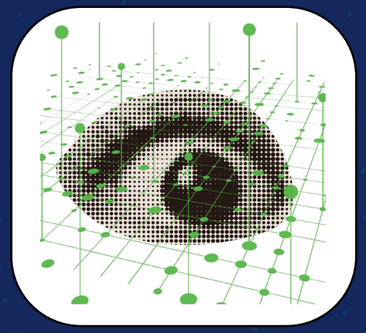


epic2024

ANNUAL REPORT

Thirty years of watching the watchers.

epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

1519 New Hampshire Avenue NW
Washington, DC 20036
(202) 483-1140
info@epic.org

epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

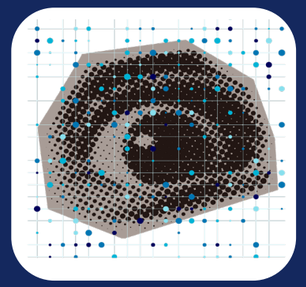
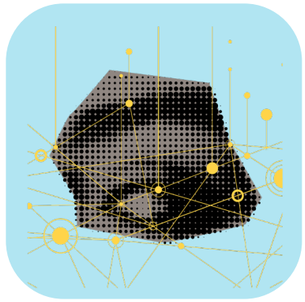


Table of Contents



About EPIC

Established in 1994, EPIC is an independent nonprofit organization. Our mission is to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.

We pursue a variety of activities, including litigating cases on emerging privacy issues, obtaining and publishing records to lift the veil on government data collection, providing expert advice to policymakers and lawmakers, and facilitating dialogue between advocates, experts, and decisionmakers.

EPIC does not accept support from corporations or government agencies. We have no clients, no customers, and no shareholders.

We believe privacy is a fundamental right, the internet belongs to the people who use it, and there is a responsible way to use technology.

Letter from the Executive Director

In 2024, we celebrated EPIC's 30th anniversary and reflected on three decades spent on the front lines defending individuals and communities against government and corporate data abuse. As we closed out our third decade, we entered a moment of chaotic transition—one that has brought us back to our core mission of holding the powerful to account for unlawful surveillance and shining light on the secret data systems impacting our lives. We are prepared in the years ahead to resist intrusions by big tech and big government alike.

The status quo is simply not acceptable. Democratic rights and institutions have been made subservient to a surveillance prerogative that poisons our discourse and threatens to rot the pillars of our constitutional order. In 2024 EPIC fought back against surveillance creep and worked to build new guardrails to protect our data, to empower individuals in our digital economy, and to ensure that AI systems and new technologies do not trample individual rights. That means holding digital platforms accountable to their users and putting the power back into the hands of individuals. Our team is working every day to shape the law toward those goals. Just this year, EPIC:

- Called out the illegal rollout of black box AI systems that impact users worldwide. We filed a complaint with the FTC urging the Commission to investigate OpenAI and filed suit against tenant screening company RentGrow for unfair and deceptive practices tied to their automated tenant screening reports.
- Played a key role in the passage of strong state privacy bills, providing critical expertise to state legislators to help them challenge Big Tech lobbyists and fight to enact legislation that would put the privacy and consumer protections of their constituents first.
- Pushed back against the expansion of facial recognition at our borders and in our cities. We challenged law enforcement agencies, including Customs and Border Protection and the Department of Homeland Security, to limit the rollout of these technologies and ensure that they are never mandatory and always accountable.
- Launched our Platform Accountability & Governance Project, which challenges Big Tech's efforts to escape liability for the harm caused by their business practices and advocates for strong governance and accountability mechanisms to protect the speech, privacy, anti-discrimination, and safety rights of internet users.
- As we are launched into the dangers of this new transition in 2025, it is more important than ever to account for power and to hold the powerful to account. EPIC prides itself on being a fierce champion for human rights, and we will fight to protect individuals against data abuse and government and corporate overreach. That fight will continue next year as we brace for new changes and threats of government and corporate overreach.

Alan Butler
EPIC Executive Director & President

Celebrating EPIC'S 30th Anniversary & 2024 Champions of Freedom Awards

2024 marked EPIC's 30th anniversary! From organizing the first internet petition to oppose the NSA's "Clipper Chip," to challenging the use of invasive body scanners in airports, to publishing The State of Privacy scorecard, EPIC has championed privacy, opposed mass surveillance, and fought to protect democratic values for decades. We celebrated our 30th Anniversary with our annual Champions of Freedom Awards dinner.

EPIC established the Champions of Freedom Awards to recognize individuals who have helped safeguard the right to privacy, open government, and democratic values with courage and integrity.

The theme of the 2024 event was **"EPIC 30/50: Looking Back and Looking Forward."** EPIC has championed privacy, opposed mass surveillance, and fought to protect democratic values for decades. As we reflected on 30 years of EPIC's work, and the 50th Anniversary of the Privacy Act of 1974, we considered what brought us all to this current moment and charted the course for the decades ahead.

EPIC celebrated public officials and leading experts who have led the charge against surveillance capitalism and data abuses. We honored three Champions of Freedom, one Privacy Champion, and one Lifetime Achievement Awardee (in memoriam):

- Senator **Sara Love** of Maryland, Representative **Maggie O'Neil** of Maine, and Representative **Monique Priestley** of Vermont
- **Damon Hewitt**, President and Executive Director, **Lawyers' Committee for Civil Rights Under Law**
- **Ross Anderson**

Program Areas & Projects

AI & Human Rights

EPIC's AI & Human Rights Program centers conversations about AI on the real-world human impacts and harms of these systems, prioritizing individual rights and protections. EPIC pushes back on assumptions about AI superiority, highlights how current AI practices run directly counter to privacy principles, and advocates for improving policies and enforcement.

AI Policy
Risk Assessments
Screening & Scoring
Government and Commercial use of AI
AI in the Criminal Justice System

Consumer Privacy

EPIC's Consumer Privacy & Data Protection Program safeguards privacy and protects the public from abusive data practices by establishing robust and enforceable limits on the collection, retention, and use of personal information. Drawing on EPIC's deep legal and technical expertise, we rein in abusive data practices and operationalize our vision for a more privacy- and rights-protective future through incisive, fearless, and relentless advocacy at all levels of power.

Online Advertising & Tracking
Data Minimization
Social Media Privacy
Data Brokers
Communications Privacy
Competition & Privacy
Children's Privacy
Location Tracking
Health & Reproductive Privacy
Cybersecurity

Platform Governance & Accountability

EPIC's Platform Governance and Accountability Program focuses on developing a human-first understanding of how online platforms operate, where those operations cause harm, and how the incentives platform companies face can be changed to minimize those harms. EPIC ensures that laws can be enforced against platform companies and develops a platform governance policy that accounts for users' many interests.

Age Assurance
Section 230
First Amendment
Online Harassment
Web Scraping

Surveillance Oversight

EPIC's Program on Surveillance Oversight opposes the unchecked expansion of surveillance systems, one of the greatest threats to our democracy. EPIC advocates for greater oversight of and restrictions on surveillance systems and works to identify, make public, and where appropriate roll back surveillance technologies that undermine our privacy, civil liberties, and civil rights.

FISA Section 702
Face Surveillance & Biometrics
Drones & Aerial Surveillance
Government Databases
Traveler Screening & Border Surveillance
Intelligence Surveillance

International Privacy

EPIC's international privacy work promotes privacy, data protection, and open government laws and policies globally. From new privacy regulations to international enforcement cooperation to data sharing agreements, information is no longer limited by geographic boundaries. Personal data must be protected globally.

In May 2024, EPIC presented its International Privacy Champion Award to the Tire Meu Rosto da Sua Mira Campaign at the Computers, Privacy and Data Protection (CPDP) Conference in Brussels. Pictured on the left is EPIC's Calli Schroeder and the 2024 Internationl Privacy Champions.

AI & Human Rights

EPIC continued advocating for greater enforcement against companies deploying harmful automated decision making systems. EPIC submitted several complaints to the Federal Trade Commission to investigate OpenAI, Deloitte, and Thomson Reuters. We called on the FTC to investigate OpenAI for failing to meet established public policy standards for responsible AI use and development, offering products with unsafe security, privacy, and business practices, perpetuating unfair and deceptive practices in their product development and release, and causing significant consumer harm. Likewise, we, along with National Health Law Program (NHeLP) and Upturn, urged the agency to investigate Deloitte for its development and maintenance of a faulty Medicaid eligibility system known as the Texas Integrated Eligibility Redesign System (TIERS). We also urged the FTC to investigate Thomson Reuters, the multinational information services conglomerate, for its development and operation of a faulty fraud detection system known as "Fraud Detect."

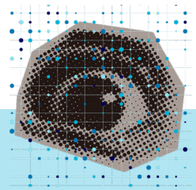
EPIC submitted public comments to a variety of state, federal, and international agencies, including the Department of Justice's National Institute of Justice, National Telecommunications and Information

Administration, Office of Management and Budget, National Institute of Standards and Technology, Federal Communications Commission, the European Commission, UK Department for Education, and the Dutch data protection authority Autoriteit Persoonsgegevens. We filed comments to the FCC urging the agency to increase the granularity of information they plan on requiring broadcasters to disclose when airing political ads that use AI content. We also submitted comments to the National Institute of Standards and Technology with feedback on three draft documents the agency produced in response to President Biden's AI Executive Order, including additional recommendations on generative AI risk classification, AI transparency, and stakeholder engagement. We submitted

> "You cannot untrain generative AI," said EPIC's Grant Fergusson, a fellow at the Electronic Privacy Information Center. ***"Once the system has been trained on something, there's no way to take that back."***
>
> *Axios (Mar. 14, 2024): Generative AI's Privacy Problem*

EPIC's Alan Butler speaks on an ABA Webinar, "AI Essentials for Lawyers: What You Need to Know to Protect Your Clients in the Digital Age" on Mar. 27, 2024

comments to the Department of Justice's National Institute of Justice, urging the agency to rein in the harmful biases, inaccuracies, and abuses at the core of criminal justice AI systems. EPIC also filed comments with the Dutch data protection authority, Autoriteit Persoonsgegevens, regarding use of and prohibitions on emotion recognition surveillance.



Litigation Spotlight

EPIC and the National Association of Consumer Advocates filed suit against tenant screening company RentGrow for unfair and deceptive practices tied to its automated tenant screening reports. The lawsuit, brought under the D.C. Consumer Protection Procedures Act, alleges that RentGrow automatically generates tenant screening reports that contain serious errors and biases. These errors and biases can cause consumers across the District—most often those from marginalized populations—to lose out on housing opportunities through no fault of their own. We allege that RentGrow neither vets the third-party information it uses to generate tenant screening reports nor monitors its services for errors and biases that could harm consumers.

EPIC's Grant Fergusson at a BenCon 2024 panel, "Emerging Legal and Policy Trends in State and Federal AI Governance" on Sep. 17, 2024

For AI policy, we published a rundown of the major privacy and AI bills that were signed into law this past California Legislative session and a brief explanation of what each law does.

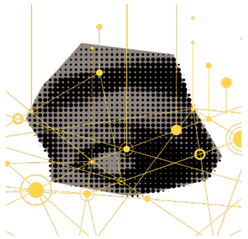
We also published analysis of the current state of federal AI regulation in the wake of Supreme Court decisions in *Loper Bright Enterprises v. Raimondo*, *SEC v. Jarkesy and Corner Post*, and *Inc. v. Board of Governors of the Federal Reserve System*. The analysis explores promising regulatory measures overseas and offers a path forward for AI regulation: product liability lawsuits.

> OpenAI is "the subject of this first complaint," said Calli Schroeder, senior counsel for EPIC. "It's because of the outsized impact they have in the industry, and they have set themselves up as leaders and front runners in this space. ***So if you want to be a leader in this space, you also have to establish better practices and be an example in that way.***"
>
> *MLex (Oct. 29, 2024): Generative AI Models Built on Data Scraped 'Indescriminately' Are a Concern, Privacy Group Tells US FTC*

Notable Analysis

On March 13, the European Union Parliament passed the Artificial Intelligence Act (AI Act), taking the penultimate step in a years-long legislative process. Originally proposed in early 2021, the sweeping, harms-based Act categorizes artificial intelligence systems by preconceived risks to fundamental rights, public safety, and public health into prohibited, high-risk, or low or no-risk systems. Depending on the category, the Act either (1) prohibits the technology from being placed on the market and deployed, (2) establishes mandatory safeguards and legal liabilities across the AI system's supply chain, or (3) recommends the installation of a voluntary code of conduct. EPIC's Maria Villegas Bravo explained the current EU data protection law to contextualize the AI Act, analyzed its provisions, and provided key takeaways for legislators aiming to implement AI legislation in the United States.

EPIC's Ben Winters speaking at a FTC Tech Summit panel, "AI + Consumer Applications" on Jan. 25, 2024



EPIC's Grant Fergusson at Yale's Information Society Project's Propaganda and Emerging Technologies Conference panel, "Emerging Forms of Propaganda in Elections" on April 5, 2024

Consumer Protection

EPIC's Christopher Frascella at the Consumer Rights Litigation Conference panel, "Data Brokers and the FCRA in the Algorithmic State" on June 26, 2024

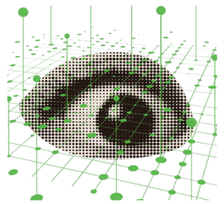
EPIC engaged in a wide range of research, education, and advocacy activities to promote the protection of and privacy of consumers.

EPIC engaged extensively with the Consumer Financial Protection Bureau's (CFPB) Fair Credit Reporting Act (FCRA) rulemaking. We published a series of resources about the rulemaking process and the urgent need to crack down on data brokers. EPIC also developed public education resources and coordinated coalition support for the rulemaking. We sent letters and comments urging the CFPB to release a proposed rule to strengthen FRCA, supporting the agency's proposed rule to largely prohibit the inclusion of medical debt information on credit reports, and supporting a petition to urge the CFPB to open a rulemaking to address issues of coerced debt.

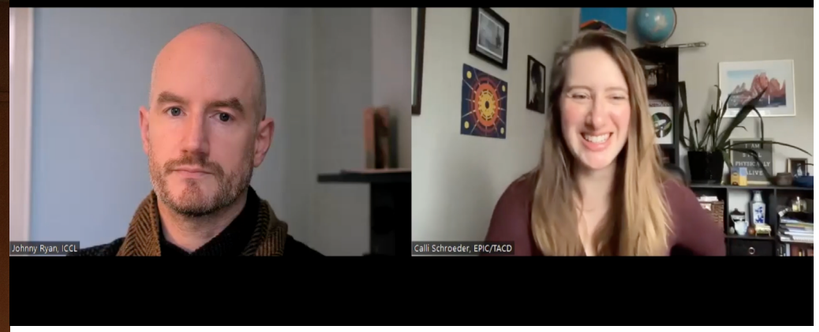
We filed and joined numerous public comments to the European Commission, California Privacy Protection Agency, FCC, FTC, CFPB, GSA, Financial Crimes Enforcement Network (FinCEN), Cybersecurity and Infrastructure Security Agency (CISA), and the U.K. ICO. Notable work included comments to the European Commission urging the Commission to address surveillance gaps in the EU-US Data Privacy Framework and protect the privacy rights of EU residents. We filed two comments to the FCC regarding its proposed rulemaking on connected cars under the Safe Connections Act.

We submitted a comment applauding the FTC's efforts to modernize the COPPA Rule and offered several recommendations to improve the efficacy of the FTC's proposed changes. We also submitted comments calling on the FCC to ensure robust oversight, accountability, and transparency for the Cyber Trust Mark program, a voluntary cybersecurity labelling program for Internet of Things (IoT).

As part of our Telephone Subscriber Privacy Project, we advocate for the FCC to strengthen privacy and data security protections. We filed an amicus brief in *Howard v. Republican National Convention (RNC)*, a case concerning whether MMS messages containing a video and sent without the recipient's consent constitute a violation of the artificial or prerecorded voice provisions of the Telephone Consumer Protection Act. We also sent a coalition letter and filed robust comments to the FCC regarding its implementation of the requirements of the Safe Connections Act of 2022. The rulemaking sought to help survivors of domestic violence separate their phone line from a shared account with an abuser, to protect the privacy of calls with hotlines and shelters, and to support survivors experiencing financial hardship through affordability programs. We also submitted an amicus brief urging the Sixth Circuit to find that the FCC has the authority to require telecom companies to notify phone subscribers when their data has been accessed without authorization.



EPIC's Sara Geoghegan and Suzanne Bernstein at GW's Ethical Tech Initiative panel, "Two Years Post-Dobbs: The Legal Landscape of Reproductive Data Privacy" on June 26, 2024



EPIC's Calli Schroeder moderating a TACD virtual panel, "Decoding AdTech: Navigating the Crossroads of Privacy, Policy, and AI in Commercial Surveillance" on March 11, 2024

Our continued work on health and reproductive privacy by filing an amicus brief in support of the Plaintiffs' arguments in *Vita v. New England Baptist*, a case concerning case concerning hospitals that used undisclosed tracking software, such as Meta or Google's pixels, to collect and disclose patients' private health information. EPIC also filed a complaint to the FTC on Google's failure to honor its public promises to delete sensitive location data revealing whether a user has visited a medical facility.

EPIC's Alan Butler in a House Committee on Energy and Commerce hearing, "Safeguarding Americans' Communications: Strengthening Cybersecurity in the Digital Era" on Jan. 11, 2024

"This information being sold or shared with data brokers and other entities ***hypercharge the online profiling*** that we're so used to at this point, and ***the more sensitive the data, the more sophisticated the profiling can be***," [Suzanne] Bernstein said.

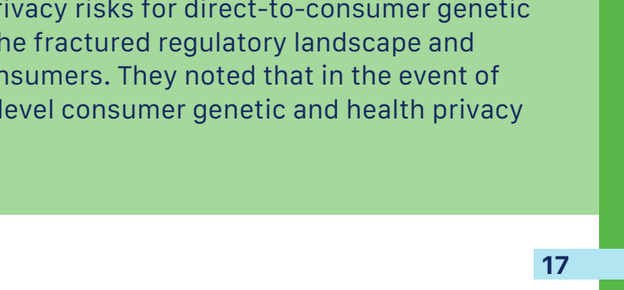
LA Times (Nov. 20, 2024): *Are You Tracking Your Health with a Device? Here's What Could Happen with the Data*

"***Meaningful privacy protection is something that comes from robust and well-enforced rules of the road, and a competitive and efficient marketplace***—and not from the choices of a few dominant platforms," [John] Davisson said.

Bloomberg Law (April 8, 2024): *Apple Hit Over Privacy as US Tries to Undercut Antitrust Defense*

Analysis

Somebody Spilled the Genes: 23andMe's Downturn Highlights Insufficient Privacy and Data Security Safeguards for Consumer Genetic Data

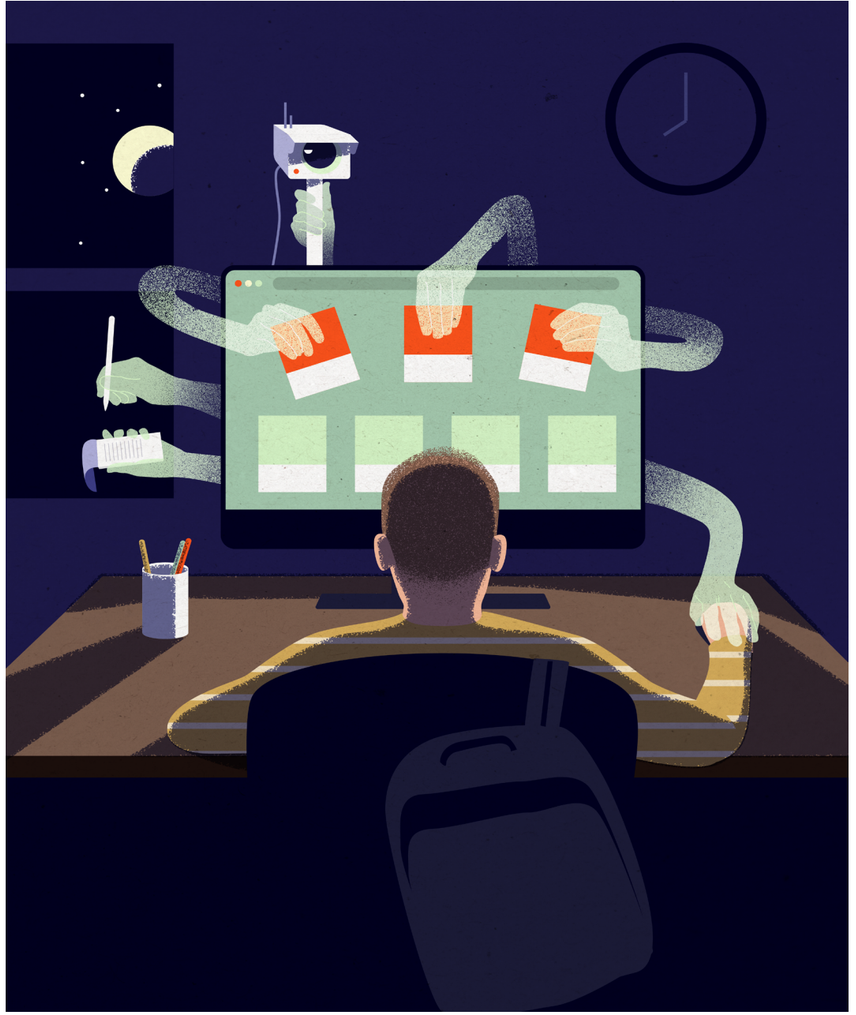


December 5, 2024 | **by Suzanne Bernstein (EPIC Counsel), Abigail Kunkler (EPIC Law Fellow), and Matthew Contursi (EPIC Fall Semester Clerk)**

Notable Analysis

Prior to 23andMe filing for bankruptcy in 2025, the direct-to-consumer testing company was facing an uncertain future due to loss of stock market value, large workforce layoffs, and a massive 2023 data breach that compromised at least 6 million users' genetic data. EPIC's Suzanne Bernstein, Abigail Kunkler, and law clerk Matthew Contursi analyzed the consumer privacy risks for direct-to-consumer genetic testing companies like 23andMe as well as the fractured regulatory landscape and unclear privacy protections for 23andMe consumers. They noted that in the event of 23andMe's downfall, the durability of state-level consumer genetic and health privacy safeguards will soon be tested.

Platform Governance & Accountability



EPIC launched the Platform Accountability and Governance program this year to focus on online platforms as important centers of privacy, attention, and speech harms. We focus on the ways platform design can cause harm and advocate for regulations that protect user's rights and safety.

EPIC's amicus strategy focused on advocating for interpretations of the First Amendment and Section 230 that provide maximal speech and privacy protections to users without giving tech companies undue immunity from accountability.

EPIC led the amicus effort in support of the California's Age-Appropriate Design Code in a First Amendment challenge brought by the lobbying group NetChoice—whose members include Google, Meta, Amazon, Twitter, and TikTok. EPIC submitted several amicus briefs at both the district and circuit court levels in the case. Over the summer, the Ninth Circuit reversed a dangerous decision of the district court that would have rendered all data privacy laws presumptively unconstitutional. The court sent the case back to the district court with instructions for NetChoice to bolster its record and constitutional argument. When NetChoice renewed its request for a preliminary injunction without doing as the Ninth Circuit required, EPIC filed another amicus brief explaining how NetChoice's arguments against the CAADC's data protection provisions fail under scrutiny.

EPIC also filed an amicus brief in another *NetChoice v. Bonta* case, where NetChoice challenged California's regulation of addictive feeds (SB 976). EPIC's amicus brief in the district court was the only amicus brief filed on either side. The judge cited to our brief and imported much of its reasoning to find that NetChoice failed to adequately support its request for a preliminary injunction against SB 976's addictive feeds restriction and age assurance requirement.

> The provision "was meant to accomplish a very limited purpose: preventing lawsuits that would force internet companies to either screen for and block all illegal content, or to not moderate their platforms at all," Iorio and McBrien wrote. "This limited purpose protects free speech online; ***an overbroad interpretation of Section 230 is a license for internet companies to act with impunity***, removing an important incentive to design safe products and comply with generally applicable laws."
>
> Roll Call (May 14, 2024): *Lawmakers Issue Ultimatum to Teach Platforms Over Data Privacy*

EPIC filed an amicus brief in *Free Speech Coalition v. Paxton*, an important Supreme Court case that could impact the viability of many recently enacted and proposed kids' safety and privacy laws. EPIC submitted a brief in this case in support of neither party. We urged the Court to use a fact- and statute-specific analytical framework that is able to distinguish between constitutional and unconstitutional uses of age assurance methods. EPIC foresaw that, in the likely event the Supreme Court ruled at least some age assurance constitutional, the Court should recognize that privacy-invasive methods impose a burden on speech where privacy-protective ones would not necessarily do the same.

