EFF

2019 ANNUAL REPORT





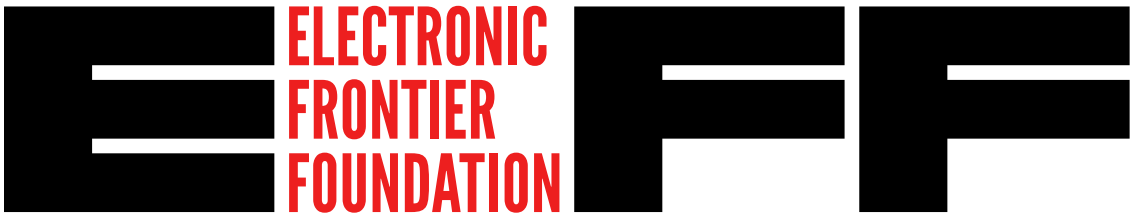

ELECTRONIC
FRONTIER
FOUNDATION

TABLE OF CONTENTS

A WORD FROM OUR EXECUTIVE DIRECTOR

Dear friends,

Looking back over 2019, there were so many unexpected moments when EFF's clear vision and skills were needed, as powerful forces tried to take or bargain away our digital rights. But every time policymakers or private companies or even private equity tried to undermine your rights online, we were there. And every time, you were right there with us. We highlight just a few of our battles in this annual report.

Our most unexpected battle came at the very end of the year. Sometime in November, 2019, we learned that .ORG, the top-level domain of leading nonprofits organizations worldwide was being sold in a shady deal to a private equity firm. We were told that the details of the deal were secret and that the deal was already done. Of course, "unstoppable" and "secret" are fighting words for our team of lawyers and activists. As you will read, we jumped into gear and ultimately helped ensure that the deal was dropped. We often say that EFF is "on patrol" for your rights – the Save .ORG campaign is one of those. We had no advance notice but were able to swiftly pivot to protect the hundreds of millions of people who rely on organizations that have .org domain names.

Our activists and lawyers also helped ignite a nationwide movement of communities standing up to pass bans on police use of facial recognition. Facial recognition identifies and tracks you and those you associate with based upon something you cannot hide and cannot change – your face. The systems are flawed and disproportionately fail on faces of color. Even if the technology could be fixed, this system is just too dangerous to both your Fourth and First Amendment rights. In 2019 we helped pass the first bans of police use of facial recognition systems, working in concert with local activists like those in our Electronic Frontier Alliance.

Our lawyers were busy in court too. They stood up for your privacy against corporate abuse, including taking on telecom giant AT&T for selling cellphone user

location data that was then used by bounty hunters, car dealers, landlords, and even stalkers. The case will help set a standard for damages in privacy cases as well as underscoring the law that prevents your telecommunications provider from selling your location data. And of course that work complements the hard work our legislative team has done to promote smart, comprehensive privacy legislation both at the state and federal levels.

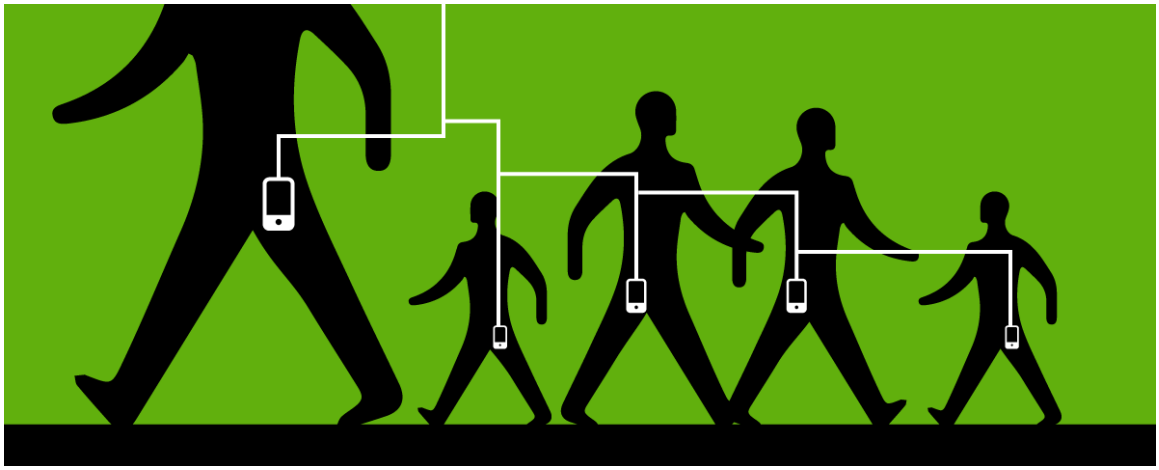
None of this would have been possible without you. We are grateful to our members and supporters for standing on the side of digital civil liberties.

