide the auditor with either the entire codebase or the code regarding any potentially concerning aspects of the software or algorithm. In the case of algorithmic auditing, companies may also need to provide the auditor with training data and other relevant information so that the auditor can test out the system in a robust manner; often, auditors need this extra information to gain a full understanding of how the system works under different circumstances.

Practical Limitations:

Even with full access to an algorithm's code, a code audit on its own may not be useful to the auditor. Even to a sophisticated auditor, it may be difficult to look through thousands or millions of lines of code to identify sources of bias or harm.

Access to the code itself may also be insufficient on its own. It is also generally difficult to test an algorithm without using training and sample input data along with the algorithm itself.³⁵ If a company chooses to disclose its algorithm but not the data it uses, identifying discrimination and other harms may not be possible because the harms may arise only in the context of specific data usage or interaction with a user.³⁶

Finally, few companies are incentivized to make their code available for third-party auditing. Many treat their code as a competitive advantage and might worry that even data shared with one external partner could wind up in the hands of a competitor. If the code became widely available, bad faith actors could potentially find loopholes to game. For example, Google guards its search results algorithms closely and constantly adjusts them to combat search engine optimization efforts that could result in less relevant results for users. On the other hand, providing access to the code could reveal instances of bias or discrimination, subjecting the company to public embarrassment or even potential liability.

Legal Limitations:

Companies currently have little to no legal obligation to release their code to auditors or regulators. To the extent that an auditor tries to access or reverse engineer code without the company's permission, they risk violating hacking laws like the Computer Fraud and Abuse Act or the Digital Millennium Copyright Act, which prohibits circumventing technical measures to protect copyrighted material. And as mentioned above, access to an algorithm's underlying code

³³ Curt Wagner, "Hackathon Points to More Biases in Twitter Algorithm," PMCA, August 18, 2021, <https://www.pcma.org/defcon-hackathon-finds-more-biases-twitter-algorithm>.

³⁴ Twitter, Inc., April 25, 2022, <https://www.prnewswire.com/news-releases/elon-musk-to-acquire-twitter-301532245.html>.

³⁵ Amanda Levendowski, "How Copyright Law Can Fix Artificial Intelligence's Implicit Bias Problem," *Washington Law Review* 93, no. 2 (2018): 628, <https://robotic.legal/wp-content/uploads/2018/09/SSRN-id3024938.pdf>.

³⁶ For example, identifying the kinds of ads a person sees on Facebook's newsfeed cannot be done with just the algorithm alone—ads are deployed based on a user's interaction with a platform, so a researcher would need access to information such as how the user has interacted with other users or what they have previously clicked on in order to get a better picture of how the algorithm deploys ads for that individual.

is not usually enough—training data and other contextual data is necessary to robustly audit an algorithm.

In addition to copyright protections over the code, training datasets themselves could include copyrighted content like artwork or copyrighted text. Regardless of whether the company had the legal right to use the copyrighted images, researchers attempting to use the training data either to test algorithms or to reverse engineer potentially problematic algorithms could run into the issue of copyright infringement, even if the company willingly made it available.³⁷

The potential for exposure to liability for such infringement may disincentivize companies from releasing their datasets in the first place.³⁸ Also, depending on the originality of the selection and arrangement of the information in the dataset, companies might try to claim copyrightability over the dataset itself, disincentivizing research from other parties—public interest, adversarial, or otherwise—for fear of infringement litigation, regardless of whether or not the use may ultimately be fair.³⁹

2. Crowdsourced Audit

Description:

A crowdsourced audit is essentially a survey of users to gather data about their normal interactions with an algorithm or platform (for example, getting users to share all of their queries on a search engine). An auditor can get volunteers to either provide information about their interactions with the algorithm or provide direct access to the auditor (with consent) to view their interactions. For example, Consumer Reports has previously done similar participatory research to identify differences in insurance cost estimators offered to consumers and to identify roadblocks for consumers trying to exercise their rights under the California Consumer Privacy Act.⁴⁰

Practical Limitations:

While crowdsourced audits can be extremely useful in shining a light on companies' practices, they do have some important practical limitations. First, testers will self-select, and may not be representative of the general population, unless researchers make careful choices about which testers to use. For example, volunteer testers may already have strong opinions about the

³⁷ Consider an example where an algorithm was developed to look at images of flowers and classify them by species. If the training set of flower images was scraped from various photography websites that specialized in nature photography, researchers attempting to reverse engineer the algorithm would likely need to obtain flower images from similar websites. This could be a copyright violation if they did not obtain permission from the owners (because this can often be costly). Larger technology companies may have the resources to pay for damages due to copyright violation and could be willing to take the risk of using these images without owner permission, while public interest researchers may not have the same ability to do so.

³⁸ Levendowski, "How Copyright Law Can Fix Artificial Intelligence's Implicit Bias Problem," 597, footnote 77.

³⁹ *Feist Publications, Inc., v. Rural Telephone Service Co., Inc.*, 499 U.S. 340 (1991), <https://cyber.harvard.edu/people/tfisher/1991%20Feist.pdf>.

