

**EFF**

**2023**

**Annual Report**

# Contents

<b>EXECUTIVE DIRECTOR'S MESSAGE</b>	<b>4</b>
<b>ISSUE AREAS</b>	<b>6</b>
<b>2023 BY THE NUMBERS</b>	<b>8</b>
<b>2023 HIGHLIGHTS</b>	<b>9</b>
<b>Free Speech Online</b>	<b>9</b>
Red Flag Machine: How GoGuardian Invades Student Privacy	9
The Internet Dodges Censorship by the Supreme Court	10
EFF to D.C. Circuit: Animal Rights Activists Shouldn't Be Censored on Government Social Media Pages	11
<b>Digital Privacy</b>	<b>12</b>
Privacy First: A Better Way to Address Online Harms	12
California Department of Justice Declares Out-of-State Sharing of License Plate Data Unlawful	14
Mapping the Growing Surveillance Tower Program at the U.S.-Mexico Border	15
<b>Creativity and Innovation</b>	<b>16</b>
Saving the News from Big Tech	16
California Makes Strides for Digital Rights	17
Decentralization	18
<b>Transparency</b>	<b>19</b>
EFF Frees the Law with Public.Resource.org	19
Ninth Circuit Allows Human Rights Case to Move Forward Against Cisco Systems	20
Win for Government Transparency and Immigrant Privacy Rights at Second Circuit	21

Police Must Give Defendant the Face Recognition Algorithms Used to Identify Him .....	22
<b>International.....</b>	<b>23</b>
Decoding the U.N. Cybercrime Treaty.....	23
Settled Human Rights Standards as Building Blocks for Platform Accountability and Regulation (Brazil).....	24
<b>Security .....</b>	<b>25</b>
Kids' Tablet Preloaded with Malware and Sketchyware .....	25
Apple and Google Collaborate on Detecting Unwanted Location Trackers .....	26
Tor University Challenge .....	27
<b>Ongoing Work.....</b>	<b>28</b>
Grassroots Organizing and the Electronic Frontier Alliance .....	28
Press and Investigations .....	29
Public Interest Technologies.....	30
Privacy Badger .....	30
Surveillance Self-Defense Guide .....	30
Certbot and Sunsetting HTTPS Everywhere .....	31
Coded Resistance, the Comic! .....	31
Impact Litigation.....	32
<b>FINANCIAL REPORT .....</b>	<b>35</b>
<b>CHIEF DEVELOPMENT OFFICER'S MESSAGE .....</b>	<b>39</b>
<b>THANK YOU .....</b>	<b>40</b>

# Executive Director's Message



2023 saw EFF doing what it does best—fighting in the courts, in the legislatures, and in the online public squares for your digital rights, all while expanding tools that help protect you online. With the generous support of our members, we have been able to rise to the occasion and win some long-standing battles.

The longest running fight we won in 2023 was to free the law: In our legal representation of PublicResource.org, we successfully ensured that copyright law does not block you from finding, reading and sharing laws, regulations and building codes online. We also won a major victory in helping to pass a law in California to increase tech users' ability to control their information. In several states across the nation, we helped boost the right to repair. All the while, EFF

garnered broad public acclaim and grew our community of Electronic Frontier Alliance groups. EFF also collaborated with incredible local organizations around the world for digital rights advocacy, including publishing a report on eight years of tracking internet service providers' responses to surveillance in Latin America and Spain. And, of course, we continued to encrypt the web and to expand Privacy Badger, giving users additional tools to protect themselves from many kinds of online tracking.

And that's just barely scratching the surface.

At over 100 staffers strong, with a mix of lawyers, technologists, activists, and investigators, EFF covers an impressive range of issues online. Our team's depth of knowledge and experience working for digital freedom remains unmatched. That's because we have worked for decades to support the vast intersection of people and organizations that recognize how important it is to fight for all users.

Tech law and policy were a staple of the public's attention in 2023. Major headlines pondered the future of internet freedom, and the issues often dominated in U.S. Congress, in state legislatures, in the U.S. Supreme Court, and in the European Union. EFF's role as the oldest, largest, and most trusted digital rights organization, with a deep understanding of how technology works, became even more important. All too often we found ourselves combatting deeply

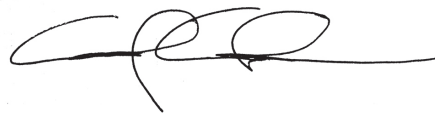


flawed censorship-based proposals that arose from concerns about the harms of our increasingly centralized and surveilled world online. From attacks on Section 230 of the Communications Decency Act, to concerns about child safety, to the damage inflicted upon journalism and small media due to the dominance of the tech giants, we knew that these strategies would not survive constitutional review in the courts. But equally importantly, we knew that these ill-advised schemes would be counterproductive, if not outright dangerous for the very people they were designed to help. And we knew that they would strike marginalized groups hardest.

We responded by continually pointing out a better way to address most of these harms: by protecting Privacy First. We advocated for this, and published a white paper demonstrating how these seemingly disparate concerns are in fact linked to the dominance of the tech giants and the surveillance business models used by most of them. We noted how these business models also feed law enforcement's increasing hunger for our data. We pushed for a comprehensive approach to privacy instead and showed how this would protect us all more effectively than harmful censorship strategies. This highlights how EFF intervenes with logic and leadership when bad ideas get traction, and how we articulate solutions to legitimate concerns with care and nuance.

We couldn't do any of this without the support of our members, large and small. I know that for many, EFF isn't just another organization: Supporting EFF is a putting a marker down on the side of a better, more humane, and more just digital world. We will continue to do our best to help build that future together.

Sincerely,

A handwritten signature in dark ink, appearing to read 'Cindy Cohn', with a stylized, flowing script.

Cindy Cohn, Executive Director

# Issue Areas

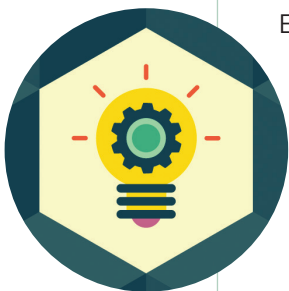


## Free Speech Online

EFF fights for free expression enabled by technology—overcoming the legal, structural, and corporate obstacles blocking people around the world from speaking their minds and accessing information and ideas. People should be able to use new technologies to share their ideas; criticize those in power; gather and report the news; and make, adapt, and share creative works. These rights are especially important for those in vulnerable communities, who must be able to safely meet, grow, and make themselves heard without being silenced or drowned out by the powerful.

## Digital Privacy

We all deserve a life free from prying eyes, and we know that a more private internet is also a more secure internet. Too many of today's technologies are undergirded by business models that facilitate and promote unparalleled invasions of privacy and reductions in security for all of us. EFF works to pass strong national and international laws that will provide comprehensive privacy against both corporate and law enforcement encroachments, and we fight bad or misguided attempts both in the legislature and in the courts. Ensuring an internet that centers users' rights requires respect for individuals' autonomy, anonymous speech, and the right to free association.



## Creativity and Innovation

EFF works to protect and strengthen fair use, innovation, open access, net neutrality, and your freedom to tinker. Our digital future depends on our ability to access, use, and build on information and technology. We challenge patent and copyright trolls in public and in court; argue in Congress for more balanced copyright and patent laws; and urge governments, funders, and educational institutions to adopt open access policies so established players do not silence the next generation of creators.

## Transparency

EFF holds governments accountable to the public through federal and state freedom of information laws, the courtroom, and the bully pulpit of our blogs, podcast, and social media. We showcase technologies and policies that help the transparency process, such as tools that make it easier to file and track public records requests, websites dedicated to whistleblowing, or open-government initiatives to improve access to information.



## International

EFF's international team advocates for privacy, free speech, and an open internet around the world. We expose mass and unwarranted surveillance and educate unlawfully targeted users on how to protect themselves and their colleagues. EFF uses individual cases to highlight the effect of technology on human rights and defend technologists from persecution and detention wherever they live.

## Security

Computer security—and the lack of it—is a fundamental issue that underpins much of how the internet does and doesn't function and is deeply intertwined with privacy. EFF works on a wide range of security issues, including defending encryption use both in the U.S. and internationally; deploying cryptographic protocols, like HTTPS Everywhere and Certbot; offering legal assistance to researchers through our Coders' Rights Project; delivering practical security advice to activists through the Surveillance Self-Defense project; directly auditing open-source codebases; and working on the development of new security standards.



## 2023 by the Numbers

**19**

Legal and  
Legislative  
Victories

**394,400**

Total *How to  
Fix the Internet*  
podcast  
downloads

**3+**

**MILLION**  
Active Privacy  
Badger users

**18**

Amicus  
Briefs Filed

**100+**  
**MILLION**

Certbot-issued  
certificates

**9.3**  
**MILLION**

EFF.org unique  
pageviews

**88**

countries with  
EFF donors

**12,090**

Atlas of  
Surveillance  
entries

**84**

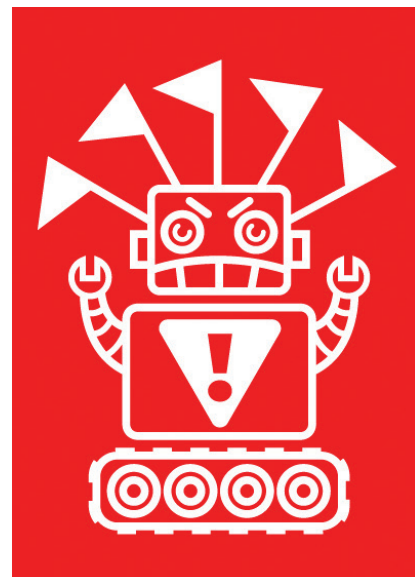
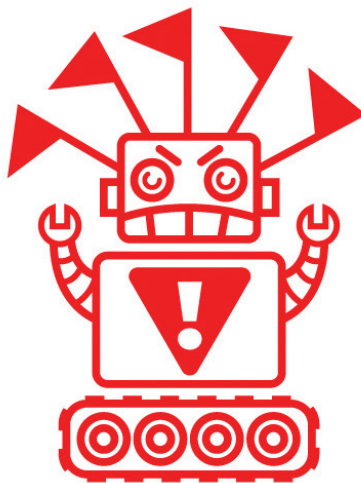
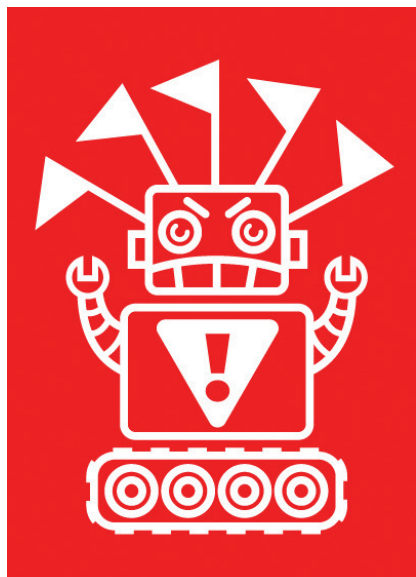
Press Mentions  
per day

**390**

Border Towers  
identified

# 2023 Highlights

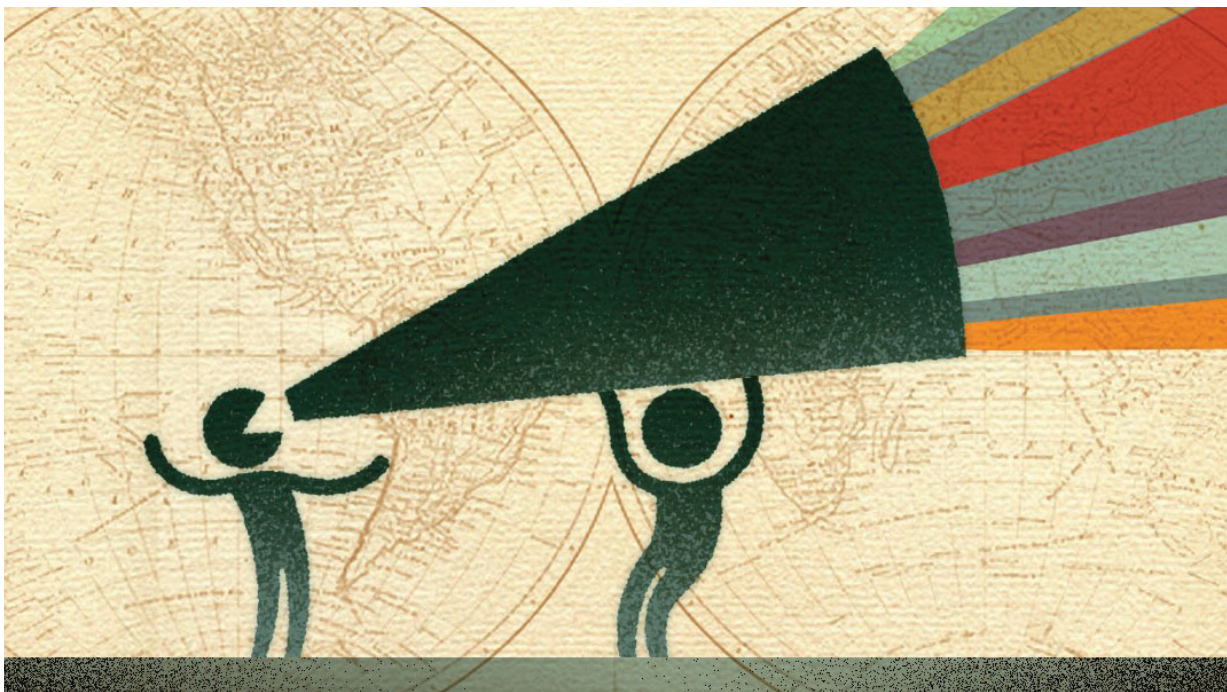
## FREE SPEECH ONLINE



### Red Flag Machine: How GoGuardian Invades Student Privacy

GoGuardian is a student monitoring tool that watches more than 27 million students across 10,000 U.S. schools, but what it does exactly, and how well it works, isn't easy for students or the public to know. To learn more about its functionality, accuracy, and impact on students, EFF filed dozens of public records requests and analyzed tens of thousands of results from the software. We published our findings in "GoGuardian: A Red Flag Machine by Design." Using data from multiple schools in districts located in states across the political spectrum, we uncovered that GoGuardian's high rate of false positives outweighs its ability to

accurately determine whether the content of a website is harmful: Tens of thousands of students were flagged for viewing content that is not only benign, but often educational or informative. Students primarily used the internet to do research for their homework, play games, and watch music videos. They indulged their curiosity, explored their identities, searched for part-time jobs, applied to colleges, and shopped for prom dresses; meanwhile, attempts to access explicit materials were relatively rare. To illustrate the shocking absurdity of GoGuardian's flagging algorithm, EFF created an interactive Red Flag Machine quiz available on EFF.org. Derived from real GoGuardian data, visitors are presented with websites that were flagged and asked to guess what keywords triggered the alert.



## The Internet Dodges Censorship by the Supreme Court

For more than 25 years, Section 230—part of the Communications Decency Act of 1996—has protected small blogs and websites, big platforms, and individual users alike. “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” These “26 words that created the internet” have repeatedly come under fire from opponents to free speech, but with its decisions in *Gonzalez v. Google* and *Twitter v. Taamneh*—for which EFF authored amicus briefs—the U.S. Supreme Court did not weaken Section 230.

In *Gonzalez*, the Supreme Court protected Section 230 by avoiding interpreting it in its decision. The Court ruled that the plaintiffs

failed to establish that YouTube could be held liable for aiding and abetting ISIS members and supporters under the Justice Against Sponsors of Terrorism Act simply because they generally provided services that those organizations used. The Supreme Court’s *Taamneh* decision was also good news, ensuring that internet users can speak about and have access to information about controversial topics, including speech about terrorism. Although the Court’s opinion rests on historical understandings of the legal concept of aiding and abetting liability, the upshot is that online platforms are generally not culpable for having a service open to users that some people used to engage in illegal acts. Both decisions are great news for a free and vibrant internet. Section 230 is an essential part of the legal architecture that enables everyone to connect, share ideas, and advocate for change without needing immense resources or technical expertise.





### **EFF to D.C. Circuit: Animal Rights Activists Shouldn't Be Censored on Government Social Media Pages**

First Amendment case law makes it clear that when a government agency opens a forum for public participation, such as the interactive spaces of the agency's social media pages, it is prohibited from censoring a particular viewpoint in that forum. EFF and the Foundation for Individual Rights and Expression filed a brief in

support of People for the Ethical Treatment of Animals in the U.S. Court of Appeals for the D.C. Circuit in a suit against the National Institutes of Health for blocking their comments against animal testing in scientific research on the agency's Facebook and Instagram pages. EFF argued that any speech restrictions that a government agency applies must be viewpoint-neutral, meaning that the restrictions should apply equally to all viewpoints related to a topic, not just to the viewpoint that the agency disagrees with.

## DIGITAL PRIVACY



### Privacy First: A Better Way to Address Online Harms

Many of the internet's ills have one thing in common: They grow out of the business model of widespread corporate surveillance online. EFF published a report, "Privacy First: A Better Way to Address Online Harms," which outlines our solutions to dismantling this system and explains how doing so will help with harms that, on their face, seem very far afield from privacy. Every year, we encounter ill-conceived bills at the state, federal, and international levels aimed at addressing a wide range of digital topics, such as child safety or artificial intelligence. These scattershot proposals often are rooted in censorship and designed mostly to play to the latest headlines. Instead of this chaotic approach, EFF advocates for a strong, comprehensive data privacy law

that would promote privacy, free expression, and security. Our recommendations include:

- **No online behavioral ads.** Companies must be prohibited from targeting ads to a person based on their online behavior.
- **Real minimization.** Companies must be prohibited from processing a person's data, except as strictly necessary to provide 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 right to access their data, to port it between platforms, to correct it, and to delete it.



- **No preemption by a federal law.** 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 corporations that violate their statutory privacy rights.
  - **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.
  - **No deceptive design.** Companies must be prohibited from presenting people with user interfaces that have the intent or substantial effect of impairing autonomy and choice, sometimes called "dark patterns."
- Our approach supports journalism, protects access to health care, fosters digital justice, limits private data collection to train generative AI, limits foreign government surveillance, and strengthens competition. Comprehensive privacy legislation won't fix everything, but with this one big step, we can take a bite out of the online harms that threaten us all, and foster a more humane, user-friendly technological future for everyone.



**“Legislating to protect a specific set of vulnerable people is no substitute for comprehensive reform that protects all vulnerable people. Left unchecked, data privacy abuses affecting us all will grow more numerous and onerous, and disproportionate impacts upon the marginalized will widen. Without a strong comprehensive data privacy law, America simply can’t have ‘liberty and justice for all.’”**

– from “Digital Privacy Legislation is Civil Rights Legislation” by EFF Senior Speech and Privacy Activist Paige Collings and Privacy Litigation Director Adam Schwartz, published April 10, 2023 by Just Security



## California Department of Justice Declares Out-of-State Sharing of License Plate Data Unlawful

In an important victory for California immigrants, abortion seekers, protesters, and everyone else who drives a car, California Attorney General Rob Bonta issued a legal interpretation and guidance for law enforcement agencies around the state underscoring that it is illegal for police to share data from automated license plate readers (ALPRs) with out-of-state or federal agencies. Bonta acted after EFF, the American Civil Liberties Union of Northern California, and the American Civil Liberties Union of Southern California sent letters to 71 California police agencies in 22 counties demanding that they stop such data sharing. Not only did this practice violate the California Civil Code (S.B. 34), which plainly prohibits such sharing, but it also

undermined California's extensive efforts to protect reproductive health privacy through A.B. 1242, a law prohibiting state and local agencies from providing abortion-related information to out-of-state agencies. In our letters, we wrote, "Law enforcement officers in anti-abortion jurisdictions who receive the locations of drivers collected by California-based ALPRs may seek to use that information to monitor abortion clinics and the vehicles seen around them and closely track the movements of abortion seekers and providers. This threatens even those obtaining or providing abortions in California, since several anti-abortion states plan to criminalize and prosecute those who seek or assist in out-of-state abortions." Every California police agency now must follow Bonta's guidance, review their data sharing, and cut off every out-of-state and federal agency—a huge win for reproductive privacy.

**“(EFF) has sent Sacramento Sheriff Jim Cooper a request that the Sheriff’s Office stop sharing license plate data with police of state agencies elsewhere who could try to use it in the prosecution of women coming to California seeking an abortion. We applaud that effort, both because the sharing is not right, and because it’s against the law.”**

*– from “Stop sharing out-of-state plates data” by the Southern California News Group editorial board, published July 21, 2023*



## Mapping the Growing Surveillance Tower Program at the U.S.-Mexico Border

EFF continued our work documenting the wide range of surveillance technologies being rapidly deployed along the U.S.-Mexico border, emphasizing the impacts on civil liberties and human rights of people living, working, or visiting the region. We met with residents, activists, humanitarian organizations, law enforcement officials, and journalists whose work is directly impacted by the expansion of surveillance technology in their communities. EFF released a

new map and dataset of more than 390 surveillance towers installed by Customs and Border Protection along the border with Mexico. Compiled using public records, satellite imagery, road trips, and even exploration in virtual reality, EFF’s data serves as a living snapshot of the virtual wall, from the California coast to the lower tip of Texas. We also included locations of proposed new towers and automated license plate readers placed at Border Patrol checkpoints. EFF’s mapping project provides invaluable information for researchers and civil society organizations working to defend human rights and hold governments accountable.

## CREATIVITY AND INNOVATION



### Saving the News from Big Tech

We published “Saving the News from Big Tech,” an investigation into anti-competitive practices that threaten an independent press, offering actionable solutions to save and improve journalism.

The default solutions proposed by media conglomerates— fees for linking and similar measures—are not the answer. EFF offers four solutions that will do as much for independent journalists and local outlets as it will for giant companies:

- Break up the ad-tech sector: Ad buyers need more options than just Google

and Meta, and giant platforms like these shouldn’t represent both buyers and sellers in the advertising marketplace.

- Pass a comprehensive privacy law that would ban surveillance advertising and allow for more context-based advertising.
- Open up app stores, eliminating the Apple-Google duopoly.
- Bring the principle of end-to-end—the idea that intermediaries should make the best effort to deliver data from willing senders to willing recipients—to social media and webmail.



## California Makes Strides for Digital Rights

California often sets the bar for technology legislation across the country, and the state enacted several laws in 2023 that strengthen consumer digital rights.

EFF was proud to support S.B. 362, the California Delete Act, which makes it easier for people to exert greater control over their digital privacy. The law, which will take effect in 2026, will require data brokers to report more information about what data they collect on consumers. It also strengthens enforcement mechanisms against data brokers who fail to comply with the reporting requirement. Overcoming serious pushback from advertisers, this law prevailed as an important,

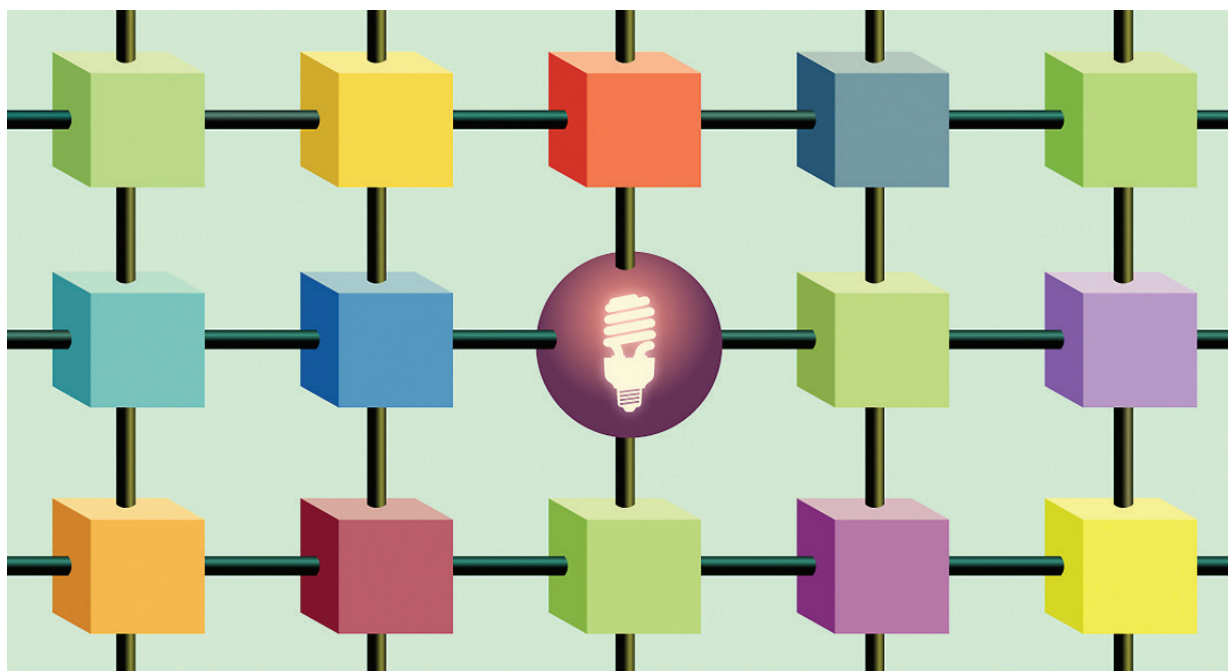
common-sense measure that makes it easier to exercise rights established by the California Consumer Privacy Act of 2018.

Californians now enjoy the right to repair: S.B. 244 makes it easier for individuals and independent repair shops to access materials and parts needed for maintenance on electronics and appliances. California's law differs from other right-to-repair laws in a few ways: For one, by building on categories set in the state's warranty laws, S.B. 244 establishes that you'll be able to get documentation, tools, and parts for devices for three years for products costing between \$50 and \$99.99, or for seven years for products costing \$100 or more. Although some electronics such as video game consoles are not included, the law still raises the bar



for other right-to-repair bills. It's one of the country's strongest, and caps off several strong years of progress on this issue thanks to a dedicated coalition led by the California Public Interest Research Group. EFF lobbied lawmakers, raised public awareness through

blog posts and actions, and participated in a press event demonstrating how much e-waste the bill would reduce. This is a huge victory for consumers, and we're excited to keep pushing to ensure that people have the freedom to tinker.

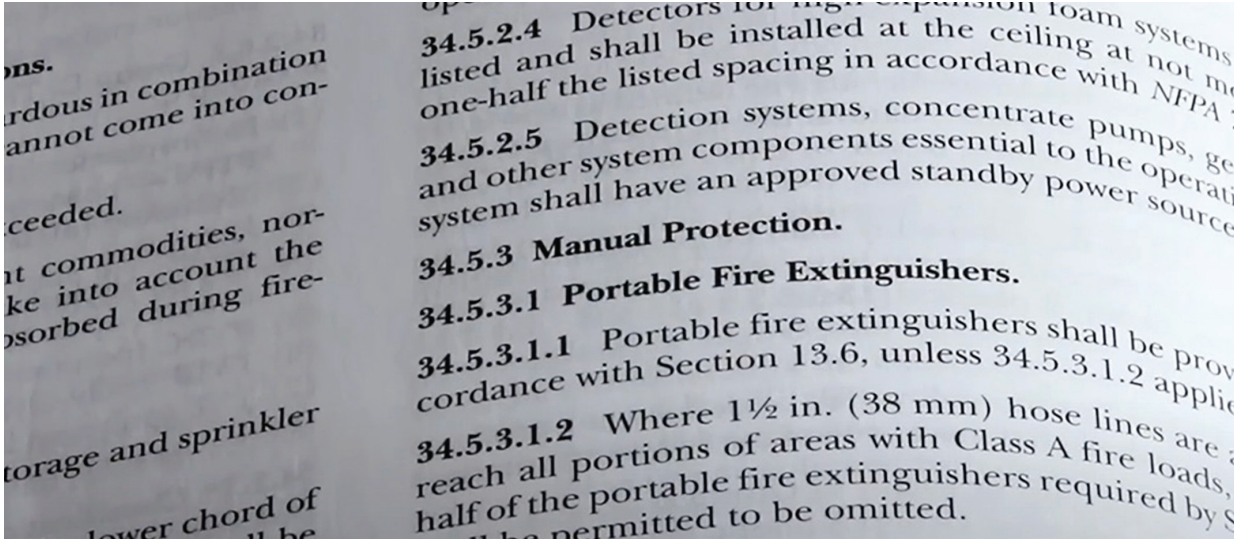


## Decentralization

Fed up with the concentration of power, violations of privacy, and threats to free expression, many users are fleeing to smaller, independently operated projects and platforms. EFF believes that a decentralized internet is a vital component of achieving our mission to ensure that technology supports freedom, justice, and innovation for all people of the world. EFF was invited to testify in June 2023 before the U.S. House Energy and Commerce Committee Subcommittee on Innovation,

Data, and Commerce. We welcomed this as an opportunity to highlight non-financial uses of decentralized blockchain technology. EFF spoke in favor of the technologies, cutting through the noise to help members of Congress understand what blockchain is outside of a financial context, how and when it can be helpful, and provide clarity on its potential downsides. In our testimony, we also reiterated that people who simply contribute open-source code to blockchain projects should not be held responsible for what others do with the code they write, absent some other factor.

## TRANSPARENCY



### EFF Frees the Law with Public.Resource.org

The decision by a three-judge panel of the U.S. Court of Appeals for the District of Columbia Circuit upholds the idea that we should be able to find, read, and share the text of laws free of registration requirements, fees, and other roadblocks. It's a long-awaited victory for EFF's client Public.Resource.org, a non-profit organization founded in 2007 to make "government information more accessible." As part of its mission of promoting public access to all kinds of government information, Public Resource acquires and posts online a wide variety of public documents, including standards incorporated into law by reference. These standards include electrical, fire safety, and consumer safety codes mandated by governments, but written by nongovernmental entities like The American Society for Testing and Materials (ASTM), National Fire Protection Association Inc. (NFPA), and

American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE). ASTM, NFPA, and ASHRAE sued Public Resource in 2013 for copyright and trademark infringement and unfair competition. Regulators at all levels of government frequently incorporate these codes and standards into regulations, making them law, but they are often difficult even to access, much less to share with others, obscuring from view areas of law that profoundly affect our daily life. Even courts have had trouble accessing the laws that they are supposed to apply. The internet lets more people understand and participate in government than ever before—that's why Public Resource's work, and this victory that protects access to law and participation in government, are so important. Standards like fire and electrical codes developed by private organizations but incorporated into public law can now be freely disseminated without any liability for copyright infringement.

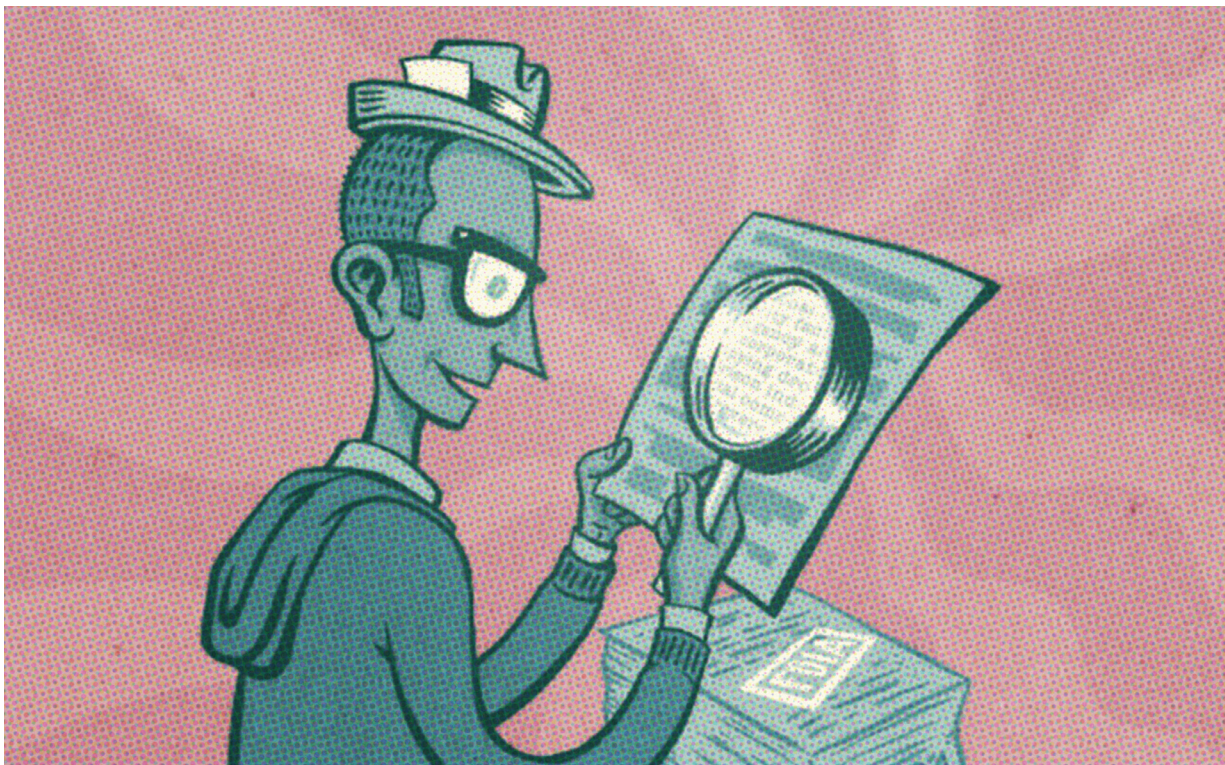


## **Ninth Circuit Allows Human Rights Case to Move Forward Against Cisco Systems**

People around the world have searched for ways to hold companies accountable for building tools used for government repression, ranging from massive surveillance systems to state-sponsored malware. Such technology too often is used to locate, track, and abuse members of vulnerable communities, journalists, and activists. The U.S. Court of Appeals for the Ninth Circuit cleared a path of legal accountability for American technology companies that facilitate human rights abuses by foreign governments. In a victory for the victims of this oppression, the court allowed victims

to sue tech giant Cisco Systems in a long-running case seeking redress for the company's role in building and deploying the "Golden Shield," also referred to as "The Great Firewall of China." It's a vast surveillance system that Cisco began building in the late 1990s and that the Chinese government used to violate the human rights of disfavored minorities, including members of the Falun Gong religion, who are the plaintiffs in the case. EFF filed multiple amicus briefs in the case, and we applaud the Ninth Circuit appeals court in helping ensure that the key statute in the case—the Alien Tort Statute—remains an important mechanism for holding companies accountable when they choose profit over human lives.

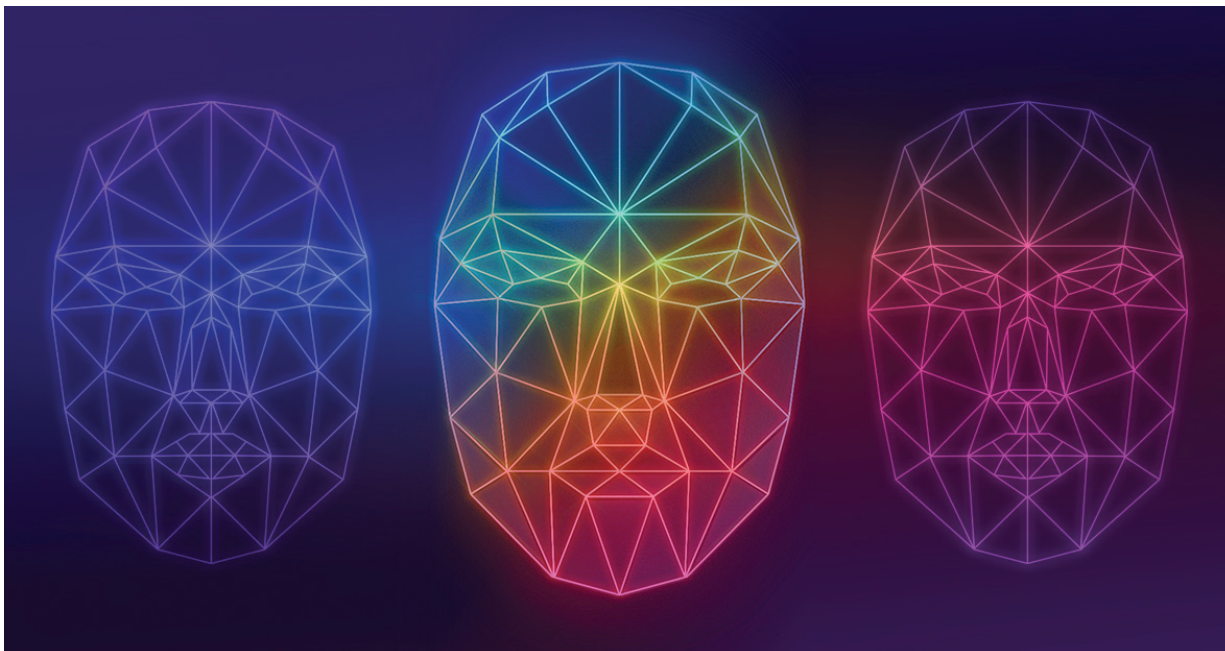




## Win for Government Transparency and Immigrant Privacy Rights at Second Circuit

In a victory for the rights of immigrants and for government transparency, the U.S. Court of Appeals for the Second Circuit held that U.S. Immigration and Customs Enforcement (ICE) must be transparent and respect privacy by producing deidentified data on how it arrests, classifies, detains, and deports immigrants in response to Freedom of Information Act (FOIA) requests. The court agreed with plaintiff American Civil Liberties Union (ACLU) that ICE must also replace Alien Identification Numbers (which would identify individual immigrants) with unique but random identifiers.

The court cited the EFF amicus brief's many examples of other courts ordering the government to use "anonymization techniques," including unique identifiers, blurring faces in videos, and scrambling identifying data. The Second Circuit also cited and agreed with EFF's amicus brief that the E-FOIA Amendments required ICE to substitute unique identifiers because that is the "form or format" ACLU requested and it is "readily reproducible." The court explained that Congress "expected agencies to take reasonable steps to effect retrieval in the requested form or format, even if that required some conversion of data." As government agencies increasingly use digital tools to track citizens and immigrants, we need to use the FOIA to make that surveillance transparent. But while the government opens its databases to public scrutiny, it must also protect individual privacy.



## Police Must Give Defendant the Face Recognition Algorithms Used to Identify Him

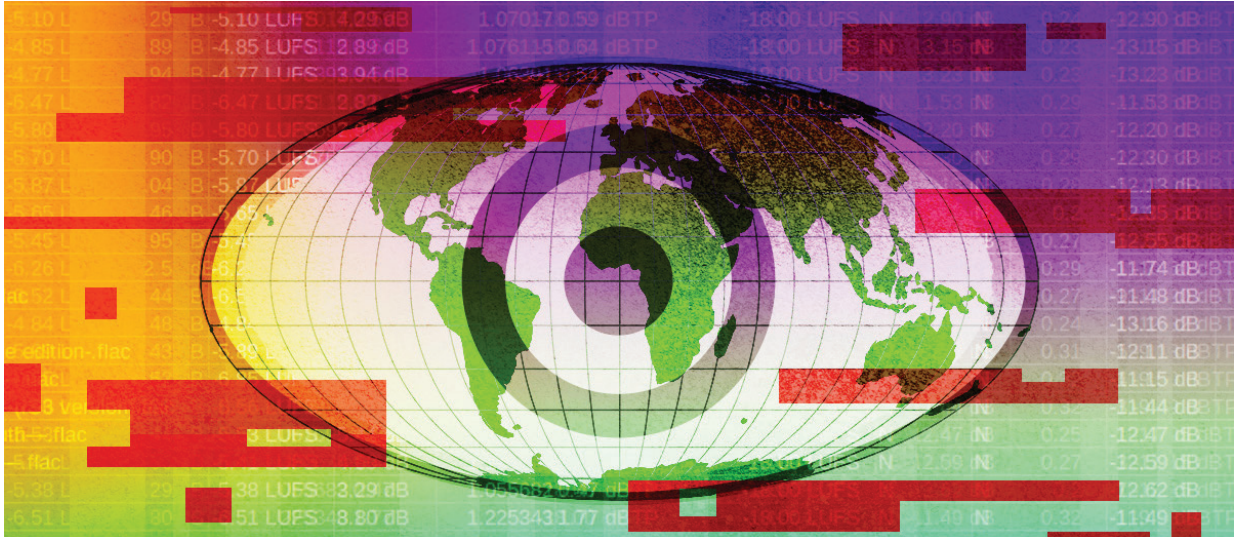
In a victory for transparency in police use of face recognition, a New Jersey appellate court ruled that state prosecutors—who charged a man for armed robbery after the technology showed he was a “possible match” for the suspect—must turn over detailed information about the face scanning software used, including how it works, its source code, and its error rate. EFF, along with Electronic Privacy Information Center and the National Association of Criminal Defense Lawyers, filed an amicus brief on behalf of the defendant, arguing that the court should allow robust discovery regarding law enforcement’s use of face recognition technology.

Study after study shows that face recognition algorithms are not always reliable, and that

error rates spike significantly when involving faces of people of color—especially Black women—as well as trans and nonbinary people. But despite heightened inaccuracy for members of vulnerable communities often targeted by the police, law enforcement has widely adopted and used this unreliable tool to identify suspects in criminal investigations. Calling face recognition “a novel and untested technology,” the appeals court in *State of New Jersey v. Francisco Arteaga* held that the defendant would be deprived of due process rights unless he could access the raw materials police used to identify him and test its reliability to build a defense. The inner workings of the face recognition software are vital to impeach witnesses’ identification of him, challenge the state’s investigation, and create reasonable doubt, the court said. The ruling is a clear win for justice, fairness, and transparency.



## INTERNATIONAL



### Decoding the U.N. Cybercrime Treaty

EFF was at the forefront of civil society input on the proposed U.N. Cybercrime Convention, which could shatter security, and harm political and social activists, journalists, security researchers, whistleblowers, and millions more around the world for decades to come. EFF attended draft negotiation sessions alongside our coalition partners, providing context-based analysis in our communications and presenting on panels at cybersecurity conferences. The draft treaty could rewrite criminal laws worldwide, adding over 30 criminal offenses and expansive police powers for domestic and international criminal investigations. These widened parameters have grave implications for billions of people—particularly the potential for stifling free speech, increasing government surveillance, and expanding state investigative techniques. Security and encryption researchers

help build a safer future for all of us using digital technologies, but too many legitimate researchers face serious legal challenges under this treaty that would inhibit their work or prevent it entirely.

“Who Defends Your Data in Latin America and Spain?” Eight Years Holding Internet Service Providers to Account for User Privacy Latin American and Spanish telecommunications companies have made important advances in their privacy policies and practices, but persistent gaps and worrying trends pose potential risks for internet and mobile phone users. EFF published “Who Defends Your Data in Latin America and Spain?” comparing the performance of regional and/or global telecom companies in 10 countries; revealing problematic trends and challenges in the region vis-à-vis the much-needed application of human rights standards to government access to data; and exploring companies’ advances

and weaknesses in data protection frameworks. Our report is comprised of series of reports by local digital rights organizations in Argentina, Brazil, Chile, Colombia, México, Nicaragua, Panamá, Paraguay, Perú, and Spain that evaluated telecommunications companies' commitments to transparency and user privacy. "Who Defends Your Data in

Latin America and Spain?" outlines the main findings of our partners' studies through a broad regional lens and includes recommendations for companies and countries to tackle both ongoing and new challenges in Latin America and Spain in the face of warrantless surveillance and weak safeguards for privacy and data protection.



### **Settled Human Rights Standards as Building Blocks for Platform Accountability and Regulation (Brazil)**

EFF and AccessNow published "Settled Human Rights Standards as Building Blocks for Platform Accountability and Regulation: A Contribution to the Brazilian Debate," an in-depth report on platform regulation in Brazil. This included the draft bill known as PL 2630 or the "Fake News Bill" and constitutional cases pending in the country's Supreme Court. The right to seek, receive, and communicate information enables the exercise of other human rights and strengthens the internet ecosystem,

but not without backlashes and critical challenges. Proper responses are not simple to craft, but we argued that any proposed speech restrictions must follow the "three-part test"—they must be clearly set by law, strictly necessary, and proportionate to achieve a legitimate aim in a democratic society. Any laws seeking to strengthen users' rights in the face of dominant internet applications must build on these principles and existing human rights safeguards. Empowering users before dominant internet platforms' huge corporate power also involves more structural and economic measures that are mainly missing from the current debate, such as fostering interoperability of social networks.

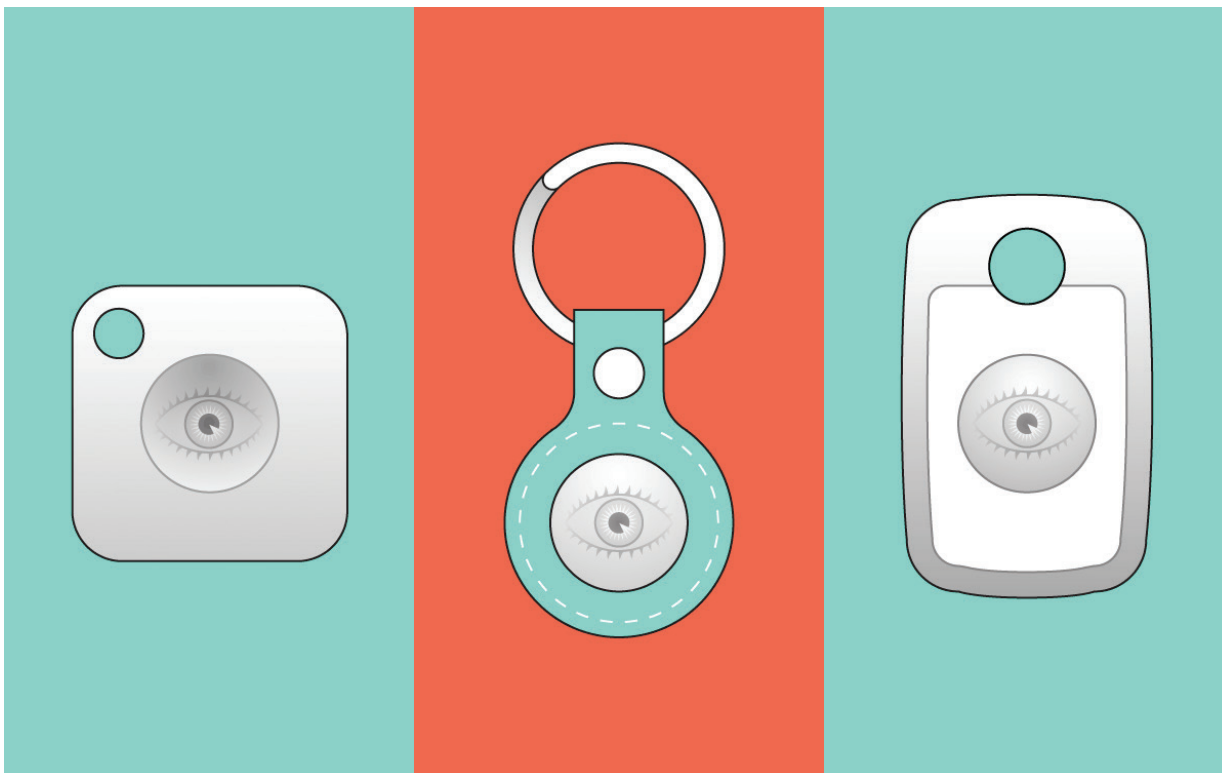
## SECURITY



### Kids' Tablet Preloaded with Malware and Sketchyware

Better digital product testing along with regulatory oversight can go a long way in mitigating new risks to our security and privacy posed by the influx of “smart” and IOT devices into our everyday lives. EFF technologists found that Dragon Touch KidzPad Y88X 10, a kid’s Android tablet sold on Amazon, came preloaded with malware. For example, KIDOZ and other apps on the tablet collect and send data on usage and the device’s physical attributes to kidoz.net and other domains, including those

belonging to apps that are no longer supported. The versions on the tablet were very out of date, meaning that device-specific information shared over primarily insecure web requests can be targeted by bad actors who want to siphon information either on that device or by obtaining the defunct domains the device is communicating with. EFF published our findings and created an easy guide for parents to help keep their kids’ devices and data safe: “How to Secure Your Kid’s Android Device” provides recommendations on parental monitoring, security, safety, and privacy.

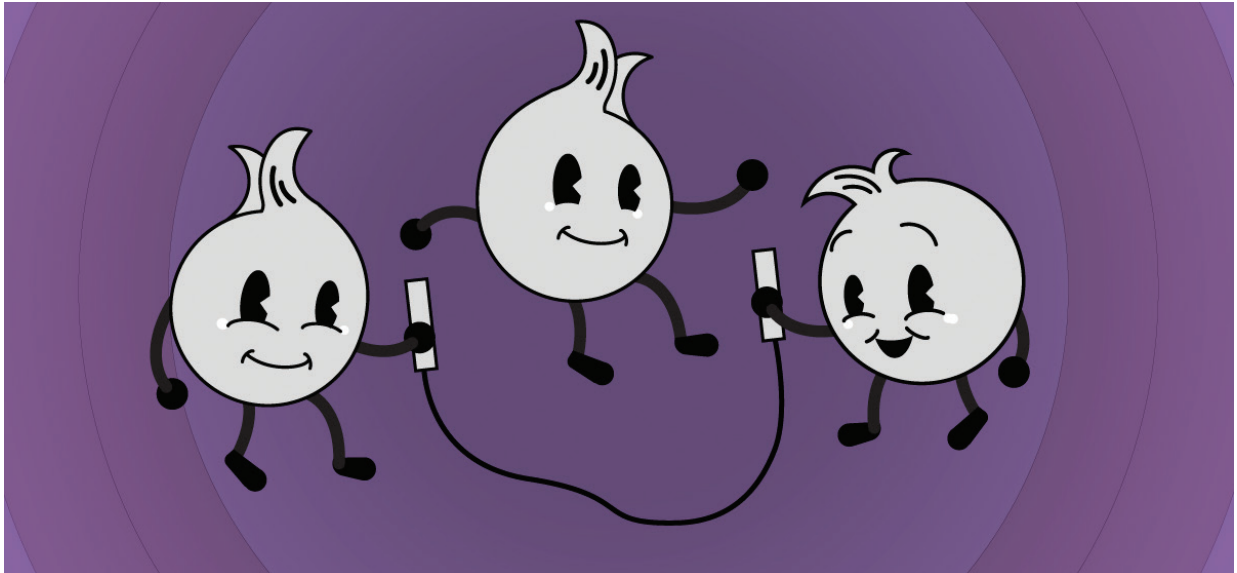


## Apple and Google Collaborate on Detecting Unwanted Location Trackers

Physical location trackers can be easily slipped surreptitiously into a bag or car, giving stalkers and abusers unprecedented access to a person's location without their knowledge. EFF has been sounding the alarm about this threat for years, especially as it pertains to survivors of domestic abuse, and has called for an industry-wide standard for detection of this transient hardware to prevent stalking and other abuse. Such standards would greatly improve the ability of both Android and iPhone devices to

detect unwanted trackers without additional apps. During the 2023 Google I/O Keynote, Google announced that Android will launch Bluetooth tracker detection for devices that may be "following" you without your knowledge. This is a big improvement beyond the subpar Tracker Detect app provided by Apple in response to Android users being susceptible to AirTag tracking without any tools to discover them. This also covers other devices such as Tile's trackers. This was announced in tandem with news that Google's Find My Device network is expanding in ways similar to Apple's Find My network AirTags expansion, but this time with safety measures.





### Tor University Challenge

EFF launched the Tor University Challenge, a campaign urging higher education institutions to support free, anonymous speech by running a Tor network relay. Made up of volunteer-run relays, the Tor network allows human rights defenders and organizations,

at-risk communities, and people experiencing online censorship or government surveillance to browse the unrestricted internet with as much privacy and anonymity as possible. After the challenge's first 4 months, more than 20 institutions worldwide were running relays.



**“Journalists, political and social activists, attorneys, businesspeople, and other users all over the world rely on Tor for unfettered, unmonitored access to knowledge and communications. Anonymous speech always has been a pillar of democratic society, letting us discuss anything without fear of retribution. And facilitating this discussion can be a great educational opportunity for students and faculty alike.”**

*- EFF Staff Technologist Cooper Quintin*

## ONGOING WORK



### Grassroots Organizing and the Electronic Frontier Alliance

Diverse grassroots organizations across the country share strong connections to EFF. We created and continue to support the Electronic Frontier Alliance (EFA), an information-sharing network which has grown to 76 member groups in 26 U.S. states and Puerto Rico. Some member organizations are fully volunteer-run, some are affiliated with a broader institution (such as student groups), and some are independent non-profit organizations. What EFA groups all share is an investment in local organizing, a not-for-profit model, and a passion for five guiding principles:

- **Free Expression:** People should be able to speak their minds to whomever will listen.
- **Security:** Technology should be trustworthy and accountable to its users.
- **Privacy:** Technology should allow private and anonymous speech and let users set their own parameters about what to share with whom.

- **Creativity:** Technology should promote progress by allowing people to build on the ideas, creations, and inventions of others.
- **Access to Knowledge:** Curiosity should be rewarded, not stifled.

EFF's organizing team conducted interviews with some of EFA's most active members. Portland's TA3M—an informal meet-up designed to connect software creators and activists who are interested in issues like censorship, surveillance, and open technology—spoke with EFF about its newly expanded scope including privacy and security. CCTV Cambridge, a longtime member, shared some of their exciting upcoming and ongoing projects like regranteeing American Rescue Plan funds to local artists and creators, and continuing their advocacy for digital equity. Finally, we connected with the New York-based Surveillance Technology Oversight Project (STOP) to learn about their education and advocacy work, and how people from across the country—New Yorkers or not—can plug in and support.





## Press and Investigations

EFF's attorneys, activists, and technologists were tapped for their expertise more than ever in 2023, with an average of 84 press mentions per day globally. Reproductive rights, free speech cases before the U.S. Supreme Court, proposed social media bans, age verification bills in state legislatures, and car privacy made up some of the most important new stories of the year. EFF staff were cited in international, national, and local print publications, as well as on television, radio, and podcasts, including *Scientific American*, *Newsweek*, *Ms. Magazine*, *The Atlantic*, *Slate*, *Salon*, the *San Francisco Chronicle*, *ABC News' Good Morning America*, and many other outlets.

EFF's investigative team also had a banner year. We collaborated with the Thomson Reuters Foundation on an investigation of Fusus, a company offering software that lets police unify multiple surveillance streams (body cams, ShotSpotter, private doorbell cams, and much more) into a single panopticon of mass surveillance. We also fought

the bureaucracy and won records about predictive policing in General Escobedo, Mexico. Working with our peers at MuckRock, our 2023 Foilies highlighted agencies representing the worst in government transparency, from the FBI to the Los Angeles Police Department.

The fourth season of EFF's "How to Fix the Internet" podcast earned a Silver Award in the 3rd Annual Anthem Awards, which honors the purpose and mission-driven work of people, companies and organizations around the world. The podcast's 10 new episodes featured writers, activists, technologists, and even a federal trade commissioner, each joining us for conversations that explored legal and technical concepts with nuance, complexity, and optimism; we averaged about 14,000 downloads per episode. Highlights included "People with Disabilities Are the Original Hackers," with disability policy expert Henry Claypool, "Don't Be Afraid to Poke the Tigers," with researcher and hacker Andrew "bunnie" Huang, and "When Tech Comes to Town," with Catherine Bracy, co-founder and CEO of the Oakland-based TechEquity Collaborative.



## Public Interest Technologies

### Privacy Badger



Privacy Badger is a browser add-on that stops advertisers and other third-party trackers from secretly tracking where you go and what pages you look at on the web. Originally launched in 2014, EFF has continued to maintain and improve the tool, including the release of a new version that updates how we fight “link tracking” across several Google products including documents, email, maps, and images results. Privacy Badger now also removes tracking

from links added after scrolling through Google Search results. Available to the public for free, Privacy Badger was the first add-on to specifically focus on blocking tracking in advertisements, instead of just the ads themselves. EFF’s open-source technology has also inspired other widely used privacy tools, including the Brave browser and Safari’s tracker blocking.

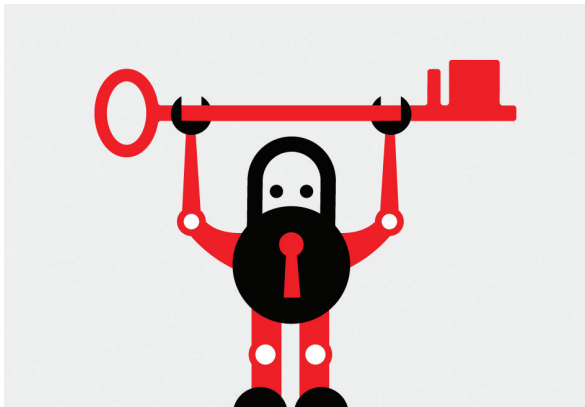
### Surveillance Self-Defense Guide



Created by EFF, this online guide provides vital information on how to use secure technology and develop careful practices.

It includes tutorials for installing and using security-friendly software, and information on making a security plan, strong passwords, protecting metadata, and much more. SSD is available in 12 languages, in whole or in part. We began a major overhaul of the guide in 2023, including 15 updates published by the end of the year; this included a brand-new guide on password managers. Several other guides were merged into one, making them easier to update, translate, and share.

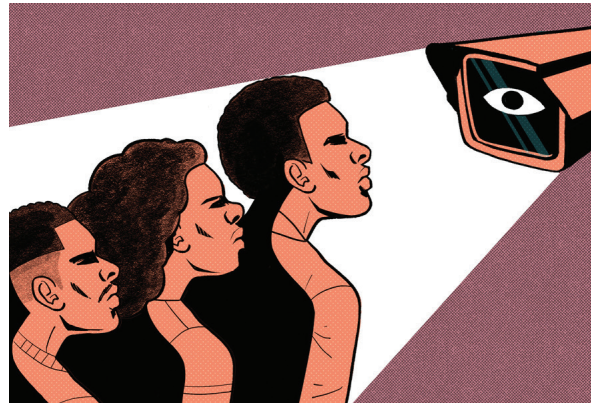
### **Certbot and Sunsetting HTTPS Everywhere**



Certbot—EFF’s free, open-source software tool to help websites encrypt their traffic and keep their sites secure—aims to build a web that is more structurally private, safe, and protected against censorship. Overall, there are 3.3 million Certbot installations maintaining 20 million certificates for 29.6 million domains. At the start of 2023, EFF sunsetted the HTTPS Everywhere web extension, which encrypted browser communications with websites and made sure users benefited from the protection of HTTPS wherever possible. HTTPS Everywhere ended because all major browsers now offer the functionality to

make HTTPS the default. This is due to the grand efforts of the many technologists and advocates involved with Let’s Encrypt, HTTPS Everywhere, and Certbot over the last 10 years. The immense impact of this “Encrypt the Web” initiative has translated into default “security for everybody.”

### **Coded Resistance, the Comic!**



From the days of chattel slavery through the modern Black Lives Matter movement, Black communities have developed innovative ways to fight back against oppression. Alexis Hancock, EFF’s Director of Engineering, documented this important history of codes, ciphers, underground telecommunications and dance in a blog post that became one of our favorite articles of 2021. In collaboration with The Nib and illustrator Chelsea Saunders, we adapted “Coded Resistance” into comic form in 2023 to further explore these stories, from the coded songs of Harriet Tubman to Darnella Frazier recording the murder of George Floyd.



## Impact Litigation

Since its founding in 1990, EFF has consistently taken critical cases, challenged tough opponents, and achieved landmark victories. EFF has prevailed in lawsuits against the federal government, the Federal Communications Commission, the world's largest entertainment companies, and major electronics companies, among others. EFF has also helped defeat bills in Congress and successfully pressured companies to respect your rights.

### *Legal and Legislative Victories*

1. [The Internet Dodges Censorship by the Supreme Court](#) EFF filed an amicus brief (5/18/23) Federal
2. [Fourth Circuit: Individuals Have a First Amendment Right to Livestream Their Own Traffic Stops](#) EFF filed an amicus brief in 2021. (2/23/23) Federal
3. [Victory at the Ninth Circuit: Twitter's Content Moderation is Not "State Action"](#) EFF filed an amicus brief (3/24/23) Federal
4. [In SAS v. WPL, the Federal Circuit Finally Gets Something Right on Computer Copyright](#) (4/10/23) Federal
5. [Federal Appeals Court Gets It: Fair Use Protects Security Research Tools](#) (5/10/23) Federal
6. [Court Rejects Efforts to Identify Anonymous Webhost](#) (7/23/23) Federal
7. [Appeals Court Upholds Public.Resource.Org's Right to Post Public Laws and Regulations Online](#) (9/12/23) Federal
8. [Victory! Montana's Unprecedented TikTok Ban is Unconstitutional](#) EFF filed an amicus brief with ACLU of Montana (12/1/23) Federal

9. [Safeguarding End-to-End Encryption in EU CSAR Compromise](#) (10/23) International
10. [First Appellate Court Finds Geofence Warrant Unconstitutional](#) (4/24/23) State
11. [Don't Mess With Texas' Anti-SLAPP Law](#) (6/1/23) State
12. [Victory in California! Police Instructors Can't Claim Copyright Protections to Block Release of Use-of-Force and Other Training Materials](#) (5/25/23) State
13. [Victory! New Jersey Court Rules Police Must Give Defendant the Facial Recognition Algorithms Used to Identify Him](#) EFF filed an amicus brief with EPIC and NACDL (6/7/23) State
14. [Facebook v. New Jersey](#) EFF filed amicus brief with EPIC, CDT, and Davis Wright Tremaine (6/29/23) State
15. [Maryland Supreme Court: Police Can't Search Digital Data When Users Revoke Consent](#) EFF filed an amicus brief with the National Association of Criminal Defense Lawyers (7/27/23) State
16. [Arizona Broadcasters Association v. Brnovich](#) EFF filed an amicus brief with National Lawyers Guild, Poder in Action, and Mass Liberation AZ (7/21/23) State
17. [California Takes Some Big Steps for Digital Rights](#) (10/13/23) State
18. [VICTORY! California Department of Justice Declares Out-of-State Sharing of License Plate Data Unlawful](#) (10/31/23) State
19. [Victory: Utah Supreme Court Upholds Right to Refuse to Tell Cops Your Passcode](#) EFF filed an amicus brief with ACLU (12/18/23) State

### ***New Lawsuits***

1. [Why We're Suing to Protect the Right of Incarcerated People to Receive Physical Mail](#) (3/13/23) State

### ***Policy Position Highlights***

1. [Government Hasn't Justified a TikTok Ban](#) (3/16/23) Federal
2. [EFF Comments on Privacy and Civil Rights to Telecommunications and Information Administration \(NTIA\)](#) (3/7/23) Federal
3. [AI Art Generators and the Online Image Market](#) (4/3/23) Federal
4. [Enough is Enough. Tell Congress to Ban Federal Use of Face Recognition](#) (4/4/23) Federal
5. [From Past Lessons to Future Protections: EFF's Advice to the EU Commission on Extended Reality Governance](#) (5/22/23) International
6. [Internet Access Shouldn't Be a Bargaining Chip In Geopolitical Battles](#) (10/20/23) International

### ***Amicus Briefs Filed***

1. [EFF Tells Supreme Court: Trademark Law Doesn't Trump the First Amendment](#) (3/7/23) Federal