2019 was also a huge year for EFF's work on other fronts. We launched a huge initiative to ensure that stalkerware is appropriately identified as malware by antivirus services, we sued to vindicate the First Amendment rights of vulnerable groups impacted by the new Internet censorship law FOSTA/SESTA, and we expanded our powerful open source tools, including Certbot, which helps millions of people set up and maintain HTTPS security on their websites for free. And of course we continued our work standing up to patent bullies, opposing the NSA's mass spying, building tools and advocating against the tech giants and their surveillance business model, and so much more. Our work spans the globe, supporting groups not only in the U.S. but around the world.

None of this would have been possible without you. We are grateful to our members and supporters for standing on the side of digital civil liberties. Thanks for calling your members of Congress, demanding better policies from the tech companies you rely on, and even helping your relatives install Privacy Badger. Together, we're building a digital future that serves everyone, not just the most powerful people.

Sincerely,

Cindy Cohn, Executive Director



THE SCOTT CASE

Defending the location privacy of AT&T customers

Adam Schwartz
SENIOR STAFF ATTORNEY

When I'm heading out to a doctor's appointment or a protest, I often switch off my phone. I'm aware that our phones are constantly interacting with nearby cell towers, automatically creating a detailed record of where we've been at what times. I've got nothing to hide. But still, I worry about police officers and corporate executives trying to infer my health status or political opinions by snooping on my phone's geolocation.

So I was shocked to learn that AT&T was disclosing its customers' real-time location data to virtually anyone who asked. According to news reports, this sensitive information ended up in the hands of bail bondsmen, bounty hunters, landlords, credit agencies, prison officials, and countless other third parties. A Missouri sheriff even used this AT&T location data to stalk a judge and fellow law enforcement officials.

AT&T risked the privacy and safety of millions of its customers. Naturally, we sued AT&T. EFF represents three AT&T customers, who seek to represent a class of other customers. We want a court to prevent AT&T from violating its customers' location privacy, and to provide damages to remedy the past violations. The case is called Scott v. AT&T.

AT&T violated the Federal Communications Act by disclosing its customers' location data without first telling them and getting their permission. It also violated the California Unfair Competition Law by deceptively claiming it would not do so. Its

invasion of customer privacy further violated California's Constitution, statutes, and common law.

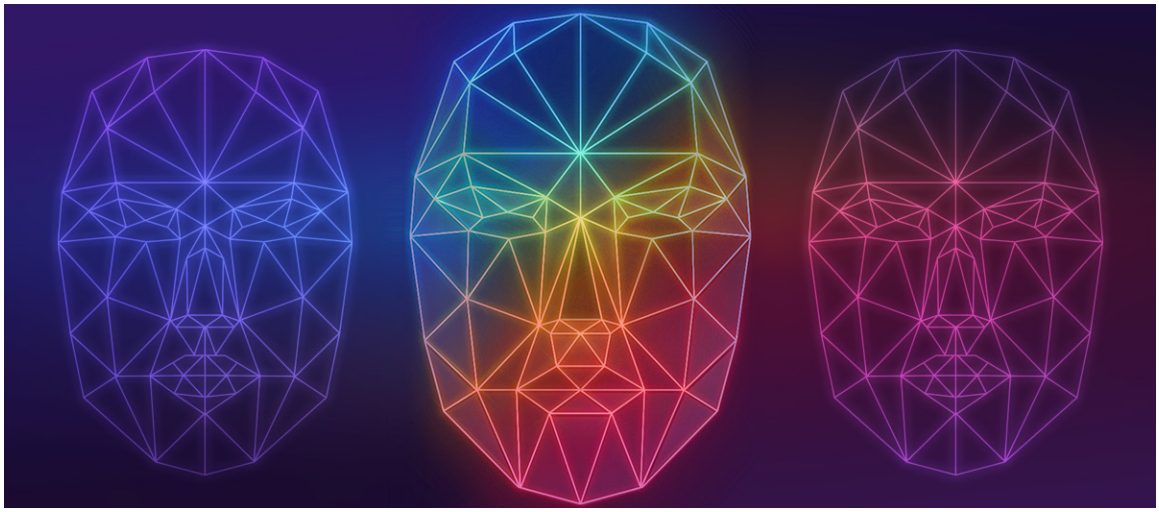
AT&T is one of the hallmark examples of the metastasizing spread of corporate-government surveillance partnerships, in which businesses harvest our personal data and then hand it over to law enforcement, intelligence, immigration, and other government officials. In 2006, we sued AT&T for illegally disclosing customer records to the NSA's dragnet surveillance program. In 2015, we sued the federal government to expose AT&T "Hemisphere" surveillance program, which provides billions of customer phone records to law enforcement agencies across the country. Now we are suing AT&T for allowing law enforcement and prisons (among others) to access customer location data.