⁴⁰ "How We Rate Health Insurance Plan Tools and Public Price Estimator Tools," Consumer Reports, November 2016, https://article.images.consumerreports.org/prod/content/dam/cro/news_articles/health/PDFs/Consumer_Reports_Health_Insurance_Tool_Ratings_Technical_Report.pdf; Maureen Mahoney, Ginny Fahs, and Don Marti, "The State of Authorized Agent Opt Outs Under the California Consumer Privacy Act," Consumer Reports, February 2021, https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_AuthorizedAgentCCPA_022021_VF_.pdf.

product or interact with it in particular ways that can skew a sample, similar to how people with strong opinions are often more likely to respond to surveys or give ratings. To be most helpful, the users sampled must exhibit a variety of attributes in order to properly identify discrimination or other potential harms.

Even with a good sample, it can be difficult for researchers to identify causality between the inputs and outputs of the algorithm; outputs could be the result of any number of factors, including previous interactions between a user and the system (which could affect future interactions, like search engine results or advertisement suggestions), which may not properly be identified to researchers.⁴¹ There can also be self-reporting errors made when users share information with the researcher. The use of sock puppet audits (*see infra*, #4) that afford researchers more control over inputs could solve many of the issues presented by crowdsourced user audits, though they also present different legal and practical challenges.

Legal Limitations:

A company's terms of service agreement could purport to limit users' participation in certain audits. For example, a website could prohibit a researcher performing a crowdsourced audit from using a volunteer's information to log in to collect data, even when the volunteer gives consent to do so, or prohibit individuals from disclosing information about their accounts or user experiences to researchers or the public.⁴² Companies have broad discretion in crafting website terms of service, and could potentially try to use contract language to frustrate crowdsourcing. In some cases, courts and regulators have found that contractual provisions that limit the publication of testing results are legally "unconscionable" or contrary to public policy.⁴³ Furthermore, the Consumer Review Fairness Act prohibits contracts from preventing consumers from giving honest reviews about a product or service.⁴⁴ However, sometimes companies may have a legitimate interest in preventing their users from sharing certain data related to their products, especially if sharing could infringe the rights of others. For example, Facebook cited concern about others' privacy when shutting down Cambridge Analytica's access to Facebook's APIs after it had exposed a loophole that allowed Cambridge Analytica to collect data not only of individuals who had taken a particular online quiz but also of their Facebook friends.⁴⁵

There is also some legal uncertainty whether violating terms of service (ToS) agreements constitutes a violation of the Computer Fraud and Abuse Act (CFAA) or other state computer hacking laws. A prosecutor could allege that accessing a computer service in contravention of its stated terms and conditions could constitute illegal hacking. The Supreme Court recently ruled in *Van Buren v. United States* that an individual given access to a database but who

⁴¹ Christian Sandvig et al., "Auditing Algorithms," 11.

⁴² James Snell, Nicola Menaldo, and Ariel Glickman, "CFAA Decision May Raise Bar On Scraping Liability," Perkins Coie LLP, August 7, 2020, <https://www.perkinscoie.com/images/content/2/3/236192/Law360-CFAA-Decision-May-Raise-Bar-On-Scraping-Liability.pdf>.

⁴³ *FTC v. Roca Labs, Inc.*, 345 F. Supp. 3d 1375 (M.D. Fla. 2018); *McAfee v. State of New York*, 149 N.Y.S.2d 547 (N.Y. Misc. 1956).

⁴⁴ 15 USC §45b.

⁴⁵ Mark Zuckerberg, Update on Cambridge Analytica, Facebook, March 21, 2018, <https://www.facebook.com/zuck/posts/10104712037900071>; Alvin Chang, "The Facebook and Cambridge Analytica scandal, explained with a simple diagram," Vox, May 2, 2018, <https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram>.

accessed the database for unauthorized purposes *did not* violate the CFAA.⁴⁶ Nevertheless, there remains the possibility that another judge looking at a different set of facts could determine that accessing a service in violation of its policies violates the CFAA, or state statutes that vary significantly in wording and scope.

3. Scraping Audit

Description:

In a scraping audit, a computer program extracts data, typically publicly available data, by repeatedly querying the algorithm and obtaining or otherwise observing the results. For example, Googlebot, Google's crawler that automatically discovers and scans websites to index in its search engine, is one of the most prolific web crawlers on the internet. Scraping is generally done by using automated scraping tools, such as a browser extension, that can accomplish specifically what the user asks it to do (such as collecting all the images in a publicly accessible website).

There are certain standards that are put in place to facilitate interactions between websites and bots. The "robot exclusion standard"—also known as "robots.txt"—allows the operator of a website to indicate whether, and to what extent, the bots can scan the website.⁴⁷ However, the robots.txt signal is only a signal; whether this request not to be scanned has any legal effect depends on jurisdiction. In most jurisdictions, the law is unclear.⁴⁸ In practice, there are plenty of bots on the internet that disregard the robots.txt standard completely.⁴⁹

There can also be some overlap between scraping and the crowdsourced audit, which can sometimes differentiate based on whether or not there was user consent to data collection. Researchers at New York University created a browser plug-in called "Ad Observer" that attempts to study advertisements featuring political content and misinformation on Facebook and YouTube.⁵⁰ The platform users could opt-in to the study by adding the plug-in to their browser, which allowed the research group to scrape advertisements seen on the users' newsfeed. The results were then aggregated in an effort to learn how ads are targeted on the Facebook platform.