2. [EFF Urges Supreme Court to Make Clear That Government Officials Have First Amendment Obligations When They Use Their Social Media Accounts for Governmental Purposes \(6/30/23\)](#) Federal
3. [EFF Files Amicus Briefs in Two Important Geofence Search Warrant Cases \(1/31/23\)](#) Federal and State
4. [Courts Must Not Allow Litigants to Plead Around The First Amendment's Speech Protections \(2/3/23\)](#) Federal
5. [EFF Files Amicus Brief to Protect the Speech Rights of Immigrants and Immigrant Rights Advocates \(2/24/23\)](#) Federal
6. [EFF and Student Press Law Center Urge Supreme Court to Require Government to Show Subjective Intent in Threat Cases \(3/2/23\)](#) Federal
7. [Appeals Court Upholds Restriction on Twitter's First Amendment Right to Publish National Security Transparency Report \(3/10/23\)](#) Federal
8. [Court Accepts EFF's Amicus Brief on the Right to Publish Code in Tornado Cash Case \(5/10/23\)](#) Federal
9. [Government Needs Both the Ability to Talk to Social Media Platforms and Clear Limits, EFF Argues in Brief to Appellate Court \(7/28/23\)](#) Federal
10. [EFF to 9th Circuit: App Stores Shouldn't Be Liable for Processing Payments for User Content \(8/4/23\)](#) Federal
11. [EFF Defends Free Speech in PETA v. Tabak \(9/15/23\)](#) Federal
12. [EFF Urges Second Circuit to Affirm Injunction of New York's Dangerous Online "Hateful Conduct" Law \(10/5/23\)](#) Federal
13. [Free Speech Coalition v. Colmenero \(9/26/23\)](#) Federal
14. [EFF to Ninth Circuit: Activists' Personal Information Unconstitutionally Collected by DHS Must Be Expunged \(11/6/23\)](#) Federal
15. [X's Anti-Speech Lawsuit Against Watchdog Center for Countering Digital Hate \(11/27/23\)](#) Federal
16. [Warner Chappell Music v. Nealy re: Statute of Limitations for Copyright Cases \(12/4/23\)](#) Federal
17. [NetChoice v. Griffin re: Free Speech and Proposed Social Media Safety Act \(7/24/23\)](#) State, Arkansas
18. [EFF to Michigan Court: Governments Shouldn't Be Allowed to Use a Drone to Spy on You Without a Warrant \(9/13/23\)](#) State, Michigan

The logo for EFF (Electronic Frontier Foundation) in red, bold, sans-serif capital letters.

**EFF**

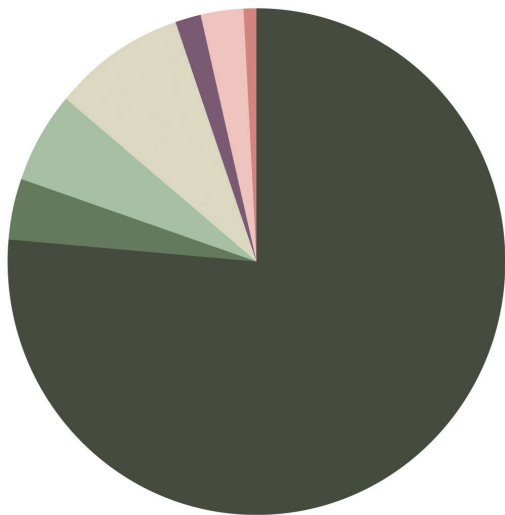
The year 2023 in a large, bold, sans-serif font. The '2' is purple, the '0' is blue, and the '23' is teal.

**2023**

The word Financials in a bold, sans-serif font, colored teal.

**Financials**

# Financial Report

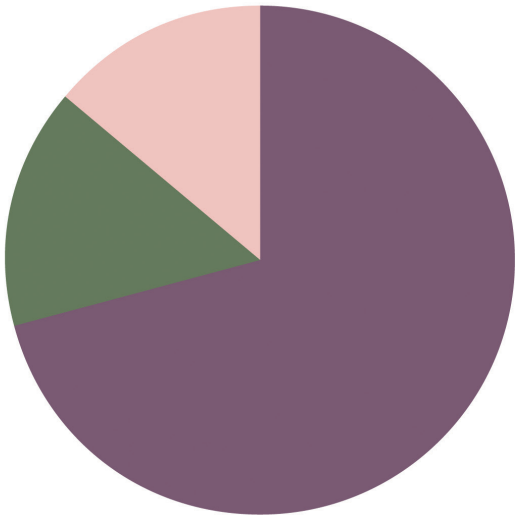


## EFF FY 2022-2023 PUBLIC SUPPORT

Individual	\$13,144,900
Individual through Foundation	684,100
Employee & Customer-Directed Gifts*	988,600
Foundation**	1,509,200
Corporate	256,700
Cy Pres	500,800
In-kind Contributions	118,200
<b>Total Public Support</b>	<b>\$17,202,500</b>
Other Revenue	2,403,900
<b>Total Public Support &amp; Revenue</b>	<b>\$19,606,400</b>

## EFF FY 2022-2023 EXPENSES

Program	\$ 13,604,800
Administrative	2,914,600
Fundraising	2,651,400
<b>Total Expenses</b>	<b>\$19,170,800</b>





## INCOME

### Public Support

Individual Contributions	
Individual Contributions over \$50,000	\$6,211,000
Individual Contributions \$10,000-\$50,000	\$1,127,600
Individual Contributions \$1,000-\$10,000	\$1,536,100
Individual Contributions under \$1,000	\$4,270,200
Total Individual Contributions	\$13,144,900
Individual Contributions through Foundations	
Individual Contributions through Foundations Over \$50,000	\$472,400
Individual Contributions through Foundations Up to \$50,000	\$211,700
Total Individual Contributions through Foundations	\$684,100
Foundation Grants**	\$1,509,200
Cy Pres Awards	
<i>Muransky v Godiva Cy Pres</i>	\$292,100
<i>Pine v. A Place for Mom Cy Pres</i>	\$208,700
Total Cy Pres Awards	\$500,800
Corporate Contributions	
Employee and Customer-Directed Gifts*	\$988,600
Other Corporate Contributions	\$256,700
Total Corporate Contributions	\$1,245,300
In-kind Legal Services	\$118,200
<b>Total Public Support</b>	<b>\$17,202,500</b>

### Revenue

Net Investment Income	\$2,222,400
Attorneys' Fees Awarded	\$35,300
EFF Event Income, net of expenses	\$46,900
Miscellaneous	\$99,300
<b>Total Revenue</b>	<b>\$2,403,900</b>

**Total Support and Revenue** **\$19,606,400**

\*This category includes payments made to match verified employee donations, charity awards chosen by employee groups, and portions of customer purchases designated for charity.

\*\*This category includes newly awarded grant amounts during FY22-23 (accrual basis) and does not include additional funds awarded in prior years but disbursed during this FY.

## EXPENSES

Salaries & Benefits	\$14,928,000
Legal & Professional Fees	\$2,029,800
Membership Expenses	\$466,000
Amortization & Depreciation	\$289,400
Building Expenses	\$263,000
Planning & Development	\$230,500
Office Expenses	\$209,500
Travel Expenses	\$160,500
Furniture & Equipment Expense	\$154,600
Corporate Insurance	\$147,100
Litigation Expenses	\$121,700
Awareness Events	\$85,900
Other Administrative Expenses	\$35,900
Intern Expenses	\$32,400
In Kind Contribution	\$14,700
Fundraising Expenses	\$1,800
<b>Total Expenses</b>	<b>\$19,170,800</b>
<b>Net Income</b>	<b>\$435,600</b>

# Chief Development Officer's Message



Thank you for your support of the Electronic Frontier Foundation. I am proud to not only be the head of EFF's fundraising team, but a member as well. I personally support EFF because I think our democracy and social movements can only survive if we have a fair and free internet.

As a supporter, you have been on the forefront of the digital civil liberties movement, fighting for freedom of speech, privacy, decentralization, and neutrality. Thank you. It is only with supporters like you that we have achieved victories like those described in this report and that we can continue to make sure technology works to support all users.

I love that EFF is member-supported. I love that I am the head of a fundraising team that believes in grassroots giving. We have 30,000 members who give an average gift of around

\$150. It means that we don't have to cater to special interests. From members giving \$5 a month to generous planned giving, we are grateful for the unrestricted funding that EFF's lawyers, activists, and technologists put to the highest and best use.

At a recent meeting, one of my EFF colleagues called our work "the infrastructure of dissent." Whether you are fighting for environmental justice, racial justice, reproductive justice, freedom of speech, smaller government, voting rights, human rights, or your right to a private conversation, EFF has your back. We are fighting to ensure that the internet that is part of our daily lives is fair and free. We believe that we can have a better internet, a better democracy, and a better relationship between people and technology.

I support EFF because our free speech and privacy depend on it. Because the life of a protestor or an LGBTQ+ kid using encryption in an authoritarian country depends on it. Because the infrastructure of our democracy depends on it. Whatever your reason for coming to this work, I am so grateful for the support you have shown EFF over the years.

Take good care,

Allison Morris  
Chief Development Officer

# Thank You

EFF's individual and organizational members around the globe drive the movement for digital privacy, the free exchange of ideas, and an online world in which the public's interests come first. Together, we make a better digital future possible.

<b>EFF is grateful for the support of the following foundations:</b>	Filecoin Foundation for the Decentralized Web	The Ford Foundation
Future of Life Institute	Kaphan Foundation	John D. and Catherine T. MacArthur Foundation
Open Society Foundations	Alfred P. Sloan Foundation	Craig Newmark Philanthropies
Mark Cuban Foundation	The Stanton Foundation	Someland Foundation

Thanks also to our Luminary Organizational Members:  
DuckDuckGo, No Starch Press, and the Hering Foundation.