AT&T risked the privacy and safety of millions of its customers. Naturally, we sued AT&T.

Our case against AT&T has taken its share of twists and turns, as with many complex class action lawsuits. AT&T tried to divert our clients into binding arbitration, which is an unfair kangaroo court, based on boilerplate legalese that nobody actually reads. We have resisted that gambit, for now. AT&T then moved to dismiss some of our claims, based on its assertion that in 2019 it stopped sharing its customers' location information with third parties known as data aggregators. We look forward to defeating AT&T's latest stratagem, and we are fortunate to have zealous co-counsel at the law firm Hagens Berman Sobol Shapiro LLP.

We practice integrated advocacy at EFF. We try to solve problems, like AT&T's violation of location privacy, with every tool in the toolbox. We blow the whistle when companies put profit over privacy, advocate for laws to prohibit these harms, rally our supporters to contact their legislators, and teach the public to practice surveillance self-defense. As here, we also sue companies like AT&T that violate privacy laws.

We're fighting for a world where we can leave our phones turned on when we go to a protest or any other sensitive place. That world is possible, one lawsuit at a time.



OPPOSING FACIAL RECOGNITION SYSTEMS

Campaigning against a surveillance tool that could quell public participation in society

Nathan 'nash' Sheard

ASSOCIATE DIRECTOR OF COMMUNITY ORGANIZING

My hometown of New York City has a history of protest and racialized surveillance that predates the United States. Growing up Black in the city of Stop & Frisk and Serpico, undue police attention seemed just as much a symptom of puberty as my changing voice and chin hairs. Though my political advocacy career also began in high school, it wasn't until weeks into the fall of 2011 that I began to embrace the power of protest and the political opportunity in organizing.

My work in the Occupy Wall Street movement initially focused on facilitation. Several nights a week, I could be found standing on the steps on the East side of the park guiding General Assemblies that not infrequently numbered in the hundreds of participants. While I'd made the informed choice to embrace a role that came with an elevated risk of targeted repression, many of the participants—be they experienced protesters, academic anarchists, or curious neighbors—could take solace in some degree of anonymity-in-numbers as they blended with the crowd. This anonymity offered visitors the freedom to explore alternative political ideologies without fear that they might be easily identified and targeted for persecution.

These systems can be used to identify people in photos, videos, or in real-time. However, face recognition software is notoriously bad at recognizing women, young people, Black people, and other ethnic minorities.

If the harms of law enforcement use of face recognition technology ended with the chilling effect they present to protesters, that would be sufficient to justify banning its use. But they don't stop there. Law enforcement use of face recognition technology poses a profound threat to personal privacy, political and religious association and expression, and the fundamental freedom to go about our lives without having our movements and associations covertly monitored and analyzed.

What is it?

Face recognition systems provide a means for identifying or verifying the identity of an individual using their face. This identification is accomplished by using algorithms to pick out distinctive details about a person's face. These details, such as the distance between your eyes or your chin's shape, are then converted into a mathematical representation and compared to data already available in the relevant face recognition database.

These systems can be used to identify people in photos, videos, or in real-time. However, face recognition software is notoriously bad at recognizing women, young people, Black people, and other ethnic minorities.

It doesn't have to be this way.