Practical Limitations:

Platforms may try to prevent researchers from scraping their sites. NYU's Ad Observer collected information only about the advertisement, including the information Facebook gives about why the ad was targeted to that particular user, who the advertiser is, and the advertisement itself. It

⁴⁶ *Van Buren v. United States*, 206 L. Ed. 2d 822 (D.D.C. 2020). Previously, at least one lower court (*Sandvig v. Barr*, U.S. District Court for the District of Columbia) concluded that the CFAA does not criminalize violations of ToS, because criminalizing constitutionally protected speech that happens to violate a ToS would be a serious threat to the First Amendment. Naomi Gilens and Jamie Williams, "Federal Judge Rules It Is Not a Crime to Violate a Website's Terms of Service," Electronic Frontier Foundation, April 6, 2020, <https://www.eff.org/deeplinks/2020/04/federal-judge-rules-it-not-crime-violate-websites-terms-service>.

⁴⁷ Essentially, a website owner can place a text file in the root of the website hierarchy in a particular format that signals to the bot where it is allowed to scan, if allowed at all. "About robots.txt," <https://www.robotstxt.org/robotstxt.html>.

⁴⁸ "Can a /robots.txt be used in a court of law?" <https://www.robotstxt.org/faq/legal.html>.

⁴⁹ Rachel Costello, "Robots.txt," Deepcrawl, <https://www.deepcrawl.com/knowledge/technical-seo-library/robots-txt/>.

⁵⁰ Ad Observer, NYU Cybersecurity for Democracy, <https://adobserver.org>.

did not share any identifiable information about the user or their friends.⁵¹ Nevertheless, in August 2021, Facebook disabled the accounts of the researchers conducting the study, effectively halting their research.⁵² Critics of the move suggested that Facebook was concerned the researchers could use the tool to gain insight into how Facebook’s ad-targeting algorithm works, how the company utilizes users’ information to target advertisements, and how its algorithms contribute to misinformation.⁵³

Legal Limitations:

As with crowdsourced audits, non-technical access restrictions such as contracts (like a terms of service) could also be used to chill algorithmic audits. In 2022, the Ninth Circuit ruled in *HiQ Labs, Inc. v. LinkedIn Corp.* that accessing information on publicly available websites—or accessing information behind a technological barrier when the user is given authorization—is not a violation of the CFAA.⁵⁴ While this decision is good news for AI researchers and auditors seeking to identify discriminatory outcomes or other harmful effects of algorithms, it may not extend to scraping of other non-public data sets to which a user has legitimate access.

An auditor scraping a public website without permission or in contravention to a robots.txt signal opting out of scraping could potentially be liable for common law trespass to chattels (or property) as well. Initially, some courts held that trespass to chattels can be a viable way to claim injury due to scraping, if there is demonstrable harm to the host computer or network. Generally, this term means an owner can claim injury if someone uses their property without the owner’s permission; in the case of computers, the “property” can refer to a computer system or network.⁵⁵ In *eBay, Inc. v. Bidder’s Edge, Inc.*, eBay successfully argued that, while Bidder’s Edge’s spidering activity minimally harmed eBay’s systems, a preliminary injunction could discourage more companies from doing the same—to not do so would encourage other companies to use web crawlers, hurting eBay’s servers with this increased use of activity.⁵⁶ Other courts have since been more skeptical. In *Ticketmaster Corp. v. Tickets.com, Inc.*, a court held that scraping information from a public website on its own was not sufficient to show the physical injury to the host computer or network required in a trespass action, stating: “This court respectfully disagrees with other district courts’ finding that mere use of a spider to enter a publically available website to gather information, without more, is sufficient to fulfill the harm requirement for trespass to chattels.”⁵⁷ There are, of course, legitimate reasons why a website owner would choose to not allow bots or other crawlers to access its web pages. Excessive bots can create high website traffic, which can strain servers and hurt the website’s performance. Certain websites could also set prices for their products depending on traffic, so this could be

⁵¹ *Id.*

⁵² The research project continues to provide a searchable database of ads but has not disclosed from where it is receiving data. Mark Scott, “Fight over online political ads heats up ahead of midterms,” Politico, August 3, 2022, <https://www.politico.com/news/2022/08/03/2022-midterms-online-political-ads-00049373>.

⁵³ Barbara Ortutay, “Facebook shuts out NYU academics’ research on political ads,” AP News, August 4, 2021, <https://apnews.com/article/technology-business-5d3021ed9f193bf249c3af158b128d18>.

⁵⁴ *HiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (9th Cir. 2019).

⁵⁵ “Trespass to Chattels,” Internet Law Treatise: Electronic Frontier Foundation, https://ilt.eff.org/Trespass_to_Chattels.html.

⁵⁶ *eBay, Inc. v. Bidder’s Edge, Inc.*, casebriefs.com, <https://www.casebriefs.com/blog/law/intellectual-property-law/intellectual-property-keyed-to-merges/state-intellectual-property-law-and-federal-preemption/ebay-inc-v-bidders-edge-inc>.

⁵⁷ *Ticketmaster Corp. v. Tickets.com, Inc.*, 2003 WL 21406289 (C.D. Cal. Mar. 7, 2003).

harmful to consumers if bot traffic artificially drives up prices (although this may be something a consumer-focused researcher would want to examine). Furthermore, scraping (using a bot or otherwise) can sometimes be harmful if a company chooses to use the data for potentially offensive purposes. Clearview AI, a controversial company that sells facial recognition tools to law enforcement, obtained billions of images used to train its models to identify individuals by scraping social media platforms and is now facing legal action from multiple governments.⁵⁸

Because the design of a website or the content it contains may be copyrightable, when a researcher scrapes (copies) a website's content or information (for example, artwork for testing or reverse engineering an image processing algorithm), those researchers may open themselves up to liability for copyright infringement litigation. In *Ticketmaster Corp. v. Tickets.com, Inc.*, for instance, the court accepted that Ticketmaster's website was copyrightable but determined that Tickets.com spidering activity was fair use.⁵⁹ Fair use is a doctrine of U.S. copyright law allowing that the use of a copyrighted work "for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright."⁶⁰ However, fair use is not a foolproof fail-safe, because the potential for high litigation costs to determine whether or not the use of a copyrighted work constituted a fair use can be a significant barrier for under-resourced or risk-averse entities likely to be conducting public interest research.

Even when using copyrighted material is considered fair use, the Digital Millennium Copyright Act prohibits the circumvention of technological measures that control access to copyright-protected works. This could include encryption systems, password-protected sections of websites, or digital rights management (DRM) software that is put in place to block access to copyrighted works—which includes software in which there is a copyright interest.⁶¹ The law also prohibits the trafficking of tools put in place to help people circumvent these protection measures,⁶² which could place in legal jeopardy researchers putting out APIs or other tools that allow individuals to audit algorithms.⁶³

4. Sock Puppet Audit

Description:

In a sock puppet audit, a researcher creates fake accounts or programmatically constructed traffic for testing an algorithm. This gives the auditor control over each account's characteristics, making it easier to identify causality for discrimination or other harms. Another benefit is that

⁵⁸ "Clearview AI's unlawful practices represented mass surveillance of Canadians, commissioners say," Office of the Privacy Commissioner of Canada, February 3, 2021, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c_210203/?=february-2-2021.

⁵⁹ *Ticketmaster Corp. v. Tickets.com, Inc.*, 2003 WL 21406289 (C.D. Cal. Mar. 7, 2003).

⁶⁰ 17 USC §107.

⁶¹ Pub. L. 105-304.

⁶² "Circumventing Copyright Controls," Digital Media Law Project: Berkman Klein Center for Internet and Society, September 10, 2021, <https://www.dmlp.org/legal-guide/circumventing-copyright-controls>.

⁶³ Consumer Reports has previously supported exemptions to section 1201 of the DMCA for good faith security research. <https://advocacy.consumerreports.org/wp-content/uploads/2021/03/DMCA-13-expanding-security-research-3-9-21-FINAL-1.pdf>.

auditors can assign characteristics to the fake accounts that volunteer participants might be hesitant to declare (such as medical history or sexual orientation).⁶⁴

Practical Limitations:

Depending upon the nature of the study, the number of sock puppet accounts created may need to be quite large. This can be time-consuming and expensive, which is why semi-automated crowdsourcing like Amazon's Mechanical Turk is sometimes used for these studies.

Another drawback to this type of audit is that injecting large amounts of fake accounts into a system could tamper with the system in a way that interferes with the audit. For example, artificial traffic could drive up prices if a company notices there is high demand for a particular product.

Platforms that are designed to detect or deactivate fake accounts (or even identify third-party tests being done on their own system) could be able to remove these accounts before an audit is complete. This could be done to deliberately frustrate the audit or could simply be a result of standard efforts to detect and remove inauthentic accounts. Alternatively, a company could deliberately present different results to sock puppet accounts in order to present a better (and misleading) picture about the results generated by its algorithms.

Legal Limitations:

Similar to the previous auditing examples, breach of contract (if a ToS prohibits the creation of fake accounts, even for research purposes)⁶⁵ and trespass to chattels could be asserted against researchers creating fake accounts to conduct a sock puppet audit. Because platforms have legitimate reasons to monitor and delete fake accounts to avoid artificially inflated user counts or content promotion and to limit abuse of network resources, a court may be sympathetic to a legal challenge against even fake accounts created for auditing purposes.

In *Sandvig v. Barr*, academic researchers sought to study whether certain employment websites discriminated based on certain characteristics, and hoped to make fake accounts with these characteristics to examine how the platforms' algorithms behaved; however, this method violated many websites' terms of service. The researchers brought a pre-enforcement First Amendment challenge, alleging that the CFAA as applied to ToS violations chilled their free speech.⁶⁶ The court concluded that the CFAA does not criminalize violations of ToS, because criminalizing constitutionally protected speech that happens to violate a ToS would be a serious threat to the First Amendment.⁶⁷

Policy Recommendations

Clearly, the legal and practical impediments to good faith public interest auditing are vast and could hinder research into identifying algorithmic harms. The various laws mentioned could

⁶⁴ Christian Sandvig et al., "Auditing Algorithms," 14.

⁶⁵ James Snell et al., "CFAA Decision May Raise Bar On Scraping Liability," Perkins Coie LLP.

⁶⁶ *Sandvig v. Barr*, 451 F. Supp. 3d 73 (D.D.C. 2020).

⁶⁷ *Id.*

pose a legal threat to auditors, preventing them from tinkering with algorithms for fear of legal recourse. We propose recommendations on ways to carve out exemptions to existing law to promote this research. Furthermore, we also provide recommendations on mandating data and code access in some cases to researchers to make model evaluation easier.

1. Access and Publication Mandates

Though code audits may not be necessary for lower-stakes applications of AI, for particularly sensitive applications, the code governing these decisions should be made available to the public, along with the training and testing data used. First, government uses of algorithms such as bail decisions in law enforcement and basic resource allocation should be transparent to the public, because these decisions impact people's liberties and basic rights (if these algorithms are to be used at all; a particular state bill would ban such sensitive algorithmic decision-making⁶⁸). Disclosure of code or an API that researchers can use to test an algorithmic system should also be provided when it has the potential to affect the public in dangerous ways (for example, if an algorithm is pointing users to wrong or harmful information regarding public health).

Second, government agencies and their technology vendors should frequently update their publicly available code and datasets—whenever significant changes are made. Engineers are constantly testing and updating their algorithms, and datasets can often become outdated or updated to more accurately train models. For algorithms with significant legal effects, disclosure of code and training data would need to be published regularly to reflect changes.

As mentioned, the datasets used to train algorithms are also often necessary to properly audit those same algorithms—giving researchers access to just code may not be enough. Due to potential copyright infringement issues, we recommend a safe harbor for researchers using copies of AI training data for public interest purposes or that such use be considered fair use.

Platforms should put in place a process for researchers either to create fake accounts for auditing purposes or to appeal takedowns of research-related fake accounts. The platforms should also treat these accounts the same way they do their regular users; platforms should not be able to frustrate testing.⁶⁹ This may be difficult for smaller companies to implement but should be required for larger ones (determined by user count or annual revenue).

Finally, whether an algorithm is open-source or not could also be a factor to consider in assessing an AI designers' liability for discrimination, because transparency could be deemed a good faith effort at rooting out bad outcomes. Some companies choose to make their software open-source (or available to the public so that anyone can inspect, download, and test their code). While in some cases there could be a competitive disadvantage for a company to make its code public, there are numerous advantages in terms of reducing algorithmic bias and other harms. Anyone, including auditors, can inspect the code and test for issues—they can also

⁶⁸ S.B. 5116, 67th Legislature, 2021 Regular Session (Washington 2021), <https://lawfilesexternal.wa.gov/biennium/2021-22/Pdf/Bills/Senate%20Bills/5116.pdf?q=20210810140732>.

⁶⁹ Frustrating testing for algorithmic harm/bias could be considered an unfair/deceptive practice or an unfair method of competition.

notify the company if anything concerning is found so that the company can fix it. Auditors can also provide code or other suggestions on how to improve the software.

2. CFAA and Computer Trespass

Recent decisions such as *HiQ* and *Van Buren* have found that users who had legitimate access to a computer service did not violate the CFAA when they exceeded the policy limitations imposed on such access.⁷⁰ This reduces the likelihood that the CFAA could be used against public interest researchers querying a database to test for bias, potentially in violation of a company's terms of service. In fact, the Department of Justice recently released a statement to federal prosecutors saying that it would not use the CFAA to prosecute good faith researchers attempting to identify security vulnerabilities.⁷¹ While the DOJ did not mention whether this new policy would also apply to researchers of algorithmic bias and other harm, it could indicate the DOJ would be more hesitant to prosecute researchers working for the public good.

Nevertheless, the holdings of recent cases are necessarily limited to the fact patterns in question in those cases, and a court looking at a slightly different scenario could decide that the CFAA limits unwanted testing of an algorithm. Moreover, many of these decisions apply only to the Computer Fraud and Abuse Act itself: There may exist potential causes of action under comparable state statutory law or common law trespass to chattels. Policymakers should consider targeted reforms of these laws to ensure that good faith public interest research that does not meaningfully tax a company's resources or compromise other interests (such as privacy) is allowed—even for public-facing sites that use a robots.txt flag.

3. Contract Law

Today, many companies put language into terms of service or license agreements purporting to limit researchers' ability to access their systems to test for bias or other problems. Even if such clauses do not trigger the Computer Fraud and Abuse Act, they could still be the basis for private litigation against a user. At the very least, the threat of such a lawsuit could serve to deter audits that could uncover serious problems.

Under existing contract law, courts may determine that such clauses are unconscionable and void as against public policy.⁷² However, that possibility does not provide certainty to risk-averse researchers who are likely to lack the resources to litigate against a large tech company.

Legislators should consider enacting legislation that explicitly prohibits contractual language unfairly limiting researchers' ability to audit algorithms for bias. Policymakers regularly pass laws

⁷⁰ Andrew Crocker, "Scraping Public Websites (Still) Isn't a Crime, Court of Appeals Declares," Electronic Frontier Foundation, April 19, 2022,

<https://www.eff.org/deeplinks/2022/04/scraping-public-websites-still-isnt-crime-court-appeals-declares>.

⁷¹ <https://www.justice.gov/opa/press-release/file/1507126/download>.

⁷² "Contracts Considered to be Contrary to Public Policy," UpCounsel,

<https://www.upcounsel.com/what-contracts-are-considered-to-be-contrary-to-public-policy>; Paul Bennett Marrow, "Contractual Unconscionability: Identifying and Understanding Its Potential Elements," Columbia.edu, 2000.

prohibiting the use of clauses that violate public policy interests: California, for example, prohibits noncompete clauses in employment contracts,⁷³ and President Biden recently signed a law that prohibits mandatory arbitration for sexual harassment claims, as well as claims of retaliation resulting from internal complaints of sexual assault or harassment.⁷⁴

In 2016, Congress passed the Consumer Review Fairness Act, which bans contractual clauses that limit a consumer's ability to post honest reviews about a company online. However, this law does not explicitly cover clauses that limit the underlying testing that could lead to a negative review. To better facilitate transparency and accountability, the protections in this law could be extended to ban anti-testing clauses as well.

4. DMCA

The Library of Congress may create temporary exemptions every three years from the anti-circumvention provisions of Section 1201(a) for specified purposes, such as reverse engineering for security research.⁷⁵ The security research exemption might be read to encompass scraping to access works for algorithmic bias or harm testing for particular applications with significant legal effects. If not, an exemption to that effect should be proposed to the Copyright Office in the next Triennial Review, due to begin in mid-2023, and to conclude with new exemptions in late 2024. Or Congress could codify a new exemption in the statute itself.

5. Copyright

If the database underlying the development of an algorithm is copyrightable, then the unlicensed use of those works for algorithmic auditing should be considered fair use. Ultimately, researchers should not have to worry about whether the data they scrape in order to reverse engineer and train or test algorithms to identify harms leads to penalties from copyright infringement.⁷⁶

6. Civil Rights, Privacy, and Security

Consumer Reports has long supported comprehensive privacy and security legislation to protect consumers.⁷⁷ Privacy and security rules should apply to public interest audits as well. While

⁷³ "Attorney General Bonta Reminds Employers and Workers That Noncompete Agreements Are Not Enforceable Under California Law," Press Release From CA Attorney General, March 15, 2022, <https://oag.ca.gov/news/press-releases/attorney-general-bonta-reminds-employers-and-workers-noncompete-agreements-are>.

⁷⁴ Public Law no: 117-90. Text: <https://www.congress.gov/117/plaws/publ90/PLAW-117publ90.pdf>.

⁷⁵ "Section 1201 Exemptions to Prohibition Against Circumvention of Technological Measures Protecting Copyrighted Works," U.S. Copyright Office, <https://www.copyright.gov/1201/2021>.

⁷⁶ "More Information on Fair Use," U.S. Copyright Office, <https://www.copyright.gov/fair-use/more-info.html>.

⁷⁷ Maureen Mahoney and Justin Brookman, "Consumer Reports Model State Privacy Act," Consumer Reports Digital Lab, February 2021, https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf.

there is clear societal value to such research, that does not mean that researchers should have unfettered access to private data stores. Research exceptions to privacy laws should be narrowly tailored to be consistent with reasonable consumer expectations, and new access mandates to facilitate public interest research should limit third-party access to identifiable information. To the extent possible, data should be deidentified and aggregated before being handed over, and researchers should generally be prohibited from secondary use or sharing of data obtained for auditing purposes.

New privacy law should also include civil rights provisions that update decades-old protections to account for technologies such as artificial intelligence. Today civil rights protections are governed by different sector-specific statutes, each with its own standards and interpretations that have evolved over the years. However, in many cases, it is not clear how these protections apply when discriminatory outcomes are driven by a machine learning algorithm instead of by a conscious choice on the part of a company. Privacy legislation should comprehensively provide that discrimination that results in a loss of economic opportunities or access to public accommodations for members of protected classes is prohibited.⁷⁸ Bills like the recently introduced American Data Privacy and Protection Act take into account civil rights and algorithms, but the U.S. has yet to pass federal data privacy legislation.⁷⁹

7. Consumer Protection Law

General purpose consumer protection law prohibits companies from engaging in “deceptive practices.” Most deception cases are predicated on a company deceiving *a consumer*—such as lying about product attributes or misstating fees. However, other types of deceptive behavior can harm the marketplace and result in consumers being misled.

Companies that become aware they are subject to a public interest audit may make the decision to feed testers inaccurate information in order to paint a positive but misleading picture. Volkswagen famously settled after installing defeat devices⁸⁰ in certain diesel vehicles to detect when a car was being operated in a test environment in order to change pollution levels.⁸¹ A third-party testing service has accused a cell phone manufacturer of engaging in similar tactics to game benchmarking tests.⁸² An algorithm developer being tested for bias could try to detect auditors testing for bias and send them cleansed results reflecting an inaccurate depiction of normal results.

Currently the law is not entirely clear as to when deceiving third-party testers is illegal. The Federal Trade Commission settled a multibillion dollar case with Volkswagen, but its deception claims were based on deceiving consumers as to the environmental impact of its diesel

⁷⁸ “Consumer Reports Model State Privacy Act,” 12.

⁷⁹ American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

⁸⁰ The EPA defines a defeat device as “any device that bypasses, defeats, or renders inoperative a required element of the vehicle’s emission control system,” <https://www.epa.gov/vw/learn-about-volkswagen-violations>.

⁸¹ “Volkswagen Clean Air Act Civil Settlement,” Environmental Protection Agency, <https://www.epa.gov/enforcement/volkswagen-clean-air-act-civil-settlement>.

⁸² Chris Smith, “Geekbench bans Galaxy S22 for cheating in benchmark tests,” BGR, March 7, 2022, <https://bgr.com/tech/geekbench-bans-galaxy-s22-for-cheating-in-benchmark-tests>.

engines, not that Volkswagen deceived testers.⁸³ The FTC’s Policy Statement on Deception—an informal but influential explanation of how the FTC interprets its legal authority—says that to allege deception, “there must be a representation, omission or practice that is likely to mislead *the consumer*” (emphasis added).⁸⁴ The FTC should update this nearly 40-year-old guidance to account for other forms of deception, and otherwise clarify to companies that providing misleading test results is actionable under the law.

⁸³ “In Final Court Summary, FTC Reports Volkswagen Repaid More Than \$9.5 Billion To Car Buyers Who Were Deceived by ‘Clean Diesel’ Ad Campaign,” Federal Trade Commission Press Release, July 27, 2020, <https://www.ftc.gov/news-events/news/press-releases/2020/07/final-court-summary-ftc-reports-volkswagen-repaid-more-95-billion-car-buyers-who-were-deceived-clean>. The FTC also alleged that Volkswagen’s behavior was “unfair” to consumers because they were induced to purchase vehicles with a lower-than-expected resale value. Regulators could potentially bring similar unfairness claims against other companies that deceive testers, resulting in consumers purchasing products with less-than-expected functionality. However, to prove unfairness, regulators typically must allege elements—such as “substantial injury”—and that those harms were not offset by countervailing benefits. Further, many consumer protection regulators do not have unfairness authority; they can only bring deception cases. As such, deception should be available to regulators as a tool to proceed against companies that evade third-party auditing.

⁸⁴ “FTC Policy Statement on Deception,” Federal Trade Commission, October 14, 1983, https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

Other Frameworks to Incentivize Public Interest Audits

Bug Bounty Programs for Algorithms

Bug bounty programs have previously been used by many websites and other software companies to identify and fix security vulnerabilities.⁸⁵ Generally, these companies offer compensation and recognition to individuals who can identify these vulnerabilities.

Companies like Twitter have been using this process to let the public identify issues with certain algorithms the platform uses. Twitter recently received backlash when it was discovered that its image-cropping algorithm, which showed previews of images and videos people tweeted, was shown to be biased toward younger, slimmer, and lighter faces.⁸⁶ For its algorithmic bias bug bounty program, the company released its code for this specific image-cropping algorithm and asked that individuals identify and taxonomize the potential harms that an algorithm like this can produce.⁸⁷

However, Twitter's bug bounty program addressed only one algorithm used on the platform—the image-cropping algorithm is not the root cause of some of the major algorithmic problems that the platform continues to host, such as opaque content moderation practices, amplification of misinformation on the platform, and harmful advertisement delivery to users. It is unlikely that Twitter would publicly release the code to these algorithms that are central to its business, but allowing researchers this access would obviously be a more transparent way for the public to understand how these problems arise and might force Twitter to address these issues.

These platforms should allow the public to view their code and tackle some of their larger problems in exchange for reduced liability for potential harms if they act in good faith. Bounty programs should be considered relevant when assessing whether a company has met its obligations to root out bias or other algorithmic harm. However, companies will always have the best and most sophisticated view into their own systems; companies cannot simply punt their own obligations to assess systems for bias to the public via bounty programs.

⁸⁵ In December 2021, the Department of Homeland Security (DHS) announced a bug bounty program to identify potential cybersecurity vulnerabilities in certain DHS systems. Cybersecurity researchers were vetted to gain access to certain external DHS systems in order to find vulnerabilities and be compensated for the bugs they identify; "DHS Announces 'Hack DHS' Bug Bounty Program to Identify Potential Cybersecurity Vulnerabilities," U.S. Department of Homeland Security, December 14, 2021, <https://www.dhs.gov/news/2021/12/14/dhs-announces-hack-dhs-bug-bounty-program-identify-potential-cybersecurity>.

⁸⁶ Alex Hern, "Student proves Twitter algorithm 'bias' toward lighter, slimmer, younger faces," The Guardian, August 10, 2021, <https://www.theguardian.com/technology/2021/aug/10/twitters-image-cropping-algorithm-prefers-younger-slimmer-faces-with-lighter-skin-analysis>.