EPIC also submitted an amicus brief in the case *Doe v. Grindr*, a case involving the proper interpretation of Section 230 of the Communications Decency Act. The case is a lawsuit against Grindr, a popular dating app for the LGBTQ+ community that has often come under fire for allegedly prioritizing profits over users' privacy and safety.

EPIC also filed an amicus brief in *X v. Bonta* addressing the fact that platform transparency is vital, and the Court should not overturn transparency statutes merely because of the hypothetical harms to free speech rights. EPIC's brief then explains that because of the nature of content moderation transparency laws and the strength of the public and government's interest in access to information, a successful challenge to a content transparency law cannot be supported by hypothetical future harm alone.

EPIC submitted comments with the Center for Digital Democracy urging the New York Attorney General to center privacy and age determination best practices in its rulemaking to implement the New York SAFE for Kids Act. The NY SAFE for Kids Act prohibits social media platforms from providing "addictive feeds" and nighttime push notifications to minors without parental consent. Additionally, EPIC submitted comments to the applauding the agency's efforts to modernize the COPPA Rule and offered several recommendations to improve the efficacy of the FTC's proposed changes.

We also published several analysis pieces on key cases related to Section 230, state content moderation laws, platform accountability, and First Amendment.

"NetChoice is very clear that they don't think that any privacy law that actually does something to protect users from privacy harms, that has data minimization requirements and use restrictions, would pass constitutional muster. ***And that is disturbing.*** They also think that any regulation of design-mediated harms, like addictive algorithms and dark patterns, they think that all of those would be unconstitutional. So it really is this push to ensure that the internet remains this lawless place where kids and parents are just scrambling to figure out what to do and tying the hands of the government from doing anything to protect Americans." – Megan Iorio

Marketplace (Mar. 27, 2024): *What a Privacy Organization and Big Tech's Lead Lobbying Group Think About Internet Regulation*

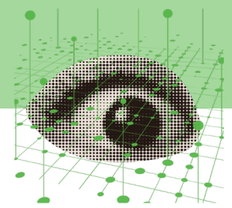
Analysis

Far From a Punt, SCOTUS's NetChoice Decision Crushes Big Tech's Big Litigation Dreams

July 16, 2024 | **Megan Iorio, Senior Counsel**

Notable Analysis

In July 2024, the Supreme Court sent NetChoice's challenges against Texas' and Florida's content moderation laws back to the lower courts because NetChoice hadn't met its burden of showing that the laws were unconstitutional in their entirety. EPIC's Megan Iorio analyzed how the decision is a huge blow to Big Tech's litigation strategy of requesting the broadest possible relief from regulation based on nothing more than vibes.



Surveillance Oversight

> "That will ultimately accelerate the use of our faces as our ID, and that has some very important implications for privacy, civil liberties, civil rights and our democracy," [Jeramie Scott] said, adding that the lack of federal regulations around facial recognition's use means that — despite TSA's current privacy requirements — ***"what may be the safeguards today does not mean they will be the safeguards tomorrow."***
>
> NextGov (Jan. 29. 2024): *TSA Uses 'Minimum' Data to Fine-Tune Its Facial Recognition, But Some Experts Still Worry*

EPIC continued to pursue important work addressing current gaps in surveillance oversight, constitutional protection, transparency, and agency accountability.

EPIC has long called for Congress to amend Section 702 of the Foreign Intelligence Surveillance Act (FISA) and has worked with members of Congress and with a bipartisan coalition of civil liberties groups to develop consensus reforms, including: more robust safeguards on the collection and querying of U.S. person information under Section 702, greater accountability and meaningful avenues for redress, and greater transparency of the government's use of Section 702 in the cybersecurity context. EPIC joined a bipartisan coalition of civil liberties organizations in underscoring the need for significant reform to warrantless government. Despite the bipartisan support for government surveillance reform, leadership in Congress enacted the Reforming Intelligence and Securing America Act (RISAA), H.R.7888, which reauthorized FISA Section 702 for two years. Although EPIC and others raised concerns that RISAA does more to expand and entrench warrantless government surveillance than rein it in, privacy champions in Congress got closer than ever to enacting significant reform. Both the amendments that were passed in the House and those considered but ultimately failed in the Senate developed a record on reform and will help set the foundation for the next reauthorization debate. We laid the groundwork to seize the next opportunity to improve oversight of government intelligence surveillance systems.

EPIC continued to engage agencies on the use of commercially available information. EPIC and a small bloc of civil society groups met with the Office of Director of National Intelligence to provide feedback directly to the Director of National Intelligence on the agency's framework for the use of commercially available information and advocate for stronger controls. Additionally, EPIC joined by a small coalition of groups submitted comments to the Office of Management and Budget to highlight how law enforcement and intelligence agencies across the federal government access commercially available information to avoid legal requirements of the Fourth Amendment and other privacy laws.

EPIC also submitted several comments to various other federal agencies and even the European Commission.

In two separate comments to the U.S. Customs and Border Protection (CBP) agency, we urged the agency to stop expanding the flawed CBP One app as well as refrain from expanding the use of facial recognition as part of its Biometric Entry-Exit Program. EPIC also submitted comments urging the Department of Justice (DOJ) and the Department of Homeland Security (DHS) to center vulnerable communities in its crafting of new guidance on the use of facial recognition, predictive policing technologies, social media surveillance tools, and DNA analysis tools. EPIC provided recommendations to create a robust framework of safeguards to protect privacy, civil rights, and civil liberties.

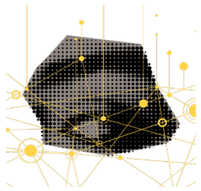
EPIC also submitted comments to the DOJ's in regard to "Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern." EPIC argued that the proposed rule is too narrow in its definition of covered data and recipients, doesn't take enough steps to safeguard the data itself, and fails to consider the myriad ways data can constitute a national security risk. We recommended DOJ modify its proposed rule to harmonize it with other U.S. regulatory efforts.

EPIC explained the dangers of federal law enforcement's use of facial recognition technology in comments to the U.S. Commission on Civil Rights and urged the Office of Management and Budget to update its Privacy Impact Assessment (PIA) guidance to close loopholes, improve transparency, and make PIAs a meaningful oversight mechanism.

In comments to the European Commission, we urged the Commission to address surveillance gaps in the EU-US Data Privacy Framework and protect the privacy rights of EU residents.

EPIC submitted a joint amicus brief in *United States v. Hunt* arguing that under the landmark Supreme Court case *Riley v. California*, police must get a warrant before searching the digital contents of a cell-phone, even if the physical phone itself was abandoned by its owner. We also joined an amicus brief in *Renderos v. Clearview AI* urging the Ninth Circuit to recognize that lawsuits against privacy-invading companies are valuable ways to protect people's rights, not back-door attempts to silence the companies' speech. *Renderos v. Clearview AI* is a lawsuit against Clearview AI, one of the most notorious face recognition companies in the world, which scraped billions of people's faces from the internet and used them to train an algorithm marketed toward the police and security services.

> "The technology hasn't been proven to be reliable as an investigative tool," [Jeramie] Scott said. ***"Knowing that facial recognition is a very powerful and pervasive surveillance tool, moving toward widespread law enforcement's use inevitably puts us in a position where our democratic values and constitutional rights will be undermined by this technology."***
>
> Baltimore Sun (Feb. 17, 2024): *Limiting Police Use of Facial Recognition Technology Gaining Support in Maryland General Assembly*



> Jeramie Scott . . . said ShotSpotter infringes on the privacy of the poor and minority populations who are predominantly exposed to it. ***"The result is undue surveillance and over-policing of marginalized communities while spending funds that could be spent on crime prevention programs instead,"*** Scott said. "Shotspotter alerts prime police to expect dangerous situations which raises the risk of harm to communities that are often already subject to a disproportionate amount of police force," Scott added.
>
> The Record (Sep. 26, 2024): *Chicago Stops Using Controversial Shotspotter Gunshot Detection System*

Analysis

Mass Hysteria Over Drones Flying in the Night Sky? It Didn't Have to Be This Way

December 20, 2024 | **Jeramie D. Scott, Director of EPIC's Project on Surveillance Oversight**

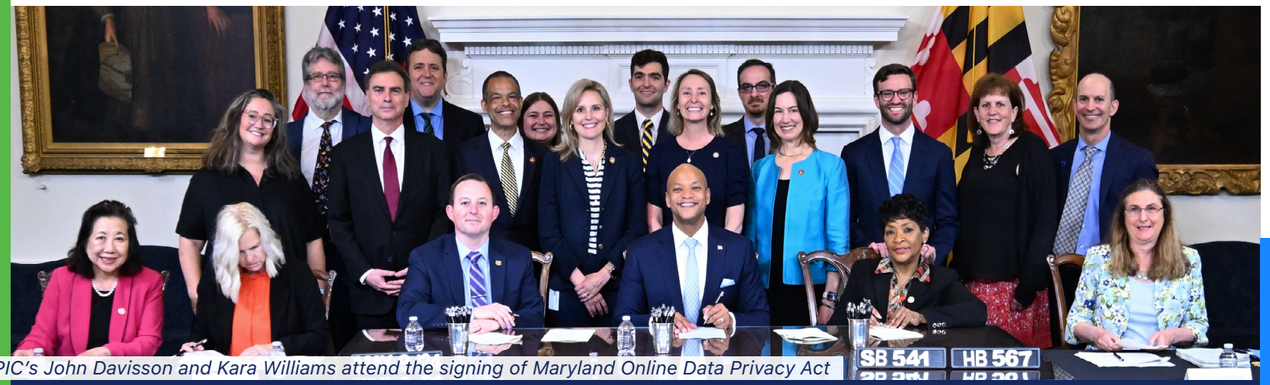
Notable Analysis

In late December 2024, nighttime drone sightings in New Jersey and other places gained national attention because of the mystery that surrounds the drones. Numerous theories popped up to fill the void left by the lack of information about why these drones were flying around at night. EPIC's Jeramie Scott discussed why aerial surveillance from these unregulated drones cause privacy concerns and how it is imperative that there needs to be more transparency about drone operations.

Policy & Testimony

In 2024, our policy work spanned across various program and issue areas, with a heavy focus on comprehensive data privacy legislation at both the federal and state level. We continued to call for comprehensive federal privacy legislation and advocated for stronger protections in the proposed American Privacy Rights Act (APRA). And as more states began to consider privacy legislation, we leveraged our work on federal privacy legislation by pushing for the strong data minimization rules from federal bills in states such as Maryland, leading to the enactment of the Maryland Online Data Privacy Act, one of the strongest privacy laws in the country. In order to build on the momentum from Maryland, EPIC and Consumer Reports released the State Data Privacy Act in September 2024, a compromise model bill built on existing state laws that meaningfully protects privacy.

EPIC is one of the nation's leading voices advocating for strong data privacy laws in the states. Versions of our state bills were introduced in Massachusetts, Maine, Illinois, Maryland, and Vermont. After tireless work supporting the drafting of, providing technical assistance on, and testifying on bills across the country, EPIC was pleased to see the passage of strong data privacy bills in Vermont and Maryland, as well as significant progress on legislation in Maine and Massachusetts.