The spread of face surveillance, and all of its privacy and civil rights threats, might seem unstoppable. It isn't. Together with a coalition including Electronic Frontier Alliance (EFA) member Oakland Privacy, the ACLU of Northern California, and the San Francisco Public Defender's Office, we successfully campaigned to pass the nation's first ban on government use of face surveillance. Since the passing of San Francisco's history-making ordinance, we've continued to successfully support the passage of face surveillance bans in the California communities of Oakland and Berkeley, as well as in the Massachusetts cities of Sommerville, Brookline, and Northampton.

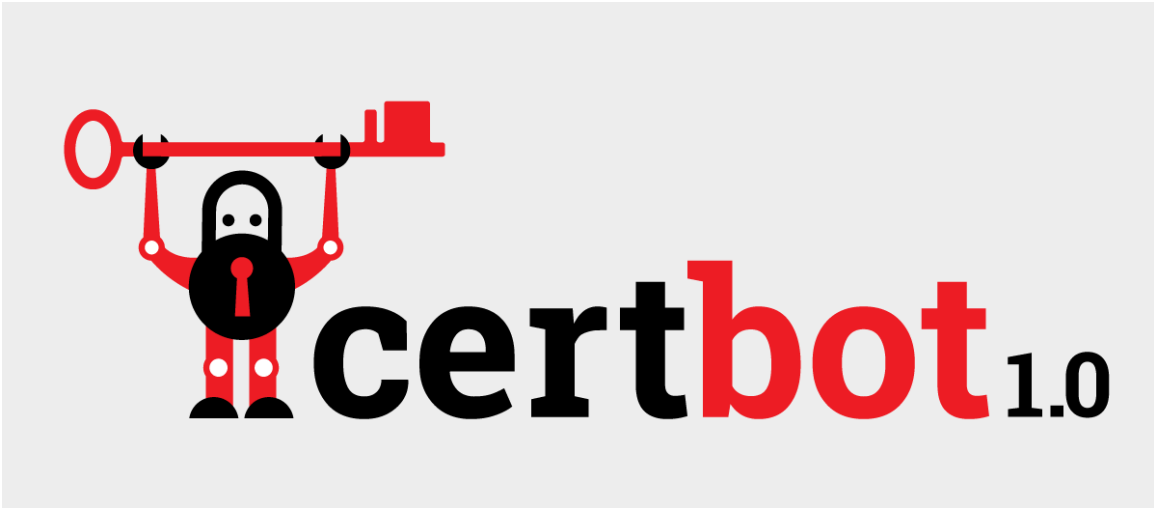
Each of the California ordinances has built on our work supporting the passage of Community Control of Police Surveillance (CCOPS) laws, which give residents

transparency and a voice on the surveillance technology used in their community. In turn, these bans paved the way for the first state-level moratorium restricting use of the technology. In October, in response to advocacy from EFF, our coalition, and our community, Governor Newsom signed A.B. 1215, establishing a three-year moratorium on law enforcement use of facial recognition technology in association with police body-worn cameras and other mobile devices. In addition to protecting all California residents from the transformation of a tool promising increased transparency into a weapon of mass surveillance, A.B. 1215 also ended one of the largest, longest-running, and most controversial face surveillance programs in the country.

In November, building on these successes and supporting communities across the country working to adopt similar protections, we launched our About Face campaign. At aboutfacenow.org, visitors and co-conspirators can find a one-pager for informing their community and legislators, guidance on engaging traditional media and developing a social media strategy, and a model bill that can be adapted to the needs and concerns of their community.

Working with local allies, petitions gathered through the About Face campaign will be delivered to local lawmakers, making it clear that our privacy and security—and our neighbors' privacy and safety—must be protected. Since May, we've proven that the daunting juggernaut of government surveillance can be stopped through community organizing and coordinated engagement.

The stakes are all too high to rest on our laurels now. We must continue to fight and win. Together.



ENCRYPTING THE WEB WITH LET'S ENCRYPT AND CERTBOT 1.0

Building free tools that protect privacy and security by automatically enabling HTTPS

Brad Warren
SENIOR SOFTWARE ARCHITECT

I started working at EFF in the summer of 2015 as a summer internship and I was planning on starting graduate school in the fall. I was interested in computer security and privacy and I was excited to spend the summer in San Francisco at EFF. I appreciated the work EFF does and they were helping build what would become Let's Encrypt and Certbot which seemed radical, new, and exciting to me. I certainly did not expect that I would choose not to attend graduate school, take a full time job at EFF, and watch Let's Encrypt and Certbot grow the way they have over the past 5 years.

