
EFF
2022
ANNUAL
REPORT
The Electronic Frontier Foundation (EFF)
is the leading nonprofit organization
defending civil liberties in the digital world.

ELECTRONIC FRONTIER FOUNDATION

TABLE OF CONTENTS

A Word From Our Executive Director

Dear friends,

At EFF, we believe that together we can create a future where our rights not only follow us online but are even enhanced by new technology. The activists, lawyers, and technologists on EFF's staff fight every day for a better future and against the kinds of dystopias best left to speculative fiction. In courts, legislatures, and corporate boardrooms, we make sure that users' needs are heard. Sometimes we send letters. Sometimes, as we did with Apple in 2021, we send an airplane carrying our message where company leaders and shareholders cannot miss them.

We had some big wins in 2022. After years of pressure, Apple finally implemented one of our longstanding demands to encrypt cloud backups. Apple also announced the final death of its dangerous plan to scan your phone (the initiative for which we hired the airplane). In San Francisco, the Board of Supervisors reversed its position on giving the SF Police Department the ability to deploy robots armed with bombs: This historic reversal happened only because EFF helped lead a strong and coordinated pushback by activists and concerned residents. These wins wouldn't have happened without you. General operating support and unrestricted donations from EFF members worldwide allow us to be both responsive to issues as they emerge, as well as to sustain long-term campaigns and legal strategies.

From local to international policy fronts, EFF's advocacy got results in 2022. In the European Union, we lobbied hard for a Digital Markets Act

that recognized the value of interoperability and meaningfully restrained the power of "gatekeeper" platforms. Sustained pressure from EFF, our members, and our allies helped protect free expression online by keeping Congress from mandating filters or link taxes. EFF also was instrumental in Congress passing the Safe Connections Act, a bill that makes it easier for survivors of domestic violence to keep their phone number while leaving a family plan. This simple protection can be essential to stopping abusers from using access to their victims' cellphone plans to track and harass.

Our skilled technologists continue to conduct original investigations and share critical digital privacy information with the public. We exposed a shadowy company called Fog Data Science that sells geolocation information of hundreds of millions of Americans to law enforcement agencies. We also researched apps used by daycare centers to collect and share information about children with their parents—finding that the apps are dangerously insecure, and the companies developing them were not interested in improving security. We encouraged parents to become advocates and published basic recommendations, such as implementing two-factor authentication, to help parents push for better security for their children's sensitive information.

EFF's reach is both broad and deep. We cannot cover everything in one report, but it's almost all available on our website and blog. And most importantly, none of our fights or victories would have been possible without our members, supporters, and all of you who stood up and took action to build a better future.

Sincerely,

Cindy Cohn, EFF Executive Director

Build a Better Digital Future.
Donate to EFF.

EFF by the Numbers:

17
Legal and Legislative Victories

78
Press Mentions Per Day (average)

20
Amicus Briefs Filed

76
Electronic Frontier Alliance (EFA) Members

16.2 million
Unique Page Views of EFF.org

154 countries
where “How to Fix the Internet” Podcast was downloaded

489,400
EFFector Newsletter Subscribers

nearly 1 in 5
EFF Members Live Outside the U.S.

34% of members
are Sustaining Donors

HIGHLIGHTS

2022

DIGITAL PRIVACY

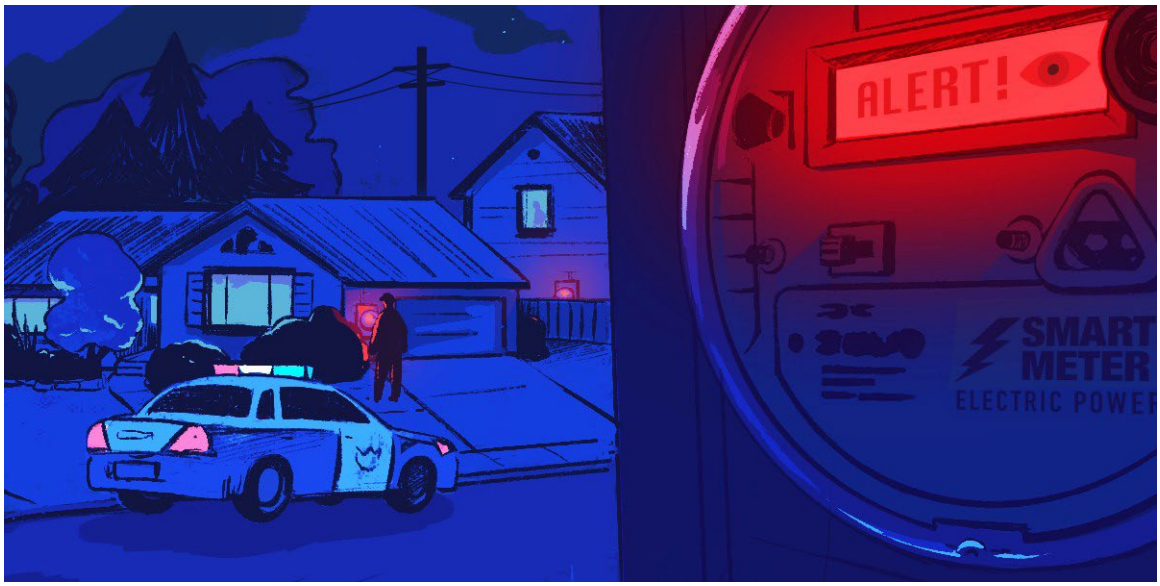
EFF's approach to privacy enables autonomy, anonymity, security, and the right to a life free from prying eyes. This allows for free association and expression, while also taking into account legitimate law enforcement concerns. National and local governments must put legal checks in place to prevent abuse of state powers, and international bodies should consider how a changing technological environment shapes security agencies' best practices.

Promoting Medical Digital Privacy

While EFF has long promoted medical digital privacy, this issue became especially urgent in 2022 when the Supreme Court reversed its protection of abortions, and digital data became a key way in which governments can try to identify people seeking reproductive care. EFF created a principled guide for platforms to respect user privacy and rights to privacy in their bodily autonomy, called on nonprofit organizations to remove trackers from their websites, and worked with legislators on commonsense privacy legislation to protect not only health-related data but the full range of consumer data that could be weaponized against abortion seekers. Working with our allies at ACLU NorCal and ACLU SoCal, we successfully pushed for the passage of AB 1242, a law that now protects the data privacy of people seeking abortion by limiting how California-based entities disclose abortion-related information. EFF continues to support federal legislation like Rep. Sara Jacobs' My Body, My Data bill, which would limit how businesses collect, retain, use, and share reproductive health data.

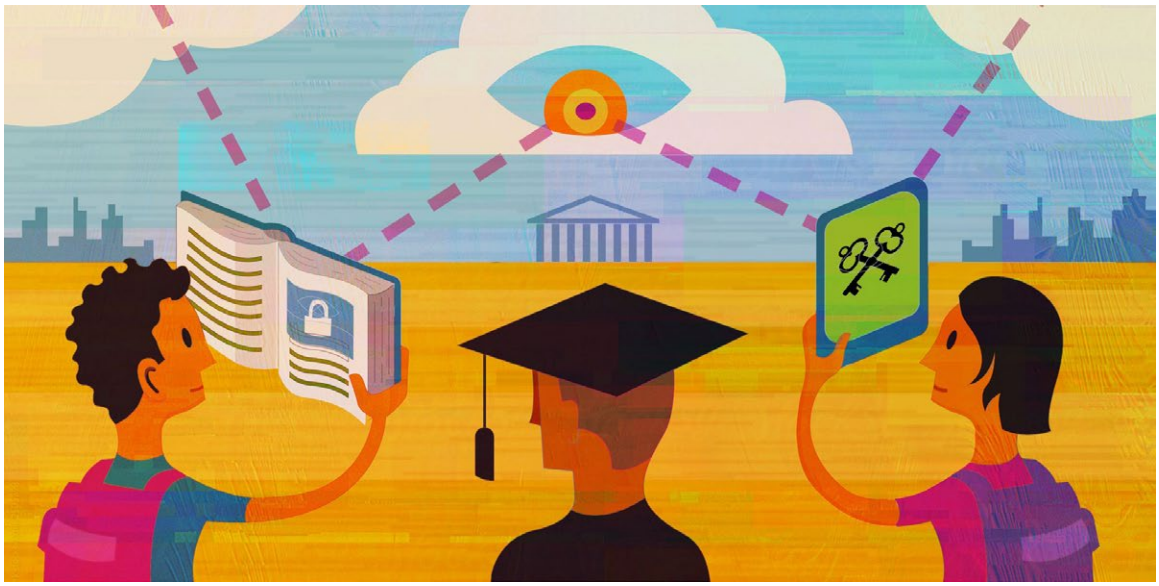
We provided critical information on how patients, their family members and friends, doctors, nurses, clinic staff, reproductive rights activists, abortion rights counselors, and even drivers who help take patients to

clinics can keep themselves and their communities safe. We highlighted information on how reproductive health workers in California can take advantage of an opt-out in the California Public Records Act and leverage the Safe at Home Program to protect the information they submit to the government. Many reports in local, national, and international print, online, and broadcast media cited EFF and its experts regarding the new data privacy risks that came with the Supreme Court's overturning of *Roe v. Wade*. Some of the most prominent included stories from The New York Times, The Washington Post, Reuters, Bloomberg, the Associated Press, NBC News, and CNN, and op-eds in Wired and the Thomson-Reuters Foundation.



