Privacy First:

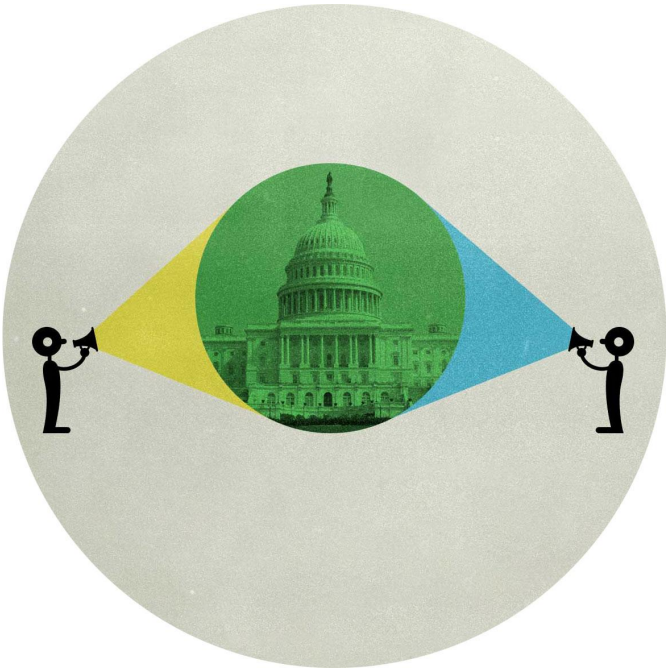
A BETTER WAY TO ADDRESS ONLINE HARMS

ELECTRONIC FRONTIER FOUNDATION

Authors: Corynne McSherry, Mario Trujillo, Cindy Cohn, Thorin Klosowski

A publication of the Electronic Frontier Foundation, 2023.

View this report online:
https://www.eff.org/wp/privacy-first-better-way-address-online-harms



Privacy First:

A BETTER WAY TO ADDRESS ONLINE HARMS

Corynne McSherry, Legal Director
Mario Trujillo, Staff Attorney
Cindy Cohn, Executive Director
Thorin Klosowski, Security and Privacy Activist

November 2023

Table of Contents

Executive Summary

State, federal, and international regulators are increasingly concerned about the harms they believe the internet and new technology is causing. The list is long, implicating child safety, journalism, access to healthcare data, digital justice, competition, artificial intelligence, and government surveillance, just to name a few. And the stories behind them are important: no one wants to live in a world where children are preyed upon, we lose access to news, or we face turbocharged discrimination or monopoly power. This concern about the impact of technology on our values is also not new—both serious concerns and outsized moral panics have accompanied many technological developments. The printing press, the automobile, the victrola, the television, and the VCR all prompted calls for new laws and regulations.

Trouble is, our lawmakers seem to be losing the forest for the trees, promoting scattered and disconnected proposals addressing whichever perceived harm is causing the loudest public anxiety in any given moment. Too often, those proposals do not carefully consider the likely unintended consequences nor even whether the law will actually reduce the harms it's supposed to target.

For example, legislators at the state and federal level are trying to require private companies to ensure that people (or just children) never see things that those lawmakers don't want them to see online. Yet the legislation almost always runs afoul of the Constitution and human rights standards. It leaves the decisions about what constitutes a "harm" to elected officials, who can vary wildly in their views. It's also unworkable in practice and likely to harm the very people we want to protect.

It's long past time to look for global solutions that can accomplish something concrete and ambitious. Happily, you don't have to look far.

The truth is many of the ills of today's internet have a single thing in common: they are built on a system of corporate surveillance. Multiple companies, large and small, collect data about where we go, what we do, what we read, who we communicate with, and so on. They use this data in multiple ways and, if it suits their business model, may sell it to anyone who wants it—including law enforcement. Addressing this shared reality will better promote human rights and civil liberties, while simultaneously holding space for free expression, creativity, and innovation than many of the issue-specific bills we've seen over the past decade.

In other words, whatever online harms you want to alleviate, you can do it better, with a broader impact, if you do privacy first.

Some examples:

- Worried about how social media algorithms are affecting children's mental health? The current accumulation of personal data—and the advertising industry that it fuels—is the starting point of a lot of online harm to children, including

the loss of personal privacy; predatory and exploitative ads that target children most vulnerable to their messaging; and discrimination resulting from consumer profiles based on a child's gender, age, race, and the like. If you ban online behavioral advertising, you remove most of the incentive to collect and weaponize children's preferences to get them to buy more things, and along with it many of the concerns about social media use by kids. It's a strategy that focuses on the key reasons underlying these harms, rather than trying to stick a band-aid over the top. And privacy law protects all of us, children included.

- Worried about how law enforcement might use apps we rely on to prosecute patients or health-care providers, whether in reproductive care, trans care or otherwise? Pass legislation preventing the collection, use, disclosure, and retention of data beyond what is strictly necessary to give the user what they asked for. The less that is collected, the less that can be used against us.

- Worried that Big Tech is undermining local journalism? Privacy protection can help level the playing field. If you protect privacy by banning surveillance-driven "behavioral advertising" (or even make it truly opt-in, as Apple recently did) you take away much of the edge that the giants now enjoy. Requiring everyone to limit their tracking takes away much of the edge that the giants now enjoy. "Contextual ads" can limit that claimed competitive advantage and protect users from tracking. True contextual ad markets are harder for tech giants to capture. While a tech company may know everything about a reader's web history and recent purchases, no one knows more about a publication's articles than its direct publisher.

- Worried about the general lack of competition in social media? A privacy-first approach, which limits how much data can be collected and, you guessed it, bans behavioral ads, would level the playing field for new entrants. Allow users to take their data and connections elsewhere, protecting privacy along the way, and we could see a range of choices and options emerge. The data surveillance business model has cemented power in the companies that moved fastest to collect the most personal information to create the most detailed user profiles. It's time to make that business model less appealing.

- Worried that foreign adversaries are spying on Americans through specific apps like TikTok or purchasing American data from data brokers? Minimize how much information all tech companies can collect and thereby limit the information that can be sold or given away. Put users in control of who retains their data and require meaningful opt-in consent.

- Worried about bias in AI systems? Same answer.

Comprehensive privacy legislation won't fix everything. Children may still see things that they shouldn't. New businesses will still have to struggle against the deep pockets of their established tech giant competitors. Governments will still have tools to surveil people directly. But a privacy-first approach would alleviate a variety of problems now, giving us some breathing room while we explore how to finish the job.

Breaking it Down: What Does Comprehensive Data Privacy Legislation Look Like?

Not all data privacy laws are equal. Comprehensive, well-written data privacy rules will preserve the critical right to user privacy, secure the free expression that privacy enables, and protect information security. As described above, it will also do much to address other concerns about the internet that we all worry about.

Specifically, it must include the following components:

- No online behavioral ads. Companies must be prohibited from targeting ads to a person based on their online behavior. These ads are especially dangerous, because they incentivize all businesses to harvest as much consumer data as possible, either to use it to target ads or to sell it to someone who will.
- Real minimization. Companies must be prohibited from processing a person's data, except as strictly necessary to provide them what they asked for.
- Strong opt-in consent. Companies must be prohibited from processing a person's data, except with their informed, voluntary, specific, opt-in consent.
- User rights. Users should have the rights to access their data, to port it, to correct it, and to delete it. These basic rights have been added to many data privacy laws and date back to a seminal 1973 government report that outlined basic fair information practices.
- No preemption by a federal law. Federal privacy law must be a floor and not a ceiling. States must be free to enact privacy laws that are stronger than the federal baseline, and to meet the challenges of tomorrow that are not foreseeable today.
- Strong enforcement with meaningful impact. People must have a private right of action to sue the corporations that violate their statutory privacy rights. Remedies must include liquidated damages, injunctive and declaratory relief, and attorney fees. People must be able to bring their claim to a judge, and not be forced into compelled arbitration.
- No pay-for-privacy schemes. Just as you shouldn't have to trade your privacy for the ability to use a service at all, you shouldn't have to pay extra for the ability to use it without being surveilled. Privacy must not be a commodity that only the wealthy can afford. This safeguard is necessary to ensure that "consent" is truly voluntary.
- No deceptive design. Companies must be prohibited from presenting people with user interfaces (sometimes called "dark patterns") that have the intent or substantial effect of impairing autonomy and choice. This protection is also necessary to ensure that consent is genuine.

Sketching the Landscape: What Real Privacy Protections Might Accomplish

Protecting Children's Mental Health

In the past few years, lawmakers have advanced legislation that ostensibly seeks to protect children's physical, mental, and emotional health from potential harm as a result of their online activity.

However, many of the proposals are laden with constitutional problems. For example, many of the laws effectively require everyone to provide proof of their age and create different rules for people judged to be children. Unsurprisingly, given the strong constitutional protections for people, including children, to access information without having to identify themselves, federal courts have blocked age verification laws in Arkansas, California, and Texas. Courts are likely to do the same in other states such as Utah.

At the federal level, a bill called the Kids Online Safety Act (KOSA) would require all websites to filter and block legal speech. It would also empower state attorneys general to bury companies in litigation over content they simply believe will be "harmful" to young people—which, in many states, could include content about trans healthcare, abortion medication, banned books and more. This law is also likely unconstitutional for similar reasons.

While those laws make their way through the courts (and the children they are supposed to protect grow up), Congress could be passing comprehensive data privacy legislation. Such legislation would protect children immediately by limiting the amount of data that companies can collect, use, and share about everyone—including children. That, in turn, would limit the kinds of harmful targeting that fuels the worry in many studies, surveys, and news reports. To be clear, issues like substance abuse, eating disorders, and depression are complex, and there is not clear agreement on their causes or their solutions. But there is clear agreement that people don't want themselves or their families bombarded with manipulative ads.

Supporting Journalism

Newsrooms of all kinds, from city newspapers to alt-weeklies, have been decimated in recent decades. There are plenty of reasons for this decline, among them mass consolidation started in the Reagan administration. In the wake of that consolidation, the launch of online advertising and online classifieds helped deal the final blow to many newsrooms. Today, most newsrooms depend on Big Tech's surveillance advertising to survive. This hurts everyone except the Big Tech intermediaries that rake in approximately half of every ad dollar.

Lawmakers in the U.S. and abroad propose to fix this via legislation like the Journalism Competition and Preservation Act (JCPA). This ill-conceived bill would not help ease the pressures online news outlets face. The worst part of this bill is a "link tax," an idea that has never worked. In essence, it requires tech companies to pay news outlets when linking to them in search engines or social media. We've already seen one result of this type of rule: companies simply refuse to allow links to news outlets. Given the prevalence of mis- and dis-information, the last thing we need is to make it hard to find and access reliable journalism.

A privacy bill that bans behavioral advertising can change the game by making contextual ads—advertisements based on the content of a publication, not the characteristics of each user—more appealing. This would benefit both national and regional journalism organizations. On a newspaper's site, instead of seeing ads hyper-personalized based on who you are and what you've looked at online, you'd see ads based on the article you're reading. No surveillance of your browsing, purchasing or location history required. These types of ads are harder for tech giants to monopolize, and at least one news organization even saw revenues increase when it switched to contextual ads.

A privacy law alone cannot rescue every newsroom, and we should recognize and resist advertisers trying to stretch the definition of contextual ads to more resemble behavioral ads. But doing privacy first would put news organizations on a far more equal and independent footing. That helps them, their advertisers and, above all, their readers.

Protecting Access to Healthcare

When the Supreme Court ruled that the U.S. Constitution does not protect the right to an abortion, triggering multiple state laws criminalizing abortion, many people worried about the potential for law enforcement to access medical data related to reproductive health. We use apps such as Facebook and others to talk to our friends and family about our health. We also store a lot of sensitive health data from smartwatches or activity trackers in smartphone apps, which provide a place to log everything we do ranging from our heart rate to menstruation. Much of this health data, like any data collected in apps, is not protected by a comprehensive national privacy law. App developers can share or sell some of it to advertisers, data brokers, or law enforcement.

Most solutions we've seen thus far, including proposals like the My Body My Data Act, focus narrowly on health data. If passed, these bills would lead to a welcome improvement to our privacy, but focusing only on health data leaves out all sorts of potential privacy harms. Information directly related to reproductive and sexual health data isn't the only kind of data that could be used against abortion seekers, providers, or their loved ones— especially the vulnerable populations that are the most likely targets.

That's why we need protections for all the data we create, and we need to protect it wherever it is stored. This means companies need clear, opt-in consent to the processing of the data, and they should provide tools to delete that data if desired. A

comprehensive law that protects privacy across the board would be less confusing for everyone and provide more robust safeguards against future threats.

Fostering Digital Justice

As a practical matter, poor people usually get poorer privacy. Corporations, governments, and others use personal data in many discriminatory ways including direct decision-making about access to vital benefits and indirect decision-making about opportunities across the board, including in job searches, housing, and pricing. For example, lower-income people are often less able to avoid corporate harvesting of their data—either because lower priced technology may be less secure or because companies may charge a higher price for privacy and security (or offer payment for you to give up your privacy).

Once data is collected, it can then be used in discriminatory ways, including by companies directing risky advertisements to vulnerable groups, companies excluding certain groups from receiving positive opportunities, or bad actors misusing data to harass individuals or groups. In addition to being highly invasive, some technologies—such as face recognition—can result in dangerous errors, particularly pertaining to Black people. Even if face recognition technology were always accurate, it would still have an unfair racially disparate impact because surveillance cameras are over-deployed in communities of color. Finally, much of the data collected by corporations can eventually be obtained by law enforcement (through subpoenas, court orders, warrants, or purchase) and feed into a criminal justice system that disproportionately impacts Black and Brown communities.

Rigorous enforcement of existing civil rights law—particularly in housing, employment, and credit—is a necessary backbone to protect against and create real remedies for overt discrimination and disparate impacts online. But privacy legislation can also help on the front end by minimizing data that companies collect and process in the first place. It is harder (though not impossible) for companies to target a person based on protected characteristics if they don't collect that data in the first place. Digital privacy legislation is civil rights legislation.

Additionally, any strong data privacy law would ban pay-for-privacy schemes, to ensure privacy is not a luxury for only those who can afford it. When a person declines to waive their privacy rights, companies must be prohibited from charging them a higher price, providing a lower quality, or refusing service.

Alleviating Generative AI Anxiety

Anxiety about generative AI is growing almost as fast as the uses of the technology itself. Artists are concerned about how their work trained generative AI; human rights workers worry about how images are used to create deepfakes and misinformation experts have noted that incorrect information related to the news or with health advice may appear in social media or search results.

But policymaking in this fast-changing area must be precise, careful, and practical. For example, while there are legitimate concerns about the well-being of artists, we should not rush to expand copyright law or the right of publicity. And while there are legitimate concerns about misinformation, we should not rush to criminalize deepfakes.

One concern deserves immediate attention: many companies are using the information they collect from their customers as training data for generative AI. These include some of the generative AI platforms, among many other business sectors. A "privacy first" approach, including minimization and consent rules, would help solve this problem, and ensure that people have a say over how their private data is used.

Inhibiting Foreign Government Surveillance

Nearly all social media platforms and other online businesses harvest and monetize our personal data and encourage other online businesses to do the same. The result is that detailed information about us is widely available to many actors, including governments, both democratic and authoritarian.

This year, lawmakers spent a lot of time focusing on TikTok in particular and a misguided attempt to ban or severely restrict its use in the United States. TikTok raises special concerns, given the surveillance and censorship practices of its home country, China. Still, the best solution to these problems is not to single out one business or country for a ban. If the government banned TikTok, it would undermine the free speech and association of millions of users. It would also intrude on TikTok's interest in disseminating its users' videos—just as bookstores have a right to sell books written by others, and newspapers have a right to publish someone else's opinion.

By reducing the massive stores of personal data collected by all businesses, however, we will reduce opportunities for all governments, China included, to buy, steal, or compel it. It's a win-win all around.

Clearing Space for Competition

A handful of technology companies run most social media, shopping, and search platforms, frequently as part of conglomerates that offer many internet-based services. Their vertical integration and lack of direct competition gives them free rein to collect as much user data as they want, use it for whatever business model they choose, and share it or hoard it as they see fit. The privacy harms of tech monopolies are well-documented, but let's tick through a few of the more prevalent competition problems that relate directly to data privacy:

- Since dominant social networks aren't interoperable, it's not possible to engage with them without an account, giving the tech platforms full control over user data.

- Big tech's ubiquity makes it difficult for startups to compete and attract funding, and even when they do, the tech companies tend to solve the problem of competition by just buying potential challengers.
- Most of these companies, including Google, Meta, and Amazon, are also vertically integrated with surveillance advertising, meaning they control data from collection to sale, making it difficult for less-harmful advertising models to compete.
- Platform-specific app stores add another layer of concern. For example, Apple doesn't allow alternative app stores on its mobile operating system, a rule that undermines the privacy of a number of its users.
- Big tech's collective power gives them outsized influence over state privacy laws, making them weaker and weaker.
- Data portability has gained acceptance after the passage of both the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). With these laws, any company that operates in California or Europe needs to offer data portability to its customers. But data portability is most effective if you have somewhere to take it. We need alternatives to make it truly useful.

The increase in antitrust lawsuits and new scrutiny of mergers we've seen over the last several years are a good start to tackling this problem. Unfortunately, the legislative proposals that attempted to create new tools to address monopoly abuse in tech, including the American Innovation and Competition Online Act, the Open App Markets Act, the ACCESS Act, and the Digital Advertising Act all stalled in Congress. Some of these have included troublesome restrictions on editorial judgment. And none of them takes a comprehensive approach.

But here, too, privacy is an essential part of the solution, particularly data portability rights that ensure users who don't like a company's privacy practices can pack up their accounts and take their data elsewhere. Combine that with a private right of action, which means users can sue companies that violate their privacy, and you get a baseline for real competition in tech. Add in limits on data collection and bans on behavioral ads, and suddenly the entrenched Big Tech business model is a lot less stable, opening the door to competitive alternatives. Privacy is also a central requirement for safe interoperability. Privacy and competition work hand in hand to address monopoly harms.

Conclusion

New technologies and business models can cause real and unexpected harms and the desire to fix them is entirely understandable. To do that, we must think beyond our reasonable emotional responses to the harms articulated and carefully consider the proposed solutions. For too long, policymakers and regulators have offered reactive and ill-considered proposals that not only cause collateral damage but don't even address the underlying problem.

Doing privacy first is an alternative, practical, way forward that has a real shot at solving the shared problem that fuels many of today's harms. It creates a path toward a better future, where the interests of the companies that create the technical platforms and tools that we all rely on are better aligned with our interests in living our lives consistent with human rights and civil liberties. We would be less stuck in a world of relentless tracking, discrimination, and the technology monopolies that limit and control our access to information and opportunities.

Privacy first isn't a cure-all. The truth is, we didn't get into this situation because of just one problem in our society and its technologies. But with this one big step in favor of privacy, we can take a bite out of many of those problems, and foster a more humane, user-friendly technological future for everyone.