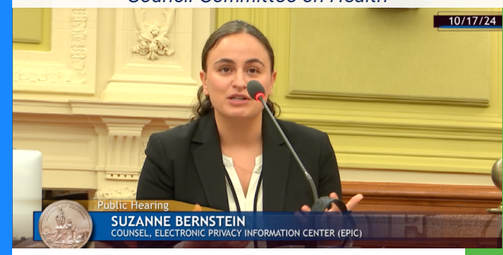
EPIC's John Davisson and Kara Williams attend the signing of Maryland Online Data Privacy Act

"Most (state laws) are copycats of each other, but especially the ones recently passed . . . It was really encouraging to see Maryland legislators say ***'No, this is not enough.' It's not enough to say companies can put whatever they want in privacy policies.*** Instead, they said companies need to look at the context of the interactions they're having with the consumer and the collection necessary for that." – Caitriona Fitzgerald

IAPP (Apr. 8, 2024): *Maryland Adds New Dimentions to US Comprehensive State Privacy Law Patchwork*

"States are stepping in and enacting state-level comprehensive data privacy laws to fill this gap, as well as laws specific to consumer health data like Washington State's My Health My Data Act. ***By passing CHIPPA, the Council has the opportunity remain a leader in consumer protection and set the bar high for Congress to do the same.***" – EPIC's Suzanne Bernstein to D.C. Council Committee on Health supporting the Consumer Health Information Privacy Protection Act (CHIPPA)

EPIC's Suzanne Bernstein testifying before the D.C. Council Committee on Health



EPIC's John Davisson testifying before the U.S. House Energy & Commerce Committee

This past year EPIC testified before the House Financial Services Committee, House Energy & Commerce Committee, and House Committee on Energy and Commerce Subcommittee on Communications and Technology on topics ranging from strengthening America's communication networks, technology in the financial sector, and how the Federal Trade Commission's practices to protect consumers.

EPIC also testified in support of various state privacy bills like: Michigan's Personal Data Privacy Act, DC Consumer Health Information Privacy Protection Act, Vermont's Data Privacy Act, and Maryland's Online Data Privacy Act.

EPIC's Alan Butler testifying before the U.S. House Financial Services Committee

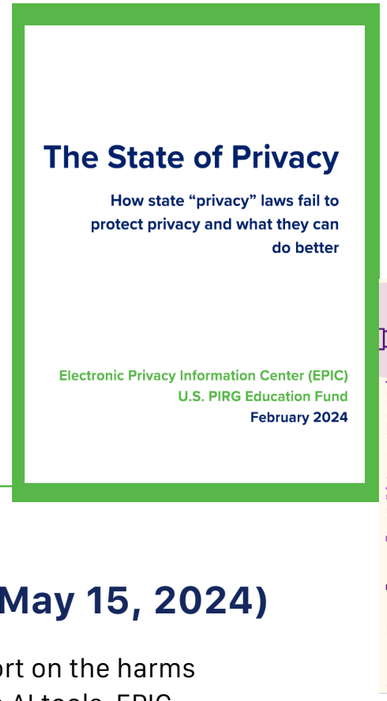
"Unfortunately, Connecticut's law allows businesses to continue collecting and using whatever personal data they want, as long as they bury what they're doing in a long privacy policy that no one ever reads. ***This is fake privacy protection—something that allows Big Tech to claim they support privacy laws, but in reality, just greenlights business as usual.***" – Caitriona Fitzgerald before the Maryland Senate Finance Commitee supporting the Maryland Online Data Privacy Act

"Far too often, the term 'innovation' has been used to obscure practices that are, at bottom, extractive and exploitative and do not serve the interests of the individuals who use these services. ***We can and should aspire for better.***" – Alan Butler before the U.S. House Financial Services Committee

Publications

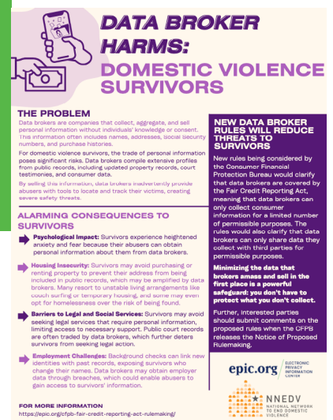
The State of Privacy: How State "Privacy" Laws Fail to Protect Privacy and What They Can Do Better (Feb. 1, 2024)

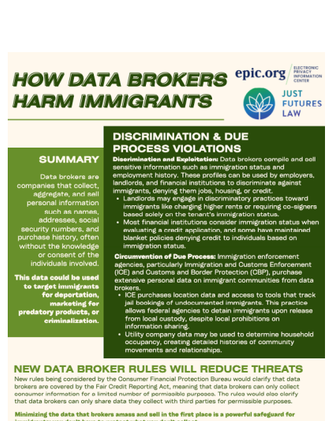
EPIC scored existing state privacy laws and made recommendations for stronger laws. In evaluating fourteen states that have passed consumer privacy legislation, nearly half received failing grades, and none received an A.

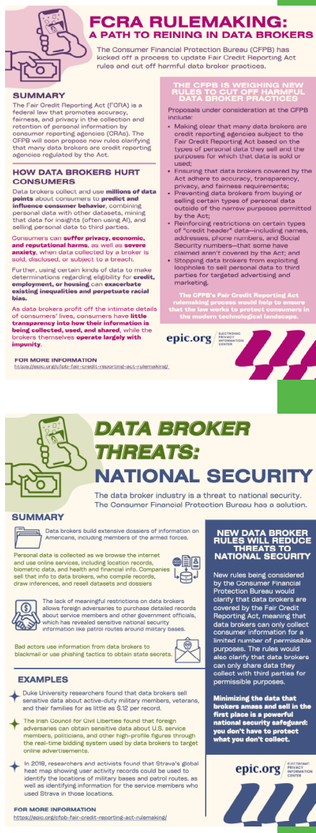


Databrokers One Pagers (June 28, 2024)

EPIC published a series of resources about the Consumer Financial Protection Bureau's (CFPB) Fair Credit Reporting Act (FCRA) rulemaking process and the urgent need to crack down on data brokers.







Generating Harms II (May 15, 2024)

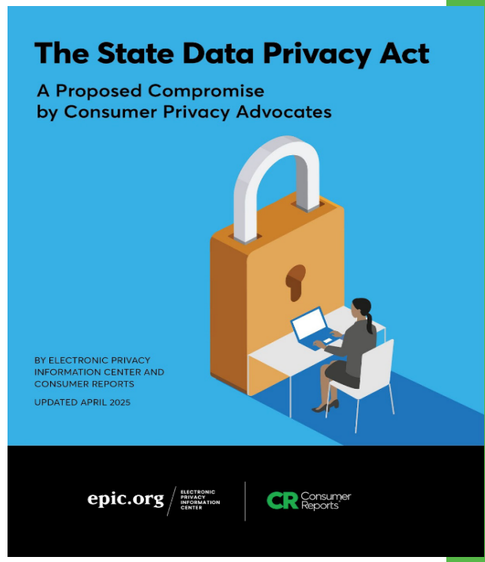
One year after its initial report on the harms stemming from generative AI tools, EPIC released a new report identifying additional harm areas and examining proposals that have been put forth to remedy generative AI harms.

AI Legislation Scorecard (June 25, 2024)

EPIC set out to create a tool to evaluate the growing wave of AI bills. Our AI Legislation Scorecard is a first-of-its-kind rubric for lawmakers, journalists, and others to use when evaluating the strength of AI bills across key metrics. EPIC's AI Legislation Scorecard came as the United States faces a tidal wave of new AI legislation, with hundreds of AI bills being introduced in at least 40 states and dozens of federal regulations following suit.

The State Data Privacy Act (Sep. 24, 2024)

In our State Data Privacy Act, in partnership with Consumer Reports, EPIC set forth a compromise bill built on existing state laws that meaningfully protects privacy while encouraging innovation. We restructured our model legislation as a set of proposed amendments to the Connecticut Data Privacy Act (CTDPA), a bill industry often cites as a model for other states to adopt. CTDPA contains far too many loopholes that prevent it from offering strong privacy protections, but we have seen across many states a demand by lawmakers to build off the CTDPA base text.



Our Work by the Numbers

SUBMITTED
40+
COMMENTS

WELCOMED
3
NEW FELLOWS

HOSTED OR PARTICIPATED IN
22
EVENTS

TESTIFIED
10
TIMES

FEATURED IN
245+
NEWS PIECES

FILED
4
COMPLAINTS

PUBLISHED
4
REPORTS

LAUNCHED
1
NEW PROGRAM

PUBLISHED
37
BLOG POSTS

CREATED
7
FACT SHEETS

ADDED
10
MEMBERS TO ADVISORY BOARD

LAUNCHED
2
PROJECTS

FILED
7
BRIEFS

EPIC Staff

EPIC hosts an Internet Public Interest Opportunities Program (IPIOP), an intensive legal internship held during the summer, fall, and spring terms. The IPIOP Program gives law students the opportunity to actively participate in various aspects of Internet law, policy, and legislation. The program provides opportunities for clerks to experience first-hand the new and exciting intersection between Internet law, privacy, and public policy. In 2024, we had the pleasure of working with legal interns from Brooklyn Law School, Benjamin N. Cardozo School of Law, Columbia, George Washington University, Georgetown, Indiana University, New York University, UC Davis, University of North Carolina School of Law, and Yale.

Alan Butler
Executive Director and President

Caitriona Fitzgerald
Deputy Director

John Davisson
Senior Counsel and Director of Litigation

Sara Geoghegan
Senior Counsel

Megan Iorio
Senior Counsel and Director of the Platform Accountability & Governance Program

Calli Schroeder
Senior Counsel and Director of the AI & Human Rights Program

Jeramie Scott
Senior Counsel and Director of the Surveillance Oversight Program

Ben Winters
Senior Counsel

Enid Zhou
Senior Counsel

Kabbas Azhar
Equal Justice Works Fellow

Chris Baumohl
Law Fellow

Suzanne Bernstein
Counsel

Maria Villegas Bravo
Law Fellow

Grant Fergusson
Counsel

Christopher Frascella
Counsel

Caroline Kraczon
Law Fellow

Abigail Kunkler
Law Fellow

Thomas McBrien
Counsel

Mayu Tobin-Miyaji
Law Fellow

Jake Wiener
Counsel

Kara Williams
Law Fellow

Jackie Buchinger
Office Manager

Becca Downes
Executive Assistant

EPIC Board of Directors

Shoshana Zuboff
Chair

Ari Ezra Waldman
Chair-Elect

Roger McNamee
Treasurer

Christopher Wolf
Secretary

Christine Borgman

Danielle Citron

Jeff Jonas

Len Kennedy

Harry Lewis

Anna Lysyanskaya

Anne Washington

See EPIC's full Advisory Board: https://epic.org/about/advisory-board/

Major Supporters

2024 Grant Funders

Reset Tech Action
Craig Newmark Philanthropies
Rose Foundation
Heising-Simons Foundation
Ford Foundation
Robert Wood Johnson Foundation
Spyware Accountability Initiative

Major Donations & Donor Advised Funds

Minneapolis Foundation
Sustainable Solutions Foundation
Franklin Conklin Foundations
Felder Trust Benefit
James Balsillie
Anonymous

Court Issued Awards in Privacy Cases (Cy Pres)

Krakauer v. Dish Network
Komins v. Yonamine
Serrano v. Open Road Delivery Holdings, Inc.
Boger v. Citrix Systems, Inc.
Vaccaro v. Delta Drugs & Vaccaro v. SuperCare
In re: Google Inc. Street View Electronic Communications Litigation

How You Can Defend Privacy

EPIC needs your support. If you would like to support EPIC, contributions are welcome and fully tax-deductible. Learn how to donate to EPIC online or by check at https://epic.org/donate-to-epic/. Additional information about EPIC's work is provided by the GuideStar Database at www.guidestar.org. A complete Form 990 for the current year is also available online.

Financials

Statement of Activities

	2022	2023	2024
Support and Revenue			
Grants and Contributions	$1,003,857	$3,066,401	$1,573,623
Awards	$1,485,127	$594,511	$1,373,212
Program Services Fees	-	$55,000	$22,373
Other Income	-	-	$12,578
Publications	$1,362	$597	$164
Interest Income	$36,735	$59,972	$53,669
Total Support and Revenue	$2,527,081	$3,77,481	$3,035,619
Expenses			
Program	$2,399,626	$2,743,783	$2,864,119
Administration	$179,962	$269,687	$226,582
Fundraising	$327,994	$297,247	$227,436
Total Expenses	$2,907,582	$3,310,717	$3,368,137
Change in Net Assets	($598,181)	$560,526	($355,718)
Net Assets, Jan. 1	$4,609,081	$4,010,900	$4,571,426
Net Assets, Dec. 31	$4,010,900	$4,571,426	$4,215,708

Based on report compiled by Councilor, Buchanan & Mitchell, P.C., Bethesda, MD