⁸⁷ "Twitter Algorithmic Bias," HackerOne, <https://hackerone.com/twitter-algorithmic-bias?type=team>.

Whistleblower Protections

Whistleblowing has the potential to be an effective way for employees to enact changes on company practices, which can include mitigating harmful algorithms. Due to the general lack of requirements that are placed on companies to be transparent about algorithmic bias, whistleblowers can often expose problems to the public that companies have no real incentive to disclose or address—particularly when the disclosure of such information could harm profits. In 2020, Google effectively forced out a top AI ethics researcher for trying to publish a paper critiquing the kinds of algorithms (large language models) that Google uses. The paper pointed out some of the harms that can come from these models, as well as other ethical considerations concerning these algorithms.⁸⁸ The conclusions of the paper itself were not entirely novel. However, this resulting controversy has led to suspicions that the creation of ethics teams within private companies may be little more than a PR stunt and that these teams do not necessarily have sway in terms of internal engineering practices and the products themselves.

It is clear that many AI companies cannot be trusted to always regulate themselves or be forthcoming about the issues in their algorithms. Whistleblowers can play an important role in providing the public and regulators with some clarity about how algorithms work and their associated impacts, particularly when companies perhaps know what the issues are but choose not to disclose or address these problems. Today, there are few protections given to whistleblowers in terms of disclosing issues related to AI. We will outline some potential policy changes that can provide some protections to whistleblowers while being fair to companies that are attempting to address discriminatory impacts of their products in good faith.

We recommend enacting protections for whistleblowers who attempt to disclose anything from algorithmic bias against protected classes to flawed research methodologies or data collection practices to false claims made by the company about its products. Individuals who bring up these issues internally to upper management if the company does not adequately address them within a certain time period, or for deployed models where potential discrimination is already in effect, should be protected from retaliation. This would include prohibiting whistleblowing in particular cases from affecting the employee's job status and prospects for promotion.

We also favor an approach that affirmatively incentivizes and protects whistleblowing (generally in the form of awards). As models, the Whistleblower Protection Enhancement Act (WPEA) protects federal employees who report fraud and abuse,⁸⁹ and the False Claims Act's qui tam provision protects anyone with evidence of fraud against federal programs or contracts and has awards for doing so. The IRS also has a whistleblower award for those who report on individuals who fail to pay the taxes they owe.⁹⁰ Other examples include the Sarbanes-Oxley Act, which provides whistleblower protections at public companies to encourage fraud reporting,

⁸⁸ Khari Johnson, "AI ethics pioneer's exit from Google involved research into risks and inequality in large language models," VentureBeat, December 3, 2020, <https://venturebeat.com/2020/12/03/ai-ethics-pioneers-exit-from-google-involved-research-into-risks-and-inequality-in-large-language-models>.

⁸⁹ "Whistleblower Information," U.S. CPSC Office of Inspector General, <https://oig.cpsc.gov/whistleblower-information>.

⁹⁰ "Whistleblower Office," Internal Revenue Service, <https://www.irs.gov/compliance/whistleblower-office>.

and to some extent the protections apply to private companies if they provide services for publicly traded ones.⁹¹ Senator Brian Schatz (D-Hawaii) and Senator John Thune (R-S.D.) introduced the Platform Accountability and Consumer Transparency (PACT) Act in 2020, which would require the Government Accountability Office to study and report on the viability of an FTC-administered whistleblower and awards program for employees or contractors of online platforms.⁹²

We also recommend prohibiting companies from forcing employees to sign nondisclosure or non-disparagement agreements regarding algorithmic bias or other unfair practices or outcomes regarding their company's technology. As a reference, California's Senate Bill 331, "The Silenced No More Act," adopted in 2021, prohibits workers from being forced to sign NDAs regarding all forms of worker discrimination and harassment in the workplace⁹³ (previous law in CA addressed only sexual harassment).

Furthermore, copyright law could hinder whistleblowers from publicly posting data or other information about algorithms. If an employee wanted to post a dataset their company was using to indicate its issues, this could be copyright infringement if the data itself was protected by copyright (for example, if the dataset contained artwork). We recommend that whistleblowers making copyrighted data related to algorithms publicly available for the purposes of disclosing its harmful effects should be considered a fair use case.

Conclusion

Certain applications of AI have the potential to roll back much of the progress made by civil rights law. Due to the lack of transparency on how these algorithms are used, the data used to train them, and how engineers go about mitigating harm when designing these algorithms, many of these algorithms may very well be discriminating against protected classes and perpetuating other kinds of harm. While the burden must not fall entirely on public interest researchers to uncover algorithmic harm, we must clear the legal barriers that hinder important public interest research as we advocate for robust algorithmic regulation in the U.S.

⁹¹ Sarbanes-Oxley Act, 18 U.S.C. §1514A.

⁹² PACT Act, S. 4066, 116th Cong. (2020).

⁹³ S.B. 331, California State Senate, 2021 Reg. Sess., (Cal. 2021), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220SB331; "California Silenced No More Act," Silenced No More Foundation, <https://silencednomore.org/the-silenced-no-more-act>.