Before Let's Encrypt and Certbot launched back in 2015, only 40% of web traffic was encrypted. Most communication with websites used non-secure HTTP which leaves users vulnerable to eavesdropping, content injection, and cookie stealing, which can be used to take over their online accounts. The solution to these problems is for websites to support the protocol HTTPS which ensures encryption, authentication, and more generally offers significant security and privacy benefits to the site's users.

Despite these benefits, many website operators historically chose not to support HTTPS. One of the main reasons people would cite for this was that setting up and maintaining HTTPS was just too difficult. To use HTTPS, the website operator needs to obtain a certificate from a certificate authority which was usually a cumbersome, bureaucratic process that could cost hundreds of dollars. Once they had a certificate, they had to configure their site to use it, set other aspects of their HTTPS configuration such as the cryptographic algorithms their server should use, and then maintain this setup over time. This ongoing maintenance is not negligible as the certificates used for HTTPS expire and the best practices for maintaining an HTTPS site change over time as new security vulnerabilities are found and new protocols are developed. All of this discouraged many people from setting up HTTPS on their website at all.

Why should offering HTTPS be so difficult and why should website operators have to pay for a certificate? If we could make the process free and automated, maybe more website operators would choose to support HTTPS.

The aim of Let's Encrypt and Certbot is to solve these problems. Why should offering HTTPS be so difficult and why should website operators have to pay for a certificate? If we could make the process free and automated, maybe more website operators would choose to support HTTPS. I think that's exactly what happened.

In the end of 2015, EFF helped launch Let's Encrypt and Certbot which are free and open source tools that automate the process of configuring and maintaining HTTPS support on a website. Let's Encrypt is a certificate authority that is now run for the public's benefit through the Internet Security Research Group (ISRG). Certbot is a tool maintained by EFF that individuals can run on their server to obtain a certificate from Let's Encrypt and configure their site to use it. By using Let's Encrypt and Certbot, people can set up HTTPS on a website in less than 30 seconds and after they've done so, Certbot will maintain the configuration going forward automatically. Best of all, the certificates are completely free.

The projects have grown significantly since they were first released. Let's Encrypt has become one of the world's largest certificate authorities and Certbot is the tool most commonly installed by users to obtain a Let's Encrypt certificate. Certbot currently has nearly 2.5 million installations that are maintaining HTTPS support for over 20 million websites.

At the end of this year we released Certbot version 1.0 which formally marks the end of Certbot's beta phase and signals the maturity of the project. Certbot 1.0 is a significant milestone and is the culmination of the work done over the past few years by myself, my coworkers at EFF, and hundreds of open source contributors from around the world.

The adoption of HTTPS worldwide has changed a lot since the projects launched as well. Now over 80% of web traffic is encrypted using HTTPS which is a dramatic change from the 40% seen just 5 years ago. It has been really rewarding for me personally to see the use of encryption on the web increase worldwide partially due to our efforts. I am excited to continue to work with my coworkers at EFF and the larger open source community to improve Certbot. We can make the tool more reliable, easier to use, and improve the security and features it offers as we continue to push for a more secure and private web.

FIGHTING TO SAVE .ORG

Defending the public interest Internet against private equity takeover

Cara Gagliano
STAFF ATTORNEY

As an attorney on EFF's IP team, much of my work focuses on how claims of trademark or copyright infringement can all too easily be abused to stifle speech that someone doesn't like. Nearly every week I hear from Internet users who've had content removed or accounts disabled because of a baseless infringement claim.

Online speech depends on several different layers of intermediaries to reach its audience, from ISPs to domain registries to web hosting services, to name just a few examples. If any of these intermediaries—or "free speech weak links"—succumbs to a takedown demand, your speech can disappear from the Internet.

This year, we took on a major campaign to stop a change that would allow for, and likely lead to, increased censorship at one of these choke points: website domain registries. A domain suspension is a drastic measure that not only takes the owner's website offline but also breaks any email accounts or apps associated with the domain name.

In July, we challenged a decision by ICANN, the organization that oversees the domain name system, to change the terms of its contract with Public Interest Registry

(PIR), the nonprofit that's managed the .ORG domain since 2002. These changes weakened protections for .ORG domain holders against claims of cybersquatting and gave PIR express permission to regulate the use of .ORG domains—including website content—in the name of protecting "legal rights of third parties." Our challenge focused on the dangers of making it easier to censor websites, especially given the importance of .ORG to noncommercial users working in the public interest.

We had reason to fear increased censorship attempts at the registry level. At least one domain registry, co-founded by PIR's current CEO, struck a deal with the Motion Picture Association under which it agreed to suspend domains based on accusations of copyright infringement from MPA members, with no court order or right to appeal. In 2017, PIR announced plans for a similar copyright enforcement scheme for .ORG, but scrapped it after public pressure from EFF and others. Outside of the copyright context, pharmaceutical industry groups have pressured registries to take down websites that provide information about how to legally import medication from abroad.

.ORG is a lifeline to their clients and the public; if a domain name is suspended or service is disrupted, that impairs the important work they do.

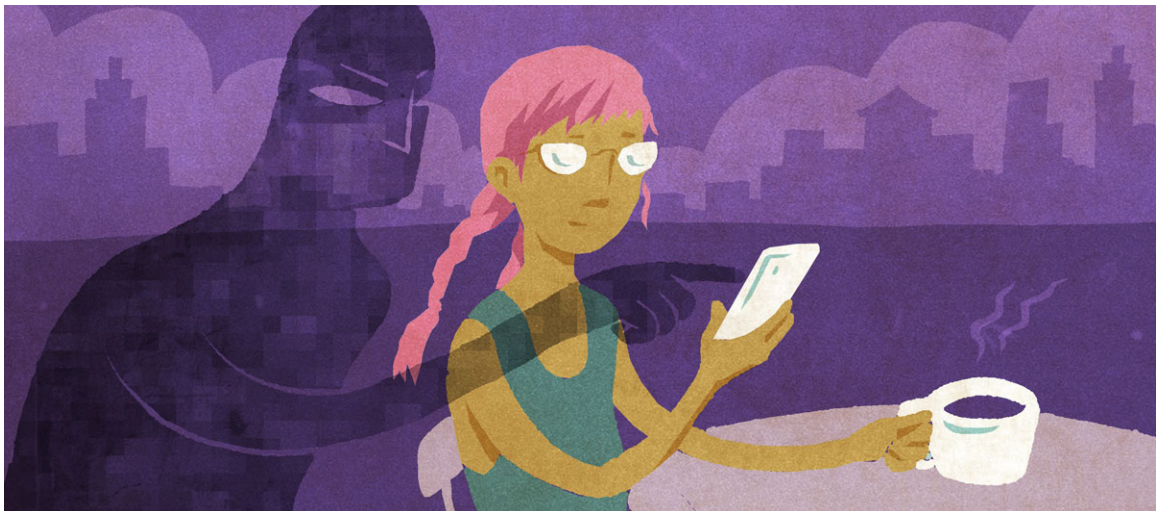
By shining a spotlight on this issue and making sure Internet users and public interest groups knew what they stood to lose, we were able to empower them to speak up for themselves and make sure PIR and ICANN knew they were watching.

Then one morning in November, as my colleagues and I were in the midst of preparing a final appeal to ICANN, we got some disturbing news: a private equity firm called Ethos Capital had just struck a deal to buy PIR from its nonprofit parent organization, the Internet Society (ISOC). Our fears about censorship of .ORG domains instantly became more acute. Before, we at least had some reason for optimism that PIR would continue to serve the interests of users in keeping with its nonprofit mission. The prospect of the registry being taken over by a private equity firm with a need to recoup its investment made censorship-for-profit seem more and more likely.

But the deal wasn't done yet, and we quickly got to work to stop it from going forward. Together with allies at NTEN and the National Council of Nonprofits, we wrote an open letter to ISOC urging it to stop the sale. Within a week of ISOC's announcements, we had 26 organizations signed on to the letter, from the American Alliance of Museums to the YMCA. Less than a month later, that number had grown to nearly 500 organizations, along with signatures from over 18,000 individuals. We also shared the letter with ICANN, which had the power to veto the takeover, and continued our advocacy there.

The outpouring of support from all corners of the public interest community was a perfect demonstration of why EFF's advocacy work is so important. Internet governance issues don't usually get much public attention, but this was an issue that had serious potential consequences for the thousands of organizations that rely on the .ORG domain to establish an online presence and provide vital services. .ORG is a lifeline to their clients and the public; if a domain name is suspended or service is disrