Comments to the Federal Trade Commission re:
Commercial Surveillance ANPR, R111004

Submitted by:

Electronic Frontier Foundation

November 21, 2022

Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94104

The Electronic Frontier Foundation is pleased to submit comments to the Federal Trade Commission regarding its Advance Notice of Proposed Rulemaking on commercial surveillance and data security practices, and how data is collected, analyzed, and monetized. EFF is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. We work to ensure that rights and freedoms are enhanced and protected as our use of technology grows. EFF represents more than 35,000 dues-paying members, including consumers, hobbyists, artists, computer programmers, entrepreneurs, students, teachers, and researchers.

EFF has long advocated for privacy protections that centers around consumers and their autonomy. Right now, people are faced with many practices that limit their ability to interact with companies on their own terms. This is true at every stage of data processing, from the moment someone navigates to a website to the point when their information is sold, shared, or accessed—and then often resold, reshared, and accessed again—without their permission in the pursuit of profit.

Data is often thought of an impersonal commodity. But data is highly personal. Where we go online or in the real world, who and how we communicate with our communities, how and when we pay for things, our faces, our voices: all these data points represent aspects of individuals' lives that should be protected and handled carefully. Often, even when stripped of "personally identifying" characteristics, companies can reassemble such points—sometimes in shockingly few steps—back into information that leads right to our doorsteps.[1] Data misuse can lead to significant harm. That harm can be specific, such as when a phone company sells access to location information which is then obtained by a bounty hunter.[2] It can be general, as when data are used to feed an algorithm that perpetuates race discrimination in mortgage lending.[3]

Regulators and lawmakers should therefore ensure there are guardrails on companies that collect, use, and share data to realign their incentives to avoid consumer harms. In these comments, we will seek to highlight some of the most common and most troubling practices people face when it comes to data privacy and corporate surveillance, provide some examples, and suggest some remedies that benefit consumers. Too often, technology, advertising, and other data-obsessed industry advocates have argued for lax privacy regulations, often asking to preserve harmful business models. They have, at best, advocated for empty guardrails that allow them to pay lip service to privacy without changing much about the way they do business. At worst, they have argued that privacy is too complicated to regulate effectively at all. While privacy is a multifaceted problem that demands a variety of creative solutions, the goals of U.S. privacy regulation should not be complicated. They should always be in line with the duty of the Federal Trade Commission itself—to protect America's consumers.

---

[1] Yves Alexandre de Montjoye, César Hidalgo, Michael Verleysen, *et al. Unique in the Crowd: The privacy bounds of human mobility. Sci Rep* 3, 1376 (2013). https://doi.org/10.1038/srep01376

[2] Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, Motherboard (Jan. 2019) https://www.vice.com/en/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile

[3] Robert Bartlett, Adair Morse, Richard Stanton, Nancy Wallace, *Consumer-lending discrimination in the FinTech Era*, Journal of Financial Economics, Volume 143, Issue 1 (2022) https://doi.org/10.1016/j.jfineco.2021.05.047

I. Empowering Consumers Through Regulation

Overbroad Data Collection and Data Minimization

One enormous privacy issue that people face today is comprehending the simply huge amount of information that is extracted from them—often for reasons they don't know about or don't understand. We are heartened to see the FTC recognize the importance of this kind of data collection limit in its enforcement action against Drizly,[4] which will require the company to limit and publicly justify its data collection. We urge the Commission to continue looking for cases where companies are collecting far more information than is necessary for their core businesses and then repurposing it for reasons other than those that justified its collection.

Regulations requiring minimization are also necessary. Minimization is the concept of collecting, retaining, using, and sharing "only what's strictly necessary" for a given use. Minimization should extend not only to what companies may choose to list within their privacy policies, but more fundamentally to what they can justify needing to deliver the product or service that the consumer requested. It is an important pillar of consumer data privacy policy because it drains the data lakes that companies have about us.[5] This helps to lower the risk that information will be used in ways people neither want nor expect. Requiring companies to think about what information they currently need, rather than simply what information they might someday want, is good practice and would also significantly limit the possibility for data misuse and overcollection.

Several companies collect far more information than they need to. For example, EFF wrote and sponsored a bill in California[6] that, as originally introduced, would have imposed strict penalties on companies that offer student proctoring services that gather, retain, use, or share more information than is strictly necessary to provide their services.[7] We championed this bill in response to concerns we heard from students about the software they saw appearing in their schools. Online and remote proctoring companies, such as ProctorU, Proctorio, and Honorlock, frequently collect data for years, including videos of students and their private spaces, biometric data, and detailed private, personally identifying information such as citizenship status. That

---

[4] *FTC Takes Action Against Drizly and its CEO James Cory Rellas for Security Failures that Exposed Data of 2.5 million Consumers*, Federal Trade Commission (Oct. 2022) https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-takes-action-against-drizly-its-ceo-james-cory-rellas-security-failures-exposed-data-25-million

[5] Adam Schwartz, *Sen. Cantwell Leads With New Consumer Data Privacy Bill*, EFF Deeplinks (Dec. 2019) https://www.eff.org/deeplinks/2019/12/sen-cantwell-leads-new-consumer-data-privacy-bill

[6] *Student Test Takers Privacy Protection Act,* S.B. 1172, as introduced (Sess. 2021-2022) https://leginfo.legislature.ca.gov/faces/billVersionsCompareClient.xhtml?bill_id=202120220SB1172&cversion=20210SB117299INT

[7] The contours of this bill were largely in line with the FTC's own May 2022 policy statement regarding education technology companies. *See* https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-crack-down-companies-illegally-surveil-children-learning-online

could be damaging if shared indiscriminately. As the Commission itself has recognized, some education companies also do not properly safeguard data they collect from students.[8]

Many of these tools gain access to parts of a user's machine that make it indistinguishable from spyware, creating massive security vulnerabilities and attack vectors. Proctoring software has also been shown to discriminate against students with certain cognitive and motor disabilities.[9] This overbroad collection is especially egregious because proctoring software is often required for students to take tests remotely—essentially leaving them no choice but to hand over extraneous information to advance their education. We hope the FTC will offer guidance around data minimization, security, and limiting the discriminatory effects of proctoring tools to help protect the millions of students who must use them.

This is just one example of the many ways that unchecked data collection can lead to harm. Others include reproductive health and gender-affirming care. With many states criminalizing these types of health care, law enforcement agencies obtain consumer information such as location data or browsing history as part of an investigation into whether someone has obtained these kinds of procedures.

Some of this information may be protected by medical privacy laws that cover health care providers and practitioners—but a large portion of data that can be used to implicate people seeking this type of care, such as information held by public health authorities or companies that collect relevant information, is not covered by the Health Information Portability and Accountability Act or similar health privacy laws.

Even before the Supreme Court overturned the *Roe v. Wade* decision, prosecutors used digital evidence to build cases against those seeking abortions. Latice Fisher of Mississippi was indicted for second-degree murder after a stillbirth when prosecutors convinced a jury that web searches retained on her phone indicated her intent to end her pregnancy.[10] Those seeking gender-affirming care now face similar threats as states move to outlaw their medical care. To protect the privacy of people seeking healthcare that may be legal in some states but criminalized in others, companies must be required to limit what they collect, and delete what they do not need as quickly as possible. It is better, for companies and for consumers, if they simply do not have it.

Constructing Strong Opt-In Consent

Data minimization is necessary, but it cannot be the only way regulators protect consumers. Consent remains an important tool for people to exercise control over the way their data are

---

[8] *FTC Brings Action Against Ed Tech Provider Chegg for Careless Security that Exposed Personal Data of Millions of Customers,* Federal Trade Commission (Oct. 2022) https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-brings-action-against-ed-tech-provider-chegg-careless-security-exposed-personal-data-millions

[9] Lydia X. Z. Brown, *How Automated Test Proctoring Software Discriminates Against Disabled Students*, CDT (Nov. 2020) https://cdt.org/insights/how-automated-test-proctoring-software-discriminates-against-disabled-students/

[10] Cynthia Conti-Cook, *Surveilling the Digital Abortion Diary*, University of Baltimore Law Review: Vol. 50 : Iss. 1 , Article 2. (2020) https://scholarworks.law.ubalt.edu/ublr/vol50/iss1/2/

collected, retained, shared, and used. It works well in laws such as the Illinois Biometric Information Privacy Act, which requires explicit opt-in consent before companies can "collect, capture, purchase, receive through trade, or otherwise obtain" a person's biometric information.[11]

Data privacy is, in many ways, about individual autonomy—giving individuals control over how their personal information moves throughout the world. That's why consent is so important. There may be cases where individuals may wish to have their data used and collected. If someone understands the risks, for example, of having a company collect and retain their biometric information so they can log in to a device, but decide that risk is outweighed by the convenience they gain, they should be able to make that decision.

Consent should be opt-in rather than opt-out: privacy should be the default. Many people do not know their data is being collected; if they do, they might not know they can opt-out; if they know that, they might not be able to expend the time and effort to opt-out across the many companies that are processing their data. Studies have shown that opt-out mechanisms often are difficult to use.[12] If regulators choose to mandate only opt-out consent (and we hope they mandate opt-in consent), regulators must provide an easy, "one and done" way to opt-out at once from processing by all businesses. For example, businesses must be required to comply with privacy signals on browser headers that say to websites, "do not track me" or "do not sell my data."[13]

We also call on the Commission to find ways to ensure that people are informed not only about how their data is processed by companies they have a relationship with, but also which third-parties have their information. People need maximum transparency about which other parties pick up their data, and where that information goes. That includes not only provisions such as the one present in the California Consumer Privacy Act that requires companies to let people know what *types* of companies have their information.[14] It also requires disclosure of which specific companies received or provided it. People should be able to understand the full extent of how information may be shared before they agree to data use and collection. They should also be able to know which specific companies to contact if they would like file requests to know, correct, or delete their personal information.

---

[11] 740 Ill. Comp. Stat. Ann. 14/15 https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

[12] Kaveh Waddell, *California's New Privacy Rights Are Tough to Use, Consumer Reports Study Finds*, Consumer Reports (Mar. 2021) https://www.consumerreports.org/privacy/californias-new-privacy-rights-are-tough-to-use-a1497188573/.

[13] Bennett Cyphers, *Announcing Global Privacy Control in Privacy Badger*, EFF Deeplinks (Oct. 2020) https://www.eff.org/gpc-privacy-badger; Coalition comments to the Office of the Attorney General of California re: Notice of Proposed Rulemaking of The California Consumer Privacy Act (Dec. 2019) https://www.eff.org/document/2019-12-06-privacy-coalition-comments-re-cag-draft-ccpa-regspdf-0; Bennett Cyphers and Adam Schwartz, *EFF Comments to the California Attorney General Regarding CCPA Rulemaking* (Mar. 2019) https://www.eff.org/files/2019/03/19/2019-03-07_-_eff_ccpa_ag_comments-resolved_0.pdf; EFF, *Do Not Track*, EFF Issue Page (accessed Nov 2022) https://www.eff.org/issues/do-not-track

[14] Cal. Civ. Code 1798.110 https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.110.

Preventing Tactics That Undermine Consent

There are reasonable concerns about "consent fatigue" – the deluge of online boxes we must click before accessing the information and services that we want. But much of this problem is caused by businesses that design these boxes in ways that undermine consent. They are unnecessarily confusing and coercive. The FTC must address these problems in any regulations mandating opt-in consent. If well-designed, consent requests can be easy to use—and decline. For example, when the Apple Store required apps to obtain their users' opt-in consent before tracking them on other companies' apps and websites, the overwhelming majority of users chose not to consent.[15]

As the FTC has recognized itself, companies often collect information from people before they even know it's happening. In its 2014 complaint against the makers of the "Brightest Flashlight App" on Google's Android App Store, the Commission found that people had no meaningful way to avoid location collection.[16]

Much has changed since 2014, but unfortunately many companies still use tactics that obscure or misrepresent the ways data are used, or trick people into allowing data collection that's broader than what they intended. The FTC has recognized the risks posed by these tactics, also known as "dark patterns"[17] or deceptive design, through workshops and its 2022 report on the subject.[18] Dark patterns undermine people's ability to understand and meaningfully consent to data collection and use.[19] Moving forward, we encourage the Commission and policymakers to continue to think carefully about how to ensure that companies do not steer people away from choices that protect their privacy. In previous comments to the California Attorney General's office, EFF expressed its support[20] for dark patterns regulations that:

- Ban consent processes "designed with the purpose or having the substantial effect of subverting or impairing a consumer's choice to opt-out."

---

[15] https://arstechnica.com/gadgets/2021/05/96-of-us-users-opt-out-of-app-tracking-in-ios-14-5-analytics-find/.

[16] *FTC Approves Final Order Settling Charges Against Flashlight App Creator*, Federal Trade Commission (April 2014) https://www.ftc.gov/news-events/news/press-releases/2014/04/ftc-approves-final-order-settling-charges-against-flashlight-app-creator

[17] See also, *Dark Commercial Patterns: OECD Digital Economy Papers* (Oct. 2022) https://www.oecd-ilibrary.org/docserver/44f5e846-en.pdf?expires=1668582641&id=id&accname=guest&checksum=41D9EB18F553A0A8186C0F89BFE39640, which defines dark commercial patterns as, "business practices employing elements of digital choice architecture, in particular in online user interfaces, that subvert or impair consumer autonomy, decision-making or choice. They often deceive, coerce, or manipulate consumers and are likely to cause direct or indirect consumer detriment in various ways, though it may be difficult or impossible to measure such detriment in many instances."

[18] Federal Trade Commission Staff Report, *Bringing Dark Patterns to Light* (Sept. 2022) https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf

[19] https://www.eff.org/deeplinks/2021/05/help-bring-dark-patterns-light; https://www.eff.org/deeplinks/2021/04/deceptive-checkboxes-should-not-open-our-checkbooks; https://www.eff.org/deeplinks/2019/02/designing-welcome-mats-invite-user-privacy-0.

[20] Adam Schwartz, *EFF comments on proposed Cal DOJ regulations on "dark patterns"* (Oct. 2020) https://www.eff.org/document/eff-comments-re-cal-doj-regs-dark-patterns

- Require consent processes to be "easy" and "require minimal steps."
- Limit the number of steps to opt-out to the number of steps to later opt back in.
- Ban "confusing language" such as "double negatives" (such as "don't not sell").
- Ban the necessity to search or scroll through a document to withhold consent.

We hope the Commission will consider using similar guidelines in its continued work to stop dark patterns.

Just as important as banning dark patterns, there should also be a ban on any pay-for-privacy provisions, which the Commission has rightly identified as a type of retaliation against consumers. Such schemes pressure all people—and particularly those with lower incomes—into giving up their privacy in unfair ways.[21]

One of these schemes is to offer a discount on a good or service in exchange for letting the company collect a person's information. There are, undoubtedly, some consumers for whom $5 or $10 per month would go a long way to make ends meet and who might be succumb to economic pressure to trade their privacy rights for such a discount. But, as such plans would likely be most appealing to those who have few other choices, they are exploitative.

EFF has also seen this concept emerge in legislation.[22] Oregon in 2019 considered a bill, sponsored by a company called Humanity.co, to directly pay people for the "value" of their health data as calculated by companies.[23] The bill would have paved the way for for-profit companies to purchase private medical information—some of the most sensitive data—and encourage people to give up highly personal information for a little bit of compensation.

Privacy is a right and should not be considered a luxury good. Both pay-for-privacy schemes and dark pattern tactics undermine a person's ability to give consent freely. They should be expressly forbidden in any meaningful consent provision or guidelines that the FTC may consider creating.

Dismantling Online Behavioral Advertising

Government must ban online behavioral advertising.[24] This dangerous practice relies on a broad array of corporations closely surveilling everything we do online and building that disparate information into dossiers about our preferences and interests. As explained below, EFF has

---

[21] Hayley Tsukayama, *Why Getting Paid for Your Data is a Bad Deal*, EFF Deeplinks (Jul. 2019) https://www.eff.org/deeplinks/2020/10/why-getting-paid-your-data-bad-deal; Adam Schwartz, *The Payoff of California's Data Dividend Must Be Stronger Privacy Laws*, EFF Deeplinks (Feb. 2019) https://www.eff.org/deeplinks/2019/02/payoff-californias-data-dividend-must-be-stronger-privacy-laws.

[22] Hayley Tsukayama, *Knowing the "Value" of Our Data Won't Fix Our Privacy Problems*, EFF Deeplinks (Jul. 2019) https://www.eff.org/deeplinks/2019/07/knowing-value-our-data-wont-fix-our-privacy-problems

[23] Sarah Jeong, *Selling Your Private Information Is a Terrible Idea,* The New York Times (Jul. 2019) https://www.nytimes.com/2019/07/05/opinion/health-data-property-privacy.html. EFF joined the Oregon affiliate of the American Civil Liberties Union to oppose, and eventually stop, that bill.

[24] Bennett Cyphers and Adam Schwartz, *Ban Online Behavioral Advertising*, EFF Deeplinks (Mar. 2022) https://www.eff.org/deeplinks/2022/03/ban-online-behavioral-advertising

developed a framework for legislators and regulators to use to ban online behavioral advertising. It carefully balances the privacy and free expression interests.

The targeting of ads to us based on our online behavior is a three-part cycle:

- **Track**: A person uses technology, and that technology quietly collects information about who they are and what they do. Most critically, trackers gather online behavioral information, like app interactions and browsing history. This information is shared with ad tech companies and data brokers.
- **Profile**: Ad tech companies and data brokers that receive this information try to link it to what they already know about the user in question. These observers draw inferences about their target: what they like, what kind of person they are (including demographics like age and gender), and what they might be interested in buying, attending, or voting for.
- **Target**: Ad tech companies use the profiles they've assembled, or obtained from data brokers, to target advertisements. Through websites, apps, TVs, and social media, advertisers use data to show tailored messages to particular people, types of people, or groups.

This business has proven extremely lucrative for the companies that participate in it: Facebook, Google, and a host of smaller competitors turn data and screen real estate into advertiser dollars at staggering scale.

Behavioral data is the raw fuel that powers targeting, but it isn't just used for ads. Data gathered for ad tech can be shared with or sold to hedge funds,[25] law enforcement agencies,[26] and military intelligence.[27] Even when sensitive information doesn't leave a company's walls, that information can be accessed and exploited by people inside the company for personal ends.[28] Moreover, online behavioral advertising has warped the development of technology so that our devices spy on us by default. For example, mobile phones come equipped with "advertising IDs," which were created for the sole purpose of enabling third-party trackers to profile users based on how they use their phones.[29]

---

[25] Joseph Cox, Leaked Document Shows How Big Companies Buy Credit Card Data on Millions of Americans, Motherboard (Feb. 2020) https://www.vice.com/en/article/jged4x/envestnet-yodlee-credit-card-bank-data-not-anonymous

[26] Lee Fang, *FBI Expands Ability to Collect Cellphone Location Data, Monitor Social Media*, *Recent Contracts Show*, The Intercept (Jun. 2020) https://theintercept.com/2020/06/24/fbi-surveillance-social-media-cellphone-dataminr-venntel/

[27] Charlie Savage, *Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says*, The New York Times (Jan. 2021) https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html

[28] Jenna Romaine, *New report says Facebook fired 52 employees caught spying on users' inboxes*, The Hill (Jul. 2021) https://thehill.com/changing-america/resilience/smart-cities/562988-new-report-says-facebook-fired-52-employees-caught/

[29] Bennett Cyphers and Gennie Gebhart, *Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance*, EFF White Paper (Dec. 2019) https://www.eff.org/wp/behind-the-one-way-mirror#Identifiersonmobile

Targeted advertising based on online behavior doesn't just hurt privacy. It also contributes to a range of other harms. Such targeting supercharges the efforts of fraudulent, exploitive, and misleading advertisers. It allows peddlers of shady products and services to reach exactly the people who, based on their online behavior, the peddlers believe are most likely to be vulnerable to their messaging. Too often, what's good for an advertiser is actively harmful for their targets.

So, we must ban the targeting of ads to people based on their online behavior. Such a ban must be narrowly tailored to protect privacy and equity without placing unnecessary burdens on speech and innovation.

To do so, we recommend focusing on the personal data most central to targeted ads: our online behavior. This includes the web searches we conduct, the web pages we visit, the mobile apps we use, the digital content we view or create, and the hour we go online. It also includes the ways our online devices document our offline lives, such as our phones using GPS to track our geolocation or fitness trackers monitoring our health.

We should ban any entity that delivers online ads from doing so by targeting users based on their online behavior. This ban would apply to dominant ad tech players like Facebook and Google, among many others. By "ad," we mean paid content that concerns the economic interests of the speaker and audience. This ban should apply whether or not an ad is targeted to a traditional personal identifier, like a name or email address.

We must also address the role of data brokers in ad tech. This sector profiles users based on their online behavior and creates lists of users to whom various ads might be delivered. But many data brokers do not subsequently deliver any ads. Rather, they sell these lists to advertisers, or directly to online ad deliverers.

Thus, we should ban an ad deliverer from using a list created by another entity, if the deliverer knows it is based on users' online behavior, or would have known but for reckless disregard of known facts. Likewise, a data broker must be banned from disclosing a list of users that is based on online behavior, if the data broker knows it will be used to deliver ads, or would have known but for reckless disregard of known facts.

We suggest two limited exceptions from these bans, both involving what a user is doing *right now*, and not over time. First, the ban should exempt "contextual ads" based on content a user is currently interacting with. For example, while a user visits an online nature magazine, they might be shown an ad about hiking boots. Second, the ban should exempt ad delivery based on a user's rough, real-time location. For example, while a user visits a particular city, they might be sent an ad for a restaurant in that city.

Empowering Consumers to Block Cookies and Persistent Identifiers

Enabling consumers to block third-party cookies and other persistent identifiers generally enhances competition. Thus, the Commission should not interfere with this practice when it allows consumers to take control of their privacy.

Apple's "App Tracking Transparency" initiative, begun in 2021, is an example of competition-enhancing privacy controls: users can enable or disable access to their persistent advertising ID for each app. That way, a user can grant access to their persistent ID to an app with a superior value proposition, including better practices concerning consumer data, while blocking access to a less protective app or one that provides a less valuable service.[30]

Blocking persistent identifiers at the operating system or browser level is valuable to consumers, and promotes competition, but only when it gives consumers meaningful choices. Google's Federated Learning of Cohorts (FLoC) proposal, and other technologies in Google's "Privacy Sandbox," purport to achieve the same goals as Apple's App Tracking Transparency. But Google's proposals, although they block the most common forms of third-party tracking through cookies and other persistent identifiers, also enable Google to conduct more sophisticated forms of tracking and behavioral modeling of consumers. Indeed, it might reveal even more sensitive data about consumers to advertisers.[31]

If new trade regulation rules address this issue, they should incentivize companies to compete to serve consumers better by providing more control over the use of browsing history and other personal data. New rules should not, in the name of promoting competition, invite a race to exploit consumer data. But it's equally important that any new rules not reward companies for stopping common forms of third-party tracking while moving to new forms of commercial surveillance without giving consumers the same level of opt-in control.

Companies Should Not Use "Trade Secrets" To Escape Accountability

We encourage the Commission to reject proposals allowing businesses to hold back information by claiming trade secrets, proprietary information, or non-disclosure agreements—or in some cases, at a minimum with auditors and regulators. This is particularly true in an automated decision-making context.

Regulation should improve understanding for the people directly affected by the automated decisions. But it's not enough to think only about the individual consumer—there is a collective, societal interest in understanding how companies are making important decisions about people, and in ensuring fairness in those decisions. The well-documented discrimination grows in algorithmic darkness.

Companies should not be allowed to escape scrutiny by claiming the commercial need to protect their intellectual property or other company information. Europe's General Data Protection Regulation (GDPR) says that in cases of automated decision-making, the data subject has the

[30] Gennie Gebhart and Bennett Cyphers, "Apple's App Tracking Transparency is Upending Mobile Phone Tracking," EFF Deeplinks (Apr. 2021), https://www.eff.org/deeplinks/2021/04/apples-apptrackingtransparency-upending-mobile-phone-tracking.

[31] Bennett Cyphers, "Google's FLoC is a Terrible Idea," EFF Deeplinks (Mar. 2021), https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea

right to access "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."[32] This is a good start.

A right to an explanation—both why an entity is collecting information, and how the system reached a final decision—is crucial to protecting consumers. This must not be sacrificed by a trade secrets claim. It is critical to be able to evaluate the reasoning behind such decisions, to ensure there is no incorrect information and that automated decision-making systems are not simply repeating (or even amplifying) historic biases from the systems they seek to replace.

II. Specific Areas of Focus

We have outlined priorities the Commission should address generally to empower consumers and curb commercial surveillance harms. There are also several specific issues and industries that we urge the Commission to address more closely. Several of the situations involve what we call "disciplinary technologies,"[33] in which subjects and victims often do not know they are being surveilled, or are coerced into it by bosses, administrators, partners, or others with power over them.

Worker Privacy

People are often subjected to data processing in situations where they have even less leverage than even an average consumer holds with a company. For example, employees—which the FTC has made clear are included in the definition of consumer for these proceedings—often must submit to data collection as part of their work life.

Even when an employer requests consent from an employee before processing their data, the consent frameworks can break down in such situations. Saying "no" to data collection in a consumer context may mean you have to use another company's service. Saying "no" to your employer could get you fired, or otherwise seriously affect your livelihood. In such situations, more thought must be given to how to balance consent with other methods that can protect workers from harmful data collection and use.

Over the past few years, more lawmakers have considered workers in consumer privacy bills, and the pandemic caused a great increase in the use of workplace surveillance software. In warehouses, for example, employers have used software to track how much time workers are spending "off-task" to push them to meet high quotas—which are often physically damaging. In office settings, employers have forced workers to install invasive monitoring software—a form of spyware often called "bossware"—to track their keystrokes, mouse movements, and other activity during the workday.[34]

---

[32] *Art. 22 GDPR – automated individual decision-making, including profiling*. General Data Protection Regulation (GDPR). (2018) https://gdpr-info.eu/art-22-gdpr/.

[33] Gennie Gebhart, Eva Galperin, Kurt Opsahl, *Fighting Disciplinary Technologies*, EFF Deeplinks (May 2021) https://www.eff.org/deeplinks/2021/05/fighting-disciplinary-technologies

[34] Drew Harwell, *Contract lawyers face a growing invasion of surveillance programs that monitor their work*, The Washington Post (Nov. 2021) https://www.washingtonpost.com/technology/2021/11/11/lawyer-facial-

The authors of some consumer privacy bills have wrestled with how to address privacy issues in an employee-employer situation—or, indeed, whether they should be considered in the same bills at all. EFF's position is simple: all workers deserve legally enforceable privacy rights. We generally agree with the principles set out in the 2021 report of the University of California's Labor Center, "*Data and Algorithms at Work: The Case for Worker Technology Rights.*"[35]

Many of these worker-focused principles are similar to those found in most consumer data privacy bills but give special attention to the unique power imbalance of an employee-employer relationship. For example, worker data should only be collected when it is necessary and closely related to the tasks of an employee's job. It should be used only for the purposes for which it was collected. Information collected for worker wellness programs, for example, should not end up in the hands of third parties to draw inferences about an individual's health. Similarly, workers should be given clear notice about how and why data are being collected, especially if it will be used in a way that could materially affect their working conditions, such as for performance evaluation or discipline.

Some consumer rights might not map as well onto an employer-employee situation. Rights to delete data, for example, must be carefully crafted to harmonize with requirements for employers to retain data for other purposes, such as for diversity reporting.

This area will continue to evolve, particularly as more companies form policies around remote and hybrid work. Worker privacy issues cross many jurisdictional boundaries; for example, the general counsel of the National Labor Relations Board recently published a memo describing the danger that workplace surveillance poses to organizing activity.[36] We support the comments of many in the labor advocacy community who urge the Commission to seek out the stories of workers who have first-hand experience with digital tracking, bossware, and other types of workplace surveillance.

Student Privacy

As with worker privacy, there are also several special considerations the FTC should pay attention to regarding companies that collect the private information of young people, especially those companies that operate in the "education technology" (EdTech) space. Often, no feasible alternative exists for students who would prefer to opt out of such data collection, and as previously mentioned, this data collection goes far beyond what is required for the software to function. There is often less recourse under the law for students who feel that these tools are invading their privacy, because education technology companies generally claim they are

---

recognition-monitoring/; https://www.eff.org/deeplinks/2020/06/inside-invasive-secretive-bossware-tracking-workers.

[35] Annette Bernhardt, Reem Suleiman, and Lisa Kresge, *Data and Algorithms at Work: The Case for Worker Technology Rights*, University of California Berkeley Labor Center (Nov. 2021) https://laborcenter.berkeley.edu/data-algorithms-at-work/

[36] Jennifer A. Abruzzo, *Electronic Monitoring and Algorithmic Management of Employees Interfering with the Exercise of Section 7 Rights*, General Counsel Memo, National Labor Relations Board (Oct. 2022) https://www.nlrb.gov/guidance/memos-research/general-counsel-memos

"school officials" with "legitimate educational interests" in students' "education records" under FERPA.[37]

This loophole has been a longstanding problem in EdTech. Google has exploited it [38] in its Google Apps for Education (GAFE) program in an attempt to get around written parental consent requirements for data collection. Online proctoring software companies, which have been[39] roundly[40] criticized [41] for their privacy practices, also use this exception. In the modern school system, where software is an essential element of education, this loophole renders FERPA's protections moot for a vast majority of students interacting with technology companies.

This is especially true when a software's sole functionality is to collect student data. Student activity monitoring software such as Bark, Gaggle, GoGuardian, and Securly, exist entirely to monitor and retain information about private student communications, web searches, and documents, and are a serious threat to student privacy. These tools give schools and these software companies access to an enormous amount of sensitive student data.[32]

A 14-page Congressional report investigating student activity monitoring software identified critical issues with the software. For example, it disproportionately flags minority groups—particularly students of color—for disciplinary action. This report also found that the surveillance software inadequately informed students and parents of the monitoring—surreptitiously gathering data on students without informed consent. The report called on federal regulators to assess "regulatory and legal gaps [that] exacerbate the risks of student activity monitoring software." It also called on regulators to determine whether these products pose risks to students' civil rights, and to address these problems when they are found.[42]

When student activity monitoring software is in use, students have essentially no privacy in their digital activity. Internet searches, communications, videos, and more are all scanned by the software against a broad and vague list of categories of supposedly objectionable content. Over the course of months and years, there is little about a student's life that will not be reflected in

---

[37] Center for Digital Democracy et al, *Comments filed in response to the Federal Trade Commission's review of COPPA* (Dec. 2019) https://www.democraticmedia.org/sites/default/files/field/public-files/2019/cdd_-ccfc-coppa-comments.pdf

[38] Jeremy Gillula and Sophia Cope, *Google Changes Its Tune When it Comes to Tracking Students*, EFF Deeplinks (Oct. 2016) https://www.eff.org/deeplinks/2016/10/google-changes-its-tune-when-it-comes-tracking-students

[39] Jason Kelley and Lindsay Oliver, *Senators Express Privacy Concerns Over Proctoring Apps*, EFF Deeplinks (Dec. 2020) https://www.eff.org/deeplinks/2020/12/senators-express-privacy-concerns-over-proctoring-apps

[40] Thomas Germain, *Poor Security at Online Proctoring Company May Have Put Student Data at Risk*, Consumer Reports (Dec. 2020) https://www.consumerreports.org/digital-security/poor-security-at-online-proctoring-company-proctortrack-may-have-put-student-data-at-risk-a8711230545/

[41] Jeffrey R. Young, *Pushback Is Growing Against Automated Proctoring Services. But So Is Their Use*, EdSurge (Nov 2020) https://www.edsurge.com/news/2020-11-13-pushback-is-growing-against-automated-proctoring-services-but-so-is-their-use

[42] *Warren, Markey Investigation Finds That EdTech Student Surveillance Platforms Need Urgent Federal Action to Protect Students* (Mar. 2022) https://www.warren.senate.gov/oversight/reports/warren-markey-investigation-finds-that-edtech-student-surveillance-platforms-need-urgent-federal-action-to-protect-students

their computer use. The result is a detailed record of students' private thoughts, accessible to school employees, the companies that make these tools, police, and other third parties.

The content filtering and flagging in these tools is ineffective. Our research and that of others demonstrates this software is generally incapable of distinguishing between the mundane and the actually dangerous. Students are frequently flagged for searching for inoffensive, but potentially sensitive health related information. For example, a search for "healthy foods to eat for irritable bowel syndrome" is flagged because responsive pages contain the word "colon." Students also are flagged for looking up information about politics because of responsive content related to guns or drug laws. And they are flagged for seeking information related to sexual health or gender, which has led to the nonconsensual disclosure of students' sexual orientation and gender identity. This is especially harmful in states with abortion bans and anti-trans healthcare laws.

In addition to flagging content, these tools block huge swathes of educational information that students may only be able to access from their school-issued devices, such as coding resources and news sites. Companies making this software determine what online information students can access. They also have the capacity to forward students' most sensitive thoughts, conversations, and interests to police or other government agencies, sometimes bypassing parents altogether. At minimum, such companies should have strict guidelines for who that data can be shared with and how long it is retained. Even better, there must be limits on what data they can collect and retain. Also, the accuracy of these apps should be regularly reviewed to remove bias, and guidance should be offered regarding problems with their effectiveness. And the software must function only during school hours and on school grounds.

The Commission must also address the privacy threats to young people online. Some flawed approaches involve further surveilling all users, or young people, with the goal of restricting *access to information* rather than restricting *data collection*. But surveillance of young people is not a good way to help young people navigate the internet. Users should have more control over the content they see online. Proposals to require platforms to create parental tools that track and log all content viewed by young people, for example, would often give far broader ability for parents to monitor and control a young person's online use than is healthy, especially when those rules do not sufficiently distinguish between a child who is five versus one who is fifteen. Instead, young people should be given broader options to control their experiences online, whether that's through filtering content, or through more responsive abilities to block or report abusive users.

Finally, the FTC must stop companies from using dark patterns to trick young users into giving up their personal information. This is clearly part of the FTC's mission to curb deceptive practices. Instead of hiding the ball, companies should be fully transparent about the types of data collected about young users and how data collection might impact them.

Daycare and Early Education Apps

Separately, EFF has found that daycare and early education apps are dangerously insecure when it comes to the privacy of young children's data.[43]

These apps collect vast quantities of very specific details about young children and infants: allergies, medications, bathroom times, age, address, eating habits, lesson plans, and nap times. Perhaps the largest category of data generated daily is photos of children and their classmates, shared with parents to allow them a window into their children's social development and behavior. If this data were breached or given to a third party, each day would form a very accurate profile on a child's development.

Great care should be taken with this highly sensitive data. Currently, however, there are insufficient safeguards to secure the data from theft or misuse, and to empower parents to control how the app companies retain, use, and share the data It is likely only a matter of time before these companies leak data or become subject of a breach. A single compromise of the application servers could affect hundreds of daycares and preschools. Proper controls should be built into the application infrastructure by the companies who create these apps to help prevent these types of attacks.

In an open letter sent to Chair Khan in September, EFF detailed several troubling findings regarding these daycare apps, and urged the Commission to review the lack of privacy and security protections.[44]

Lackluster security was rampant.[45] Common practices included public access to children's photos, weak password policies, and inadequate or even absent encryption. Another study found that privacy policies sometimes failed to identify the data the apps were collecting, or falsely claimed to not share data with third parties.[46]

Parents are left in a bind: either enroll their children into daycares which use apps that put their children's data at risk, or look for another childcare arrangement, which is difficult for many families. Parents must wade through obtuse privacy policies that often omit important facts on the data they collect, just to make themselves aware of the dangers. Even for parents who do this, there is often no opt-out mechanism, and thus no meaningful recourse.

These problems with these apps – privacy policy defects and lackluster security practices –fall squarely under the "unfair or deceptive acts or practices" clause built into the Federal Trade

---

[43] *EFF Urges FTC to Address Security and Privacy Problems in Daycare and Early Education Apps*, EFF Press Release (Sep. 2022) https://www.eff.org/press/releases/eff-urges-ftc-address-security-and-privacy-problems-daycare-and-early-education-apps

[44] *See* Appendix A. Also available at: https://www.eff.org/document/eff-letter-ftc-daycare-apps-9-28-2022.

[45] Alexis Hancock, *Daycare Apps Are Dangerously Insecure*, EFF Deeplinks (Jun. 2022) https://www.eff.org/deeplinks/2022/06/daycare-apps-are-dangerously-insecure

[46] Moritz Gruber, Christian Höfig, Maximilian Golla, Tobias Urban, and Matteo Große-Kampmann, *"We may share the number of diaper changes": A Privacy and Security Analysis of Mobile Child Care Applications* (Mar. 2022) https://www.researchgate.net/publication/358904572

Commission Act. It is deceptive to mislead parents and daycares into thinking these apps collect less information than they do. It is unfair practice to expose young children to the risk of their data being misused or breached.

Stalkerware

EFF also renews its call for an investigation of app makers that create "stalkerware," that is, consumer-grade spyware that enables anyone to track and monitor people without their consent. EFF has previously called on the Commission to investigate 1Byte and its network of stalkerware apps[47] to protect the potential targets of stalkers and domestic abusers. As TechCrunch's Zack Whittaker has reported, these apps not only collect an enormous amount of information, but they are also highly insecure.[48]

Stalkerware is, in and of itself, a dangerous tool for tech-enabled abuse. Insecure stalkerware is doubly dangerous, because it leaves victims vulnerable to an entirely new range of abusers.

The FTC has previously cracked down on app makers that produce similar software, and we urge the Commission to act again against these companies with robust rulemaking.

Location Data Brokers

We applaud the FTC's recent enforcement action against Kochava, which lays out a powerful case that the company's brokering of location data is unfair and thus unlawful.[49] We hope other location data brokers will take a hard look at their own business model or risk similar judicial consequences. We also hope the FTC will now issue rules to protect the public from this dangerous industry.

Many companies have taken the location tracking tactics invented by the advertising industry and repurposed them for law enforcement—a truly troubling development.[50] Sometimes this relationship takes the form of a company contracting with a government entity to share a feed of location data.[51] Other times, agencies simply pay for data. The Commission should address all data brokers that sell location data on the open market. As explained in comments from the Brennan Center for Justice at the New York School of Law, the Commission should give special attention to brokers that share data with government entities.

---

[47] Zack Whittaker, *Behind the stalkerware network spilling the private phone data of hundreds of thousands* (Feb 2022) https://techcrunch.com/2022/02/22/stalkerware-network-spilling-data/

[48] *Ibid*.

[49] *FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations*, Federal Trade Commission (Aug. 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; https://www.eff.org/deeplinks/2022/09/ftc-sues-location-data-broker.

[50] Will Greenberg, *How Ad Tech Became Cop Spy Tech* (Aug. 2022) https://www.eff.org/deeplinks/2022/08/how-ad-tech-became-cop-spy-tech

[51] Jamie Williams, *Unchecked Smart Cities are Surveillance Cities. What We Need are Smart Enough Cities*, EFF Deeplinks (Mar. 2018) https://www.eff.org/deeplinks/2020/03/unchecked-smart-cities-are-surveillance-cities-what-we-need-are-smart-enough

EFF has recently published an in-depth look into another location data broker, Fog Data Science.[52] This investigation was based on public records requests sent to dozens of state and local law enforcement agencies. Fog Data Science provides law enforcement with easy and often warrantless access to the precise and continuous geolocation of hundreds of millions of unsuspecting Americans, collected through their smartphone apps and then aggregated by shadowy data brokers. According to documents created by the company, Fog purchases "billions of data points" derived from some "250 million devices" around the United States. Then, for a subscription fee that many law enforcement agencies are happy to pay, Fog provides access to a massive, searchable database of where people are located. This is mass surveillance, often with no judicial oversight, and flies in the face of Fourth Amendment protections against unreasonable search and seizure.

Rep. Anna Eshoo in September sent a strong letter to the Commission asking for an investigation into Fog, specifically on the ways it allows law enforcement agencies to circumvent the Fourth Amendment.[53] EFF also urges the Commission to launch such an investigation.

Privacy and Competition

We have outlined examples of how the Commission may address issues through its jurisdiction over privacy and consumer protection. We also have recommendations relating to the Commission's authority to protect the competitive process, and how this relates to privacy.

Many recent proposed and completed mergers and acquisitions have troubling implications for consumer privacy, because they are likely to result in consumers' data being used for new and unanticipated purposes. For example, purchasers of fitness tracking devices may consent to the collection of data from the device. But if the service underlying a fitness tracker is acquired by a larger conglomerate, that data may be used to market other products as part of a comprehensive profile of the consumer. Data-heavy mergers and acquisitions make it effectively impossible for consumers to anticipate how their data may be used in the future. The Commission should ensure that new rules on commercial surveillance continue to apply to consumer data following a merger, bankruptcy, or buyout. The Commission should also use its competition authority to challenge proposed mergers and acquisitions that would have the effect of diminishing consumers' control over their personal data—a species of harm to competition that can be compared to higher prices.[54]

Any new trade regulation rule on data security or commercial surveillance should consider the size of the businesses that will be bound. Although consumers need protection against

[52] Matthew Guariglia, *What is Fog Data Science? Why is the Surveillance Company so Dangerous?*, EFF Deeplinks (Aug. 2022) https://www.eff.org/deeplinks/2022/06/what-fog-data-science-why-surveillance-company-so-dangerous; https://apnews.com/article/technology-police-government-surveillance-d395409ef5a8c6c3f6cdab5b1d0e27ef.

[53] Matthew Guariglia, *Members of Congress Urge FTC to Investigate Fog Data Science*, EFF Deeplinks (Sept. 2022) https://www.eff.org/deeplinks/2022/09/members-congress-urge-ftc-investigate-fog-data-science

[54] *See* Dina Srinivasan, *The Antitrust Case Against Facebook*, 16:1 Berkeley Bus. Law J. 39 (2018) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3247362).

commercial surveillance by both large and small firms, new rules should not impose disproportionate compliance burdens on smaller competitors.

Conclusion

There must be many tools in the toolbox to protect consumers. But there are many places in which American's data privacy is not adequately protected by any current privacy law. The Commission must issue new rules to place new limits on companies that violate our trust and strengthen the general privacy landscape. As the federal government's privacy enforcer, the FTC must be the vanguard for privacy protections. We thank you for the opportunity to provide comment.

Respectfully submitted,
s/ Hayley Tsukayama
Senior Legislative Activist

on behalf of

Electronic Frontier Foundation
815 Eddy Street
San Francisco CA 94104
hayleyt@eff.org

Appendix A

September 28, 2022
The Honorable Lina Khan
Chair
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Daycare App Security & Privacy Practices

Dear Chair Khan,

The Electronic Frontier Foundation (EFF) urges the Federal Trade Commission to review the lack of privacy and security protections among daycare and early education apps. A recent investigation[55] conducted by EFF substantiated research[56] presented in March at the Privacy Enhancing Technologies (PET) Symposium, finding daycare apps dangerously negligent when it comes to the privacy and security of young children's data.

EFF found that early education and daycare apps have several troubling security risks: some allow public access to children's photos via insecure cloud storage; many have dangerously weak password policies; at least one application (Tadpoles for Parents) sends "event" data including when the app is activated and deactivated to Facebook; and several applications enable cleartext traffic that can be exploited by network eavesdroppers.[57] Of 42 daycare apps researched, 13 companies did not specify the data they collect in their privacy policies. In policies of those that do describe data collection processes, the apps admitted to sharing sensitive information (such as the average number of diaper changes per day) with third parties. Only 10 of the 42 apps stated in their privacy policy that they did not share data with third parties. But 7 of those 10 were sharing data with third parties anyway, contrary to their policy.[58]

Due to current gaps in the law, children are not protected from having their data collected via daycare apps. The Children's Online Privacy Protection Act (COPPA) only applies to operators of online services "directed to" children under 13.[59] Early education and daycare apps, however,

---

[55] Alexis Hancock, *Daycare Apps Are Dangerously Insecure*, EFF (Jun. 2022) https://www.eff.org/deeplinks/2022/06/daycare-apps-are-dangerously-insecure

[56] Moritz Gruber, Christian Höfig, Maximilian Golla, Tobias Urban, and Matteo Große-Kampmann, *"We may share the number of diaper changes": A Privacy and Security Analysis of Mobile Child Care Applications* (Mar. 2022) https://www.researchgate.net/publication/358904572

[57] Hancock, *Daycare Apps.*

[58] Gruber et al., *"We may share"*

[59] See 16 C.F.R. § 312.2 (definition of "Web site or online service directed to children," paragraph (1) and (2)).

are used solely by adults like teachers. COPPA can protect children from websites or apps that target and appeal to them, but it does not protect children's information that adults enter into apps.

The Family Educational Rights and Privacy Act (FERPA) also falls short. FERPA protects the privacy of student "education records" by restricting schools from disclosing them to certain third parties without parental consent. Though FERPA regulates schools' responsibilities when handling and disclosing certain student data, it does not regulate the actions of third parties who may receive that data, such as daycare apps. At most, FERPA only applies to certain childcare programs[60] and preschools[61] that receive funds under an applicable program of the U.S. Department of Education.[62] This leaves out private daycares, and it also does not solve the larger security risks present in daycare apps.

Parents who wish to enroll their children in daycare often have little ability to delete the sensitive data collected by these apps. Researchers have found that email correspondence is slow and unreliable for removing data, and the majority of apps studied did not provide any information at all on subject access requests. Parents find themselves in a bind: either enroll children at a daycare and be forced to share sensitive information with these apps, or don't enroll them at all. Paths for parents to opt a child out of data sharing are, with rare exception, completely absent. Since parents do not have the tools or proper information to currently assess the privacy and security of their children's data in daycare and early education apps, the Federal Trade Commission should review the current gaps in the law and assess potential paths to strengthen protections for young children's data, or investigate other means to improve protections for children's data in this context.

Best Regards,
Electronic Frontier Foundation

[60] U.S. DEPARTMENT OF EDUCATION, *Childcare Access Means Parents in School Program* (Last modified May 20, 2022), https://www2.ed.gov/programs/campisp/index.html.

[61] U.S. DEPARTMENT OF EDUCATION, *Preschool Development Grants* (Last modified Jan 21, 2020), https://www2.ed.gov/programs/preschooldevelopmentgrants/index.html.

[62] See *34 C.F.R.* § *99.1(a).*