Illegal Data Sharing Leads to Targeting of Asian Americans

Utility data can provide a detailed picture of what occurs within a home, and the advent of smart utility meters has only enhanced that image. Smart meters provide usage information in increments of 15 minutes or less; this granular information is beamed wirelessly to the utility several times each day and can be stored in the utility's databases for years. As that data accumulates over time, it can provide inferences about private daily routines such as what devices are being used, when they are in use, and how this changes over time. California laws require that such information be shared only as required by federal or state law, and upon a court order or law enforcement request relative to an ongoing investigation. But the Sacramento Municipal Utility District (SMUD) has been searching entire zip codes' worth of people's private data and disclosing it to the Sacramento Police Department (SPD) without a warrant or any individualized suspicion of wrongdoing, in search of illicit cannabis operations—a scheme that specifically targeted Asian-American communities. In response, EFF filed a lawsuit against SMUD and SPD on behalf of the Asian American Liberation Network and a few individual Asian-American Sacramento residents to fight this illegal data sharing practice.

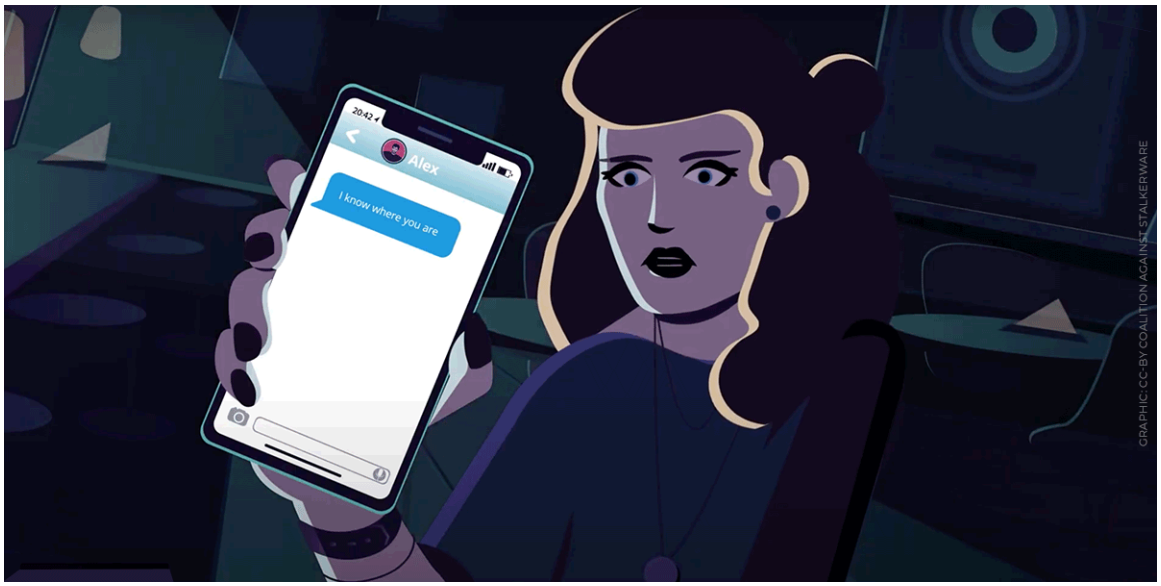


Highlighting Student and Youth Privacy

Giving parents and schools proper security controls and hardening application infrastructure should be the top priority for apps that handle children's data, especially children in daycare. Daycare and preschool applications frequently include notifications for things like feedings, diaper changes, pictures, activities, and which guardian picked-up/dropped-off the child. Many childcare providers require parents to use these apps, and troublingly, an EFF investigation found that the apps were not secure. Our technologists conducted static and dynamic analyses of several popular daycare and early education apps, and quickly found issues as basic as a lack of minimal security measures like multi-factor authentication. We also encountered privacy-compromising features such as weak password policies, Facebook tracking, cleartext traffic enabled, and vectors for malicious apps to view sensitive data. It's imperative that the developers of these applications address common and easily fixed security vulnerabilities. EFF called on all these services to prioritize basic protections and guidelines and provided parents with the information they need to put the necessary pressure on these services.

SECURITY

Computer security—and the lack of it—is a fundamental issue that underpins much of how the internet does and doesn't function. EFF works on a wide range of security issues, including standing up for encryption 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.

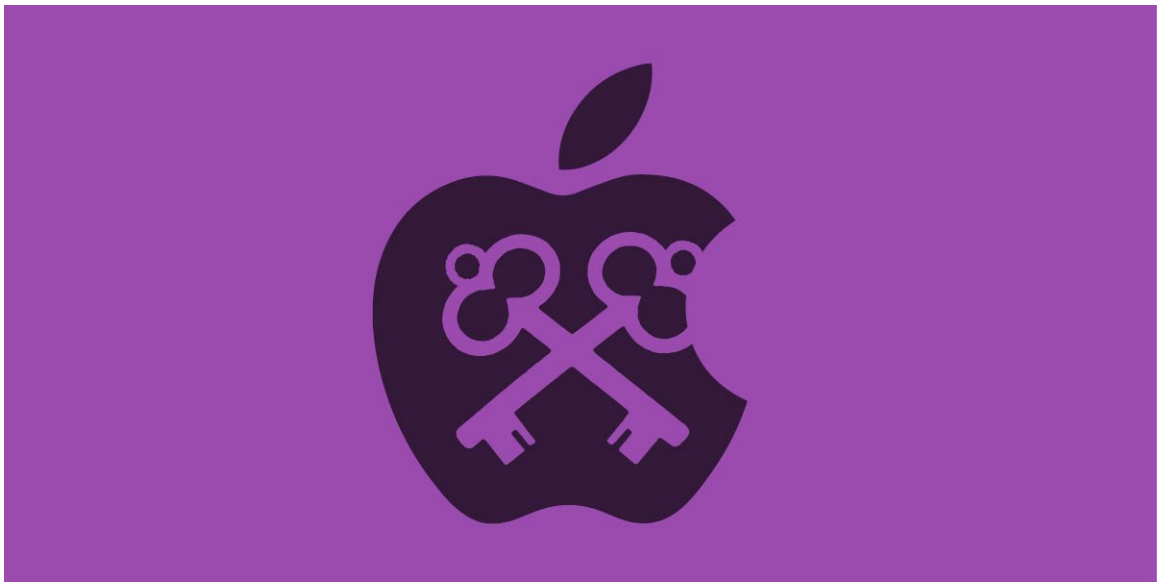


Fighting Stalkerware and Tech-Enabled Abuse

EFF had significant victories in the fight against tech-enabled domestic and personal abuse. We celebrated the passage of the Safe Connections Act, almost two years after it was first introduced. This common-sense federal law makes it easier for survivors of domestic violence to separate their phone line from a family plan while keeping their phone number. The bill also requires the Federal Communications Commission (FCC) to create rules to protect victims' privacy. This victory followed the unanimous passage of Maryland's S.B. 134, a bill developed in collaboration with EFF's cybersecurity experts. This law requires law enforcement officers to be trained in identifying the use of stalkerware in domestic violence and intimate partner abuse.

EFF successfully advocated for a comprehensive approach to anti-stalking mitigations for physical trackers. Apple's AirTag has been commonly misused as a physical tracker, and while iPhone users were alerted to the presence of an AirTag nearby, Android users had no tools available to detect the device. Tile's proprietary trackers have been misused in the same way, and anyone without the Tile app would also have no means of detecting the tracker. We called on all manufacturers

to agree on and publish an industry standard that would let developers incorporate physical tracking detection into both mobile apps and operating systems. In response to our advocacy, Apple took new steps to increase protections against the use of AirTags by stalkers by releasing an Android app called Tracker Detect. Tile also released a scanning app that lets people concerned about nonconsensual tracking discover whether a Tile is being used to track them. While we welcome these changes, both require a proactive scan to search for unwanted tracking devices. We are continuing to push for more protections industry-wide, but tracking detectors like these are a necessary first step.



Pushing Apple to Encrypt iCloud Backups

Apple announced it will provide fully encrypted iCloud backups, finally meeting a longstanding demand by EFF and other privacy-focused organizations. We applaud Apple for listening to experts, child advocates, and users who want to protect their most sensitive data. Encryption is one of the most important tools we have for maintaining privacy and security online. Apple's on-device encryption is strong, but some especially sensitive iCloud data, such as photos and backups, continued to be vulnerable to government demands and hackers. Users who opt into Apple's new proposed feature—which the company calls Advanced Data Protection for iCloud—will be protected even if there is a data breach in the cloud, a government demand, or a breach from within Apple (such as a rogue employee).

With this action, along with officially dropping plans to install photo-scanning software which would have inspected users' private photos on their devices, Apple took a big step forward towards protecting user privacy and human rights. There are a number of implementation choices that can affect the overall security of the new feature, and we'll be pushing Apple to make sure the encryption is as strong as possible. We'd like Apple to go a step further: Turn on these privacy-protective features by default and protect the rights of all users.

Investigating Apps and Malware

EFF's Threat Lab malware analysis team focused its attention on the Android ecosystem, investigating a multi-stage class of malware called "tor-hydra." This malware masquerades as banking apps to lure unsuspecting customers into installing them. To illustrate our process, we published a blog post investigating one such malware that presents itself as the banking app for BAWAG (a prominent financial institution in Austria) and provided information to help other researchers understand and identify it. The malware uses a number of obfuscation techniques to hide its true functionality: adding devices to a network controlled by malicious hackers in order to launch large scale attacks. Upon first run, the app prompts the user to give "accessibility services" permission to the app. The accessibility services permission grants an app broad access to read the infected device's screen and mimic user interaction. Upon granting the permission, the app backgrounds itself. Any attempt by the user to uninstall the app is prevented by the app interrupting and closing the uninstall dialogues. Attempting to open the app again also fails—nothing happens, making it difficult for users to detect and remove the malware.

Our work to stop malware also included building new apps, publishing guides, and exposing other malware. We continued building an Android

app downloading application called apkeep—which assists security researchers and analysts in downloading multiple apps from various sources—and brought it to more platforms for wider access. We also exposed and intervened in a new campaign by the cyber mercenary group we previously dubbed "Dark Caracal," which resulted in hundreds of infections across more than a dozen countries since March 2022. In addition to investigating instances of Android malware, we described in detail a technique researchers can use to observe the behavior of apps they are researching without the need for a sophisticated multi-device lab setup, or where complex real-world interactions (such as unlocking a car door with an app) are being analyzed.

TRANSPARENCY

EFF holds governments accountable to the public through federal and state freedom of information laws, the courtroom, and our megaphone. 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.

Exposing Mass Surveillance of Cell Phone Users by Law Enforcement

EFF investigated Fog Data Science, LLC, a shadowy data broker that sells millions of Americans' geolocation data to state and local law enforcement agencies on the cheap, violating our Fourth Amendment right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." We found that Fog Data Science provides law enforcement with easy and often warrantless access to the precise and continuous geolocation of hundreds of millions of Americans, collected through a wide range of smartphone apps and then aggregated by intermediary data brokers. We worked with the Associated Press for an exclusive story, which was carried by hundreds if not thousands of subscribers in English, Spanish, French, German, Polish, Chinese, and Japanese. It also generated significant secondary attention via requests for interviews at other media outlets, and an op-ed in Slate. Lawmakers from Oregon and California cited our investigation in their comments to the Federal Trade Commission urging them to investigate Fog Data Science's practices.

EFF used public records to investigate how Fog's service works, where its data comes from, who is behind the company, and how the service

threatens people's privacy and safety. The company's marketing materials boast of access to "billions" of data points from "over 250 million" devices, and claim this data can be used to learn about where people work, live, and associate. EFF found that this personal data is obtained from thousands of different apps on Android and iOS stores as part of a larger location data marketplace. Fog sells access to this data to both private and public sector customers, including law enforcement agencies from the local to federal level.

Unfortunately, Fog is not the only company with location data for sale—data brokerage is a multi-billion-dollar industry. This study highlights the urgency for data privacy laws that limit how corporations obtain and process our data, and how that data is used by third parties. In the meantime, EFF provided simple instructions on how to turn off location tracking on Android and iOS devices (as well as other data privacy tips via our Surveillance Self Defense guides), which has become one of our most popular blog posts.

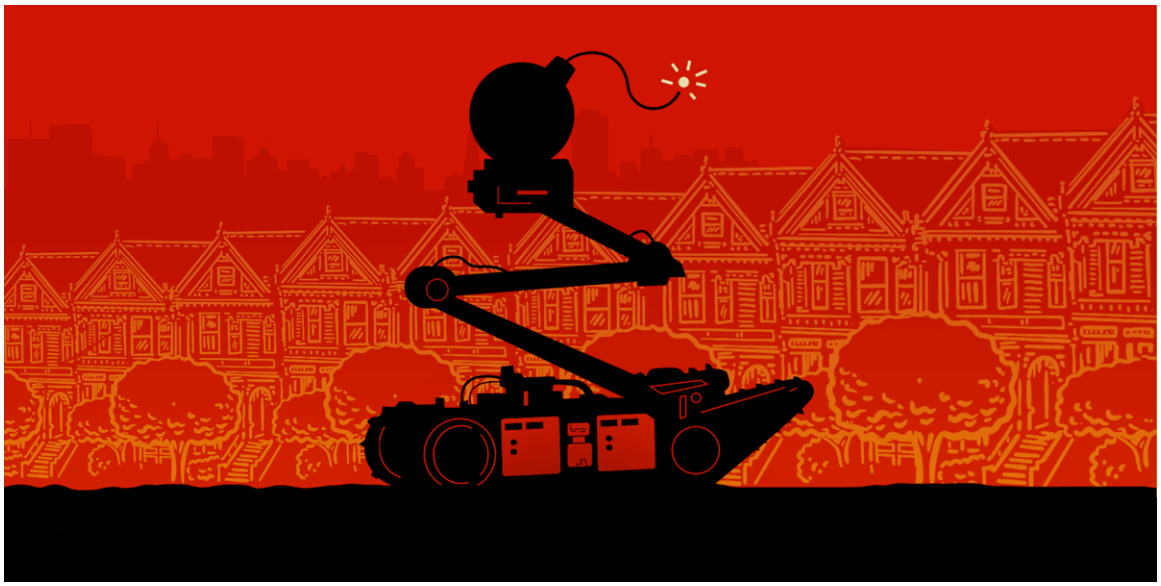
Revealing the Alarming Surveillance Technology at the U.S.-Mexico Border

To better educate the public on escalating border surveillance and make information available to researchers, EFF published photos of our research trips to the U.S.-Mexico border and created a map of surveillance towers along the border for wide release. Throughout this work, we have met with various stakeholders in California, Arizona, New Mexico, Texas, and border cities like Tijuana and Ciudad Juarez: These included search-and-rescue organizations, journalists, human rights advocates, anti-surveillance activists, humanitarian workers, journalists, and law enforcement. We built support for movements against automated license plate readers in Imperial County, California and Austin, Texas. Our investigations revealed a disturbing expansion of surveillance deployed by federal agencies such as Customs and Border Protection (CBP), and its sub-division, the U.S. Border Patrol. We found constant surveillance and a digital dragnet that threatens the civil liberties and human rights of millions of unsuspecting people along the border—sometimes up to seven miles away from a surveillance tower. We gathered data on a variety of surveillance towers, documented two new surveillance blimps, and attended a Border Security Expo in Texas. EFF toured surveillance technologies in the desert and within

cities, visited migrant shelters, and recorded audio and video media for eventual public-facing materials. CBP is planning yet another massive expansion of surveillance, including the installation of 307 new towers along the Southern border. We will continue to investigate and share with stakeholders and the public our findings about the state of surveillance along the border.

"The rapid expansion of digital surveillance along the U.S.-Mexico border doesn't just affect migrants—it affects anyone living near either side of the border as well, putting them in the constant shadow of billions of dollars worth of privacy-invading technology. About two out of three Americans live within 100 miles of a land or sea border, putting them within Customs and Border Protection's special enforcement zone, so surveillance overreach must concern us all."

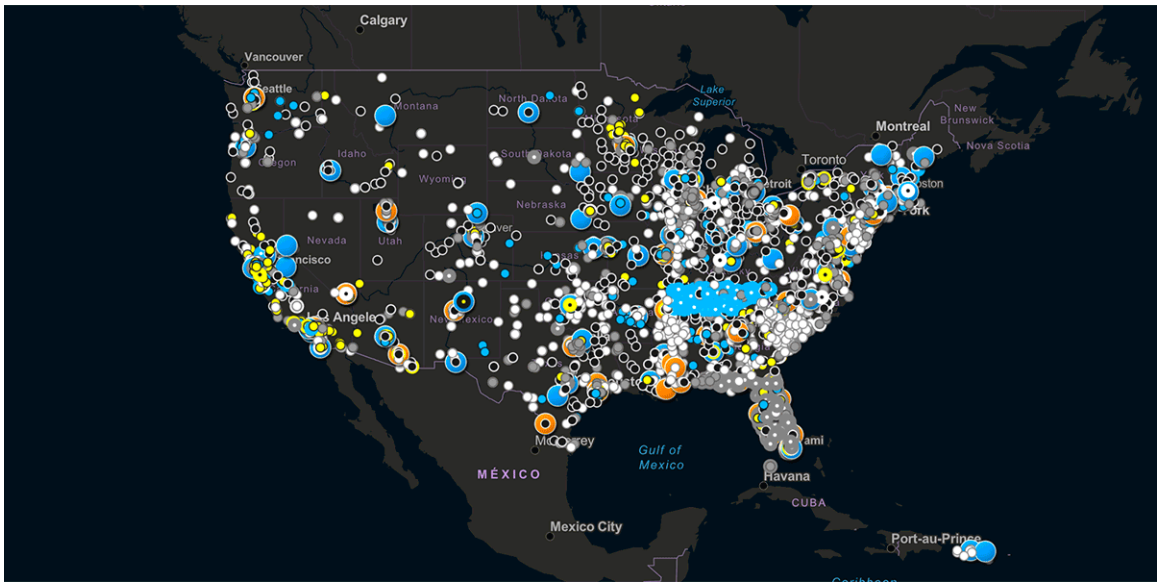
— EFF Activism Director Jason Kelley



Stopping San Francisco's Killer Robots

EFF led a coalition to oppose a San Francisco Board of Supervisors bill to set use policy for various police technologies, including authorizing the San Francisco Police Department to deploy deadly force via remote control robots. This broad policy would have let police bring robots carrying bombs to deploy deadly force at any arrest, and any execution of a warrant to search a house or vehicle or device. Depending on how police choose to define the words "critical" or "exigent," police might even have been able to bring these armed robots to a protest.

Thanks to EFF's work, the campaign to stop killer robots was covered by news outlets all over the world. Over 50 local organizations, including EFF and Electronic Frontier Alliance (EFA) members, signed a coalition letter demanding that the supervisors reverse their course on killer robots, and they did. Despite an 8-to-3 approval on initial vote, public pressure led to a reversal on the final vote, plus passage of a stopgap ban on killer robots—all over the course of just one week. This could not have been achieved without the hard work of activists and residents across the Bay Area who worked together to tell the Board that this policy was unacceptable—and that message was impossible for the Board, and the world, to ignore.



Showcasing U.S. Law Enforcement Technologies via the Atlas of Surveillance

The Atlas of Surveillance is a database of surveillance technologies deployed by law enforcement in communities across the United States. This includes drones, body-worn cameras, automated license plate readers, facial recognition, and more. The research was compiled by more than 1,000 students and volunteers and incorporates datasets from a variety of public and non-profit sources. In 2022, the Atlas of Surveillance grew to over 10,000 data points. It was cited in filings with the U.S. Supreme Court and the Federal Trade Commission, and we continue to hear from journalists and researchers who are using the Atlas in their work. The growth is thanks to a five–year partnership with journalism students from University of Nevada, Reno (UNR), as well as the incorporation of data from small rural-tribal body-worn camera grants, and public records we obtained listing every agency in Michigan that uses face recognition. We have leveled up our Cybersecurity and Surveillance course, introducing virtual reality-based instruction on border technology and increasing the number of guest speakers. The Freedom of Information Act (FOIA) class taught by EFF staff at UNR is also moving along strongly, with students filing nearly a dozen public records requests related to police drones.

FREE SPEECH

EFF fights for free expression offered by new technology—overcoming the legal, structural, and corporate obstacles in the way of people around the world speaking their mind and accessing information and ideas. We should be able to use new technologies to publish our ideas; criticize those in power; gather and report the news; and make, adapt, and share creative works. This right is especially important for vulnerable communities, who must be able to safely meet, grow, and make themselves heard without being silenced or drowned out by the powerful.

Protecting Student Speech

Remote learning has blurred the lines between school and home, and online proctoring and other sinister forms of surveillance and disciplinary technology have made it increasingly difficult for students to protect their privacy and freely express themselves. Students have fought back, and often won, and we're glad to have been on their side. In a victory for fair use, and against bad faith Digital Millennium Copyright Act (DMCA) takedowns used to silence critics, EFF represented Erik Johnson, a computer engineering undergraduate, in his lawsuit against exam surveillance software maker Proctorio. Johnson examined the software's functions, and in a series of tweets, critiqued Proctorio's invasive practices and the potential mishandling of private information collected from students' computers. Proctorio attempted to use the copyright takedown provisions of the DMCA to remove Johnson's tweets, which included links to short excerpts of its software code and a screenshot. Johnson's tweets may have rankled Proctorio by revealing to the public how the company's software worked, but he did not infringe on the company's intellectual property. Fair use means using pieces of code to explain your research or support criticism, and is no different from quoting a book in a review. We asked the court to rule Johnson's posts were protected by the fair use doctrine, and to hold Proctorio

responsible for submitting takedown notices in bad faith. Under the settlement, Proctorio dropped its copyright claim and others it had filed blaming Johnson for damaging its reputation. In return, Johnson dropped his claims against Proctorio.

It's Time for a Federal Anti-SLAPP Law

Our country's fair and independent courts exist to resolve serious disputes, not for bad actors to abuse the civil litigation process to silence others' speech. Unfortunately, some parties take advantage of our systems to do just that. In such Strategic Lawsuits Against Public Participation (SLAPP), which have been on the rise over the past few decades, plaintiffs use the high cost of litigation to harass, intimidate, and silence those who speak out against them—those who may not have the financial resources to withstand a protracted legal battle. EFF has championed anti-SLAPP laws for more than a decade: More than half of the states now have robust anti-SLAPP laws in place, but we need comprehensive federal protection as well. EFF urged Congress to pass the Strategic Lawsuits Against Public Participation Protection Act of 2022 (H.R. 8864) and will continue to fight for protections against lawsuits that intend to harass people into silence.

As awareness of SLAPP lawsuits has grown, the Uniform Law Commission published its Uniform Public Expression Protection Act (UPEPA), a model anti-SLAPP bill for states to follow. EFF joined with civil society groups from across the political spectrum including the American Civil Liberties Union (ACLU), Institute for Justice, Public

Participation Project, Reporters Committee for Freedom of the Press, and other free speech groups to endorse UPEPA. These groups cover a wide range of interests, but we agree on this principle: Our courts should be focused on resolving disputes and should not be hijacked to stifle the right to free expression.

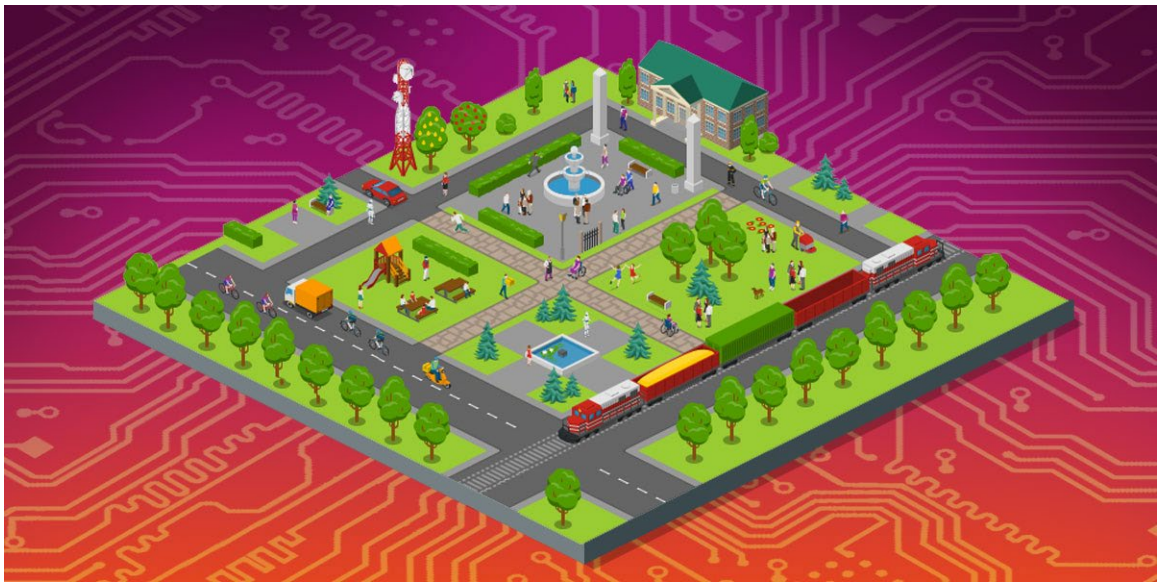
Internet Infrastructure Providers Should Avoid Content Policing

Human rights are at risk when companies that constitute basic internet infrastructure (such as internet service providers, certificate authorities, domain name registrars, and hosting providers) intervene to take down speech and other content online. The same is true of payment processors and many other critical internet services. EFF and an international coalition of 56 human and digital rights organizations from around the world have called on technology companies to "Protect the Stack." This is a global effort to educate users, lawmakers, regulators, companies, and activists about how content policing practices can and have caused risks to human rights and marginalized groups. It is currently available in English, Spanish, Arabic, French, German, Portuguese, Hebrew, and Hindi.

"Internet infrastructure companies help make the web a safe and robust space for free speech and expression. Content-based interventions at the infrastructure level often cause collateral damage that disproportionately harms less powerful groups. So, except in rare cases, stack services should stay out of content policing."
— Corynne McSherry, EFF Legal Director

CREATIVITY & INNOVATION

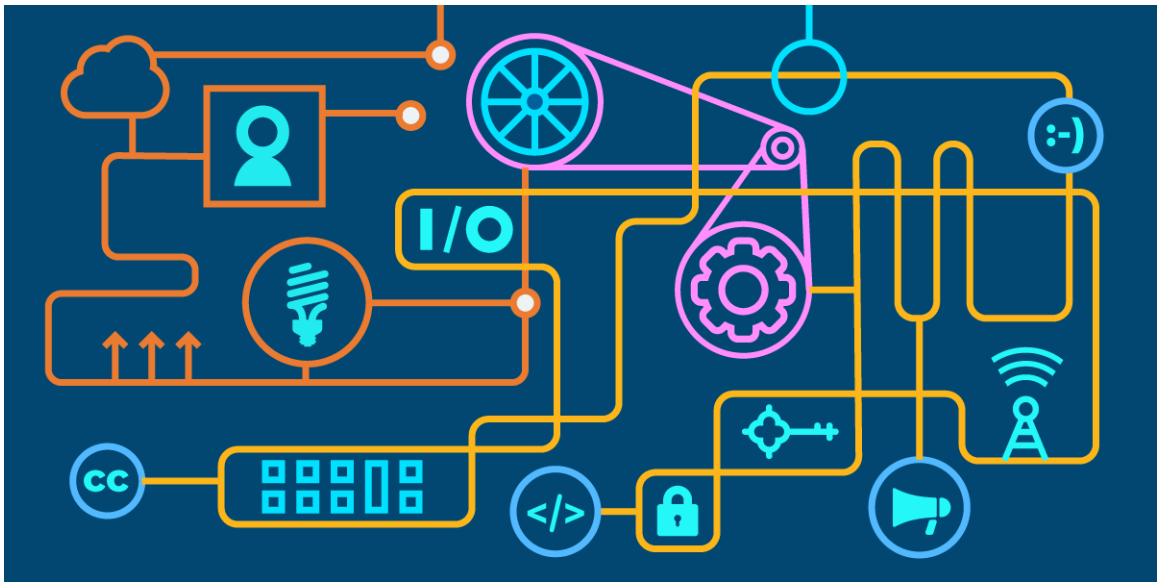
EFF works to protect and strengthen fair use, innovation, open access, net neutrality, and your freedom to tinker. We challenge patent and copyright trolls in public and in court; argue in Congress for more balanced copyright and patent laws; and urge governments, funders, and educational institutions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



Promoting Decentralization and the Fediverse

For too long, users have felt trapped into using social media and other services that don't serve them well and whose surveillance business models violate their privacy. 2022 was a roller coaster for the movement to decentralize the services and tools that we rely on every day. Overall, it was an exciting time for the broader decentralization movement, but it was just the beginning. When changes in leadership at Twitter prompted many users to leave or reduce their presence on the platform, EFF published a series of blogs explaining the fediverse, its potential, and how to find a home there and get settled. The fediverse isn't a single, gigantic social media platform—it's an expanding ecosystem of interconnected social media sites and services that let people interact with each other, regardless of which site and service they use. That means they can tailor and better control their social media experiences. Each server (or "instance") can experiment and build its own experience for users, and those users aren't obligated to a platform simply because their contacts are on that platform. Anyone on (almost) any server can follow and be followed by people on any server. Better yet, the fediverse has mechanisms for moving accounts between servers, including ways

to export and import your posts, follow and block lists, and redirect your profile from one server to another. This new spark of competition between platforms and federations holds the potential for new innovations and improvements to our autonomy online.



Advocating for Adversarial Interoperability

Another technique for giving users more choice and power against the tech monopolies is through adversarial interoperability—the ability to create a new product or service that plugs into the existing ones without requiring permission of the companies that make them. For comparison, think of third-party printer ink, alternative app stores, or independent repair shops that use compatible parts from rival manufacturers to repair your car, phone, or equipment. EFF published a white paper, "Interoperable Facebook," and produced a short "design fiction" video to demonstrate this concept. Empowering developers to engineer new tools as they see fit, rather than at the whim of tech giants, creates space for innovation and more user choice in how and where their data is stored and used, as well as who they can interact with.

Encouraging Right to Repair

EFF supported Right to Repair laws in several states because we believe owners should have control over their own devices. Thanks to the hard work of legislators, policy makers, and grassroots activists, the New York State legislature passed the Digital Fair Repair Act, supported by the Repair Coalition. This landmark legislation requires manufacturers to sell parts and special tools at "fair and reasonable terms'' to users and third-party repair technicians. Manufacturers are also required to provide access to repair information, software, and the ability to apply firmware patches. New York's bill comes after a success in Colorado for wheelchair users quite literally stranded by Digital Rights Management. A study revealed dismally frequent incidents of wheelchair failures (93% of respondents needed wheelchair service in the previous year, 68% needed two or more repairs), and the long service delays that wheelchair users must endure: 62% waited four or more weeks for each repair and 40% waited seven or more weeks.

EFF also celebrated the hard work of Right to Repair activists and policy makers. We honored Kyle Wiens with 2022's EFF Award for Right to Repair Advocacy. In addition to his amazing advocacy work, Wiens has been running the website iFixIt since 2003, providing a home for the users and activists in the right to repair movement to share guides on

how to repair everything. We also hosted Adam Savage—a Right to Repair advocate known for his shows MythBusters and Savage Builds—on our podcast, "How to Fix the Internet." In the episode "Making Hope," Adam, Cindy Cohn, and Danny O'Brien discussed creating a world built on collaboration and creativity.

Exposing Underhanded Operations of Patent Trolls

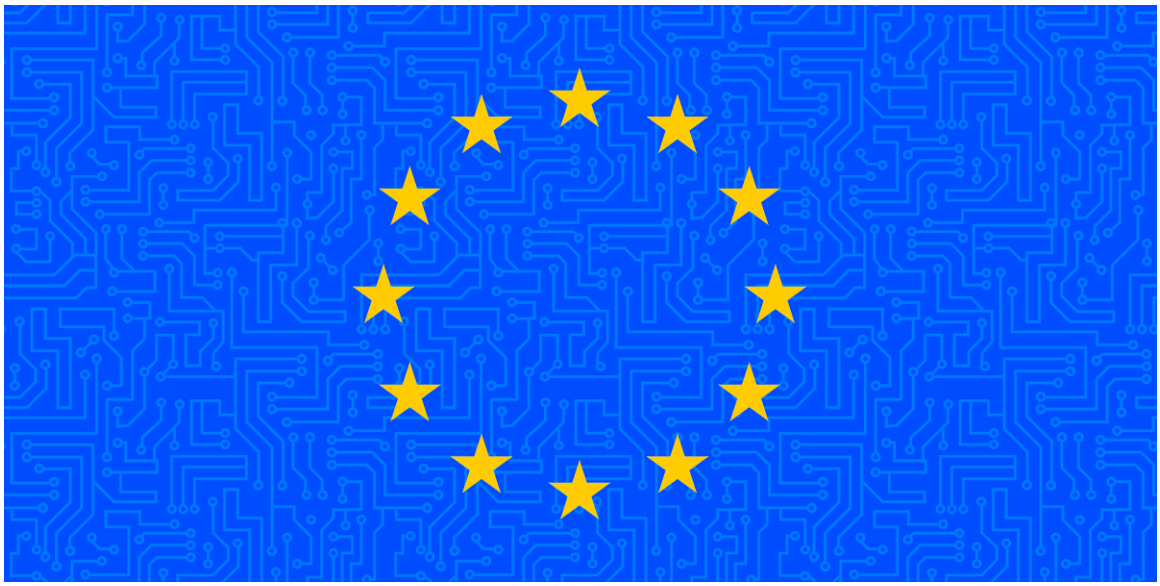
Patent trolls rely on secrecy to perpetuate their business, and EFF shines a light on these underhanded operations to expose them to the public and elected officials. EFF's legal wins against patent trolls are part of a positive trend of federal courts increasingly demanding more transparency in patent cases, including disclosures about litigation funding. EFF had a big win in our long-running legal case seeking to unseal records related to Uniloc's patent trolling; this includes licensing agreements that Uniloc used to convince a private equity firm called Fortress to fund its patent-trolling activities. The case began in 2018 as an effort to understand heavily redacted filings in a patent infringement case between Uniloc and Apple. Thanks to our litigation, the great majority of Uniloc's previously secret court records showing how they shook down many major tech companies are now public.

EFF also filed an amicus brief *In Re: Nimitz Technologies LLC*, a case in which a Delaware federal judge scrutinized several patent troll companies: He asked owners of several patent-holding LLCs (which have filed 69 lawsuits in his court so far) to testify about their histories and financing. The trolls' lawyers sought to have an appeals court shut down

the investigation. EFF's brief explained that judges must be allowed to demand more information about the patent troll companies that are abusing our public courts for their business. The U.S. Court of Appeals for the Federal Circuit accepted EFF's brief, denied the petition brought by patent troll Nimitz Technologies, and allowed the investigation to proceed.

INTERNATIONAL

EFF's international team advocates for privacy, free speech, and an open internet in international venues and 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.



Protecting Online Expression Worldwide

EFF is deeply engaged in the global fight for free expression online. In 2022, we worked with the Digital Services Act Human Rights Alliance to ensure that European Union lawmakers consider the global impacts of their legislation. We also joined the Arab Alliance for Digital Rights, a newly formed coalition that brings together groups across the Middle East/North Africa region and international partners to protect civic space online. EFF continued our work as a long-term member of the International Freedom of Expression Exchange network. We participated in a number of international fora, including the Balkans-based Political Accountability and New Technologies conference, Forum on Internet Freedom in Africa, Bread and Net in Lebanon, and the Organization for Security and Cooperation in Europe.

"With authoritarianism encroaching around the globe, we must be more vigilant than ever in protecting human rights advocates from threats to their digital security."
— EFF Civil Liberties Director David Greene

Standing in Support of Iranian Technologists and Digital Rights Defenders

EFF joined Access Now, Article19, and Front-Line Defenders to issue a statement calling on Iran to stop the persecution of the digital rights community and to release detainees. Iran is well-known for its extreme censorship and filtering of internet traffic, but the popular uprising organized by Iranians protesting the death of Jina (Mahsa) Amini at the hands of Iran's morality police represented a new low for an already oppressive regime. Leading Iranian digital rights activists and technologists, including Amiremad (Jadi) Mirmirani and Aryan Eqbal, were among the many protestors arrested, detained, and tortured at the hands of Iranian authorities in their brutal retaliatory crackdown.

In the early days of the protests, Iranian security forces quickly resorted to a total communications blackout, cutting Iran off from the internet to prevent information from reaching the rest of the world. Though the protests were overwhelmingly peaceful, cruel physical tactics were frequently used to repress opposition and punish protestors. In EFF's statement, we expressed that we were "deeply alarmed by the violent and unrestrained crackdown and the unlawful use of lethal force against protesters and bystanders who do not pose an imminent threat of death or serious injury across Iran, alongside the violent arrest and arbitrary

detention of the digital rights and other human rights defenders and ongoing internet restrictions." Thankfully, Aryan Eqbal eventually was released along with other digital rights defenders. Jadi Mirmirani remains wrongfully detained, and we continue to press for his release.

"We stand with Ukrainians and with all people in crisis zones who rely upon the free flow of information to survive. Social media platforms must recognize that all too often their services are misused to both spread misinformation and block from view desperately needed factual information, including evidence of war crimes and other gross human rights violations. These companies must take real steps to ensure that their policies are applied even-handedly and transparently and that their efforts continue after the immediate media spotlight moves on."

— EFF Director for International Freedom of Expression Jillian C. York

Winning User Privacy and Human Rights in XR, AR, VR, and Wearable Tech

Extended reality (XR) technologies, including virtual and augmented reality, are the foundations of emerging digital environments. While XR can have many positive impacts on our daily lives, it can also pose substantial risks to human rights. Virtual reality (VR) headsets, augmented reality (AR) glasses, and other wearables can continue the march toward ever-more-invasive data collection and surveillance. These devices collect huge amounts of data about our bodies and our homes, and mishandling of this data could exacerbate already severe privacy intrusions. EFF's work, along with that of our allies, resulted in a significant win for users' privacy in augmented reality, virtual reality, and wearable tech. We secured a commitment from Meta to allow VR users to "unlink" their devices from Facebook by creating separate Meta and Horizon accounts, neither of which are subject to Facebook's strict "real names" policies.

Continuing this conversation within human rights communities, we hosted two events at RightsCon 2022 to reinforce our commitment to existing safeguards in AR and VR. In one event, we demonstrated where previous policies and regulations fail to provide sufficient protections

for users in the present and future—especially regarding the new types of biometric data (such as heart rate, sleep patterns, and so on), that can be collected by personal wearable tech devices. EFF believes XR data should be used in our own interests, not to harm or manipulate us.

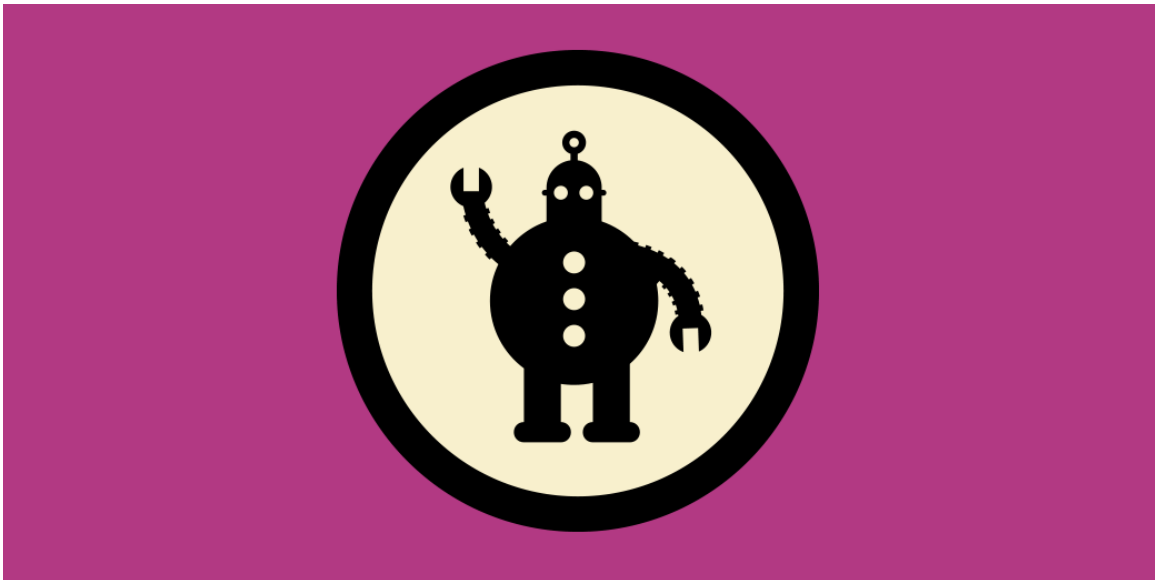

ONGOING
2022

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 members are fully volunteer-run, some are affiliated with a broader institution (such as student groups), and others 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 answer 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.

If there is an EFA group in your area, it can be a great resource for finding like-minded neighbors and activists to amplify your efforts.



Public Interest Technology

Privacy Badger

Privacy Badger is a browser add-on created and maintained by EFF that stops advertisers and other third-party trackers from secretly tracking where you go and what pages you look at on the web. If an advertiser seems to be tracking you across multiple websites without your permission, Privacy Badger automatically blocks that advertiser from loading any more content in your browser. To the advertiser seeking to track you, it's like you suddenly disappeared. 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 (SSD) 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.

CertBot

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. We released Certbot 2.0, and nearly 3 million new certificates were issued in 2022. Overall, there are 3.3 million installations maintaining 20 million certificates for 29.6 million domains.

"As someone who saw the shift from HTTP to HTTPS as a web developer, and as the Certbot project's manager today, I am proud of the work this team has done to make HTTPS ubiquitous on the web. Encrypting web traffic is one of the clearest, strongest gains in internet security of the past decade. I am pleased that EFF had such a big role in bringing it about."
— EFF Director of Engineering Alexis Hancock

Press and Communications

EFF leveraged our communications to advance advocacy and shape public conversations: In 2022, we had nearly 20,000 press mentions globally, or an average of 78 per day, along with a following of nearly half a million subscribers to our EFFector newsletter and 28 million page views (for EFF.org, our Action page, and several other websites we host). EFF experts were cited in a range of issues in The New York Times, CNN, NPR, Vice, USA Today, The Guardian, The Washington Post, and dozens of local news outlets. EFF's "How to Fix the Internet" podcast was downloaded in 154 countries (nearly 80% of the world's countries). We released fourteen episodes featuring interviews with technologists, right to repair advocates, and security experts envisioning a better way forward. Guests included comedian and host of the iconic "WTF" podcast Marc Maron, Academy Award-winning filmmaker Laura Poitras, elections security expert Pamela Smith, and maker extraordinaire Adam Savage.

In 2022, EFF compiled its first-ever sizzle reel, a supercut of the many TV appearances EFF staff made this year. Media Relations Director Josh Richman gives a behind-the-scenes breakdown on the reel and how his team works with various press outlets to reach millions of people around the world to highlight our activism, legal, and technology work.

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 (FCC), the world's largest entertainment companies, and major electronics companies, among others. EFF has also beaten bills in Congress and pressured companies to respect your rights.

Legal and Legislative Victories

1. California Prevails on Net Neutrality Rules EFF filed an amicus brief in 2021. (1/28/22) Federal

2. More Lawsuits Proceed Against Clearview's Face Surveillance EFF filed amicus briefs in 2021. (2/15/22) Federal, State

3. EFF Client Erik Johnson and Proctorio Settle Lawsuit Over Bogus DMCA Claims (3/25/22) Federal

4. Making Government Information More Accessible with Public.Resource.Org (4/1/22) Federal

5. Court Rules That DMCA Does Not Override First Amendment's Anonymous Speech Protections EFF filed an amicus brief in February 2022. (6/21/22) Federal

6. Another Court Protects the Right to Record Police EFF filed an amicus brief in late 2021 (7/12/22) Federal

7. Federal Court Upholds First Amendment Protections for Student's Off-Campus Social Media Post EFF filed an amicus brief in 2021. (8/5/22) Federal

8. Government Finally Releases Secretive Court Rulings Sought By EFF (8/22/22) Federal

9. Court Unseals Records Showing Patent Troll's Shakedown Efforts (9/30/22) Federal

10. The Safe Connections Act is Now Law (12/7/22) Federal

11. There Is No Link Tax in the End-of-Year Bills (12/20/22) Federal

12. Maryland Legislature Says Police Must Now Be Trained to Recognize Stalkerware (4/22/22) State

13. New York's Vaccine Privacy Bill Heads to Governor's Desk (6/22/22) State

14. South Carolina Will Not Advance Bill That Banned Speaking About Abortions Online (8/26/22) State

15. San Francisco Mayor Withdraws Harmful Measure Against Surveillance Oversight Law (3/1/22) Local

16. San Francisco Police Nailed for Violating Public Records Laws Regarding Face Recognition and Fusion Center Documents (6/2/22) Local

17. San Francisco Bans Killer Robots...For Now (12/7/22) Local

New Lawsuits

1. Uniloc 2017 LLC v. Google (4/25/22)

2. SMUD and Sacramento Police Violate State Law and Utility Customers' Privacy by Sharing Data Without a Warrant (9/12/22)

Policy Position Highlights

1. Cybersecurity Experts Urge EU Lawmakers to Fix Website Authentication Proposal That Puts Internet Users' Security and Privacy at Risk (3/3/22) International

2. EFF Statement on EU Parliament's Adoption of Digital Services Act and Digital Markets Act (7/5/22) International

3. EFF Opposes Anti-Fiber, Anti-Affordability Legislation in California That Will Raise Prices on Middle Income Users (5/23/22) State

4. EFF to Supreme Court: Put Texas Social Media Law Back on Hold (5/17/22) State

Amicus Briefs Filed

EFF's legal team shapes a wide range of decision-making through submission of amicus briefs. Through these "friend of the court" briefs, we provide expert advice or other relevant information, and have been cited by judges in their rulings.

1. EFF to European Court: "Right to be Forgotten" Shouldn't Stop The Public From Reading The News (3/7/22) International

2. EFF to European Court: No Intermediary Liability for Social Media Users (4/26/22) International

3. EFF to Inter-American Court of Human Rights: Colombia's Surveillance of Human Rights-Defending Lawyers Group Violated International Law (6/3/22) International

4. EFF to European Court: Keep Encryption Alive (6/28/22) International

5. EFF to Appeals Court: Apple's Monopoly Doesn't Make Users Safer (2/4/22) Federal

6. EFF to Court: Security Research Is a Fair Use (2/17/22) Federal

7. Copyright is Not a Shortcut Around the Constitution's Anonymous Speech Protections, EFF Tells Court (2/18/22) Federal

8. EFF and Partners to Ninth Circuit Court of Appeals: Retaliatory Investigation of Twitter Chills First Amendment Rights (4/12/22) Federal

9. Our Digital Lives Rest on a Robust, Flexible, and Stable Fair Use Regime (6/17/22) Federal

10. EFF Warns Another Court About the Dangers of Broad Site-Blocking Orders (6/17/22) Federal

11. When "Jawboning" Creates Private Liability (6/21/22) Federal

12. EFF and ACLU File Amicus Brief Objecting to Warrantless, Suspicionless Electronic Device Searches at the Border (7/14/22) Federal

13. EFF to Ninth Circuit: Social Media Content Moderation is Not "State Action" (9/7/22) Federal

14. EFF to Fifth Circuit: The First Amendment Protects the Right to Make Jokes on Social Media (11/22/22) Federal

15. Let Data Breach Victims Sue Marriott (11/30/22) Federal

16. This Judge's Investigation of Patent Trolls Must Be Allowed to Move Forward (12/2/22) Federal

17. EFF to Court: No Qualified Immunity for Wrongful Arrest of Independent Journalists (12/12/22) Federal

18. EFF to NJ court: Give Defendants Information Regarding Police Use of Facial Recognition Technology (9/30/22) State

19. EFF Files Amicus Brief Challenging Orange County, CA's Controversial DNA Collection Program (11/10/22) State

20. California Courts Must Protect Data Privacy (12/21/22) State

FINANCIALS

2022

A Message from EFF's Chief Development Officer:

ALLISON MORRIS
CHIEF DEVELOPMENT OFFICER

I am proud to not only lead EFF's fundraising efforts, but to be a member, too. In 2022, EFF was supported by 34,500 members, including nearly 12,000 sustaining donors. We were also supported by foundation grants and corporate members who share EFF's vision for a digital world that fosters free speech, privacy, and innovation. This financial support allowed EFF to take on the incredible work you read about in this report and more.

EFF raised over $23 million in public support during the 2021-22 fiscal year. Nearly 60% of our revenue came from individual donors, who joined us through membership drives including at DEF CON, BSides and other conferences. Of that $13 million from individuals, almost $5.5 million came from donations of less than $1,000 each. Foundation support increased by $3.7 million from the prior year, thanks to new and returning public foundations that awarded flexible general support—including over $4 million allocated for the next two years. This helped make up for the unrealized loss of investment income that EFF and so many others experienced in the stock market as the economic downturn began. The federal Paycheck Protection Program COVID loan forgiveness program also sunsetted. I am proud that EFF was able to maintain the quality and volume of work in 2022 despite these financial reductions.

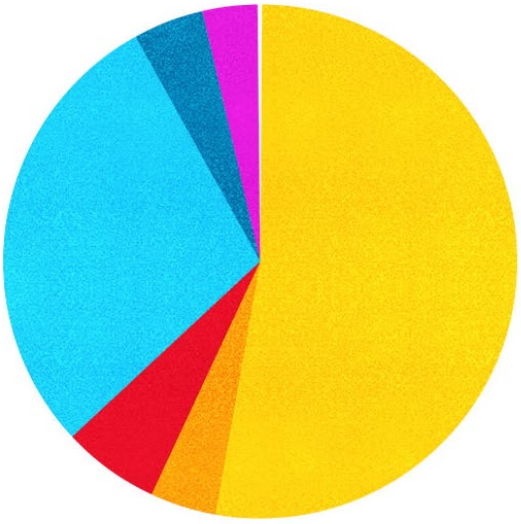
Our members and donors did much more than contribute to the financial health of EFF. In our activism, advocacy, and legal work, we spoke with the power of 34,500 voices. When working with local, state, national and international governing bodies, you are the power of our movement. As the world learned what it meant to move from the acute phase of the COVID pandemic to the new version of normal, so did EFF. It was wonderful to reconnect with so many people in person, and to maintain relationships with supporters through online engagement.

It is our honor and privilege to be trusted stewards of your financial support. For the tenth year in a row, Charity Navigator, the watchdog non-profit organization dedicated to providing unbiased, objective, data-based assessments of over 9,000 global organizations, gave EFF the highest possible rating of four stars in accountability and transparency.

For every action EFF took—each legislative victory, each spotlight shone on bad actors, each day in court, each technology we developed—you were beside us as a part of the movement. We cannot do this without you. Thank you for your support, your commitment to EFF's mission, and your trust. Thank you for standing together for digital civil liberties.

Take good care,

Allison Morris
Chief Development Officer
Donate to EFF.

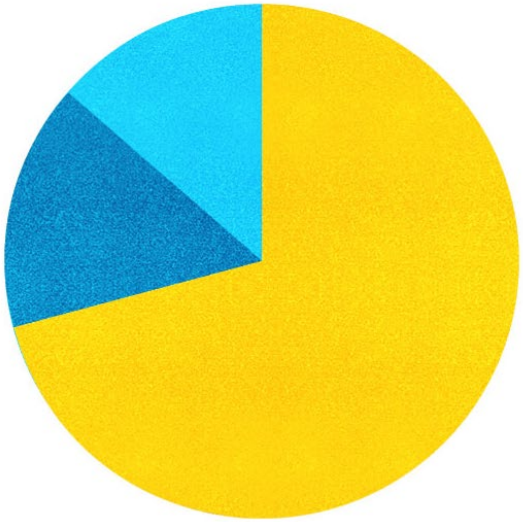


EFF FY 2021-2022 PUBLIC SUPPORT

Individual	$ 12,356,800
Individual through Foundation	786,600
Employee & Customer-Directed Gifts	1,007,000
Foundation	6,795,400
Corporate	736,400
Cy Pres	1,403,100
In-kind Contributions	34,100
Total Public Support	**$23,119,400**

EFF FY 2021-2022 EXPENSES

Program	$ 11,898,700
Administrative	2,487,400
Fundraising	2,274,400
Total Expenses	**$16,660,500**



INCOME

PUBLIC SUPPORT

Individual Contributions	
Individual Contributions over $50,000	$3,992,500
Individual Contributions $10,000-$50,000	$1,254,000
Individual Contributions $1,000-$10,000	$1,665,800
Individual Contributions under $1,000	$5,444,500
Total Individual Contributions	$12,356,800
Individual Contributions through Foundations	
Individual Contributions through Foundations Over $50,000	$410,000
Individual Contributions through Foundations Up to $50,000	$376,600
Total Individual Contributions through Foundations	$786,600
Foundation Grants*	$6,795,400
Cy Pres Awards	
Flaum v. Doctors Associates, Inc. (Subway)	$1,033,500
Buchanan v. SiriusXM Radio	$92,300
In re Carrier IQ, Inc. Consumer Privacy Litigation	$277,300
Total Cy Pres Awards	$1,403,100
Corporate Contributions	
Employee and Customer-Directed Gifts**	$1,007,000
Other Corporate Contributions	$736,400
Total Corporate Contributions	$1,743,400
In-kind Legal Services	$34,100
TOTAL PUBLIC SUPPORT	$23,119,400

REVENUE

Net Investment Income***	-$6,601,800
Attorneys' Fees Awarded	$4,400
EFF Event Income, net of expenses	$23,900
Miscellaneous	$90,700
TOTAL REVENUE	**-$6,482,800**

TOTAL SUPPORT AND REVENUE $16,636,600

* Includes over $4M allocated for future years.

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

*** Includes unrealized losses resulting from changes in the stock market.

EXPENSES

Salaries & Benefits	$13,740,600
Legal & Professional Fees	$1,253,500
Membership Expenses	$417,600
Amortization & Depreciation	$305,500
Building Expenses	$218,600
Office Expenses	$163,800
Travel Expenses	$34,400
Litigation Expenses	$128,100
Corporate Insurance	$137,900
Planning & Development	$69,700
Furniture & Equipment Expense	$90,200
Other Administrative Expenses	$41,900
Awareness Events	$26,300
Intern Expenses	$15,600
Fundraising Expenses	$9,100
In Kind Contribution	$7,700
TOTAL EXPENSES	**$16,660,500**

NET INCOME -$23,900

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.

EFF is grateful for the support of these public foundations:

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
California Community Foundation
Swedish Postcode Foundation
The Rose Foundation for Communities and the Environment

EFF Membership Form

The Electronic Frontier Foundation (EFF) is the leading organization defending civil liberties in the digital world. We guard free speech online, champion online privacy, support emerging technologies, defend digital innovators, and work to ensure that our rights and freedoms are enhanced, rather than eroded, as our use of technology grows.

Help us protect digital freedom – **BECOME AN EFF MEMBER TODAY!** Complete this form or go sign up at eff.org/join.
EFF is a U.S. 501(c)(3) nonprofit and donations are tax deductible as allowed by law.

MEMBERSHIP INFORMATION

Name: _____

Email: _____

☐ **Yes!** I would like to join EFF's mailing list for EFF news, events, campaigns, and ways to support digital freedom. ☐ **No thanks**

Phone Number: _____

Street Address: _____

City/State/Province: _____

Postal Code/Country: _____

We respect your privacy!

EFF *does not* sell or exchange donor information. Your phone number will only be used if there's a problem processing your membership.

MEMBERSHIP LEVEL

Silicon: ($25-64)
$ _____
☐ Stickers

Copper: ($65-99)
$ _____
☐ Shirt

Gold: ($100-249)
$ _____
Choose one:
☐ Shirt
☐ Hat

Titanium: ($250-499)
$ _____
Choose one:
☐ Hoodie
☐ Stickers, shirt, & hat

Rare Earths ($500-999)
$ _____
Choose one:
☐ Hoodie
☐ Stickers, shirt, & hat

Guardian ($1000+)
$ _____
☐ Shirt, hat, hoodie, metal membership card

SHIRT/HOODIE SIZE:

☐ XS ☐ S ☐ M ☐ L ☐ XL ☐ 2XL ☐ 3XL

PAYMENT INFORMATION

Credit Card #: _____

Expiration Date: _____

Signature: _____

You may also pay via cash, personal check, traveler's check, or money order. Please make all checks payable to EFF.

Please return membership form to:

ELECTRONIC FRONTIER FOUNDATION

815 Eddy Street
San Francisco, CA 94109
Phone: (415)436-9333
Email: membership@eff.org
Web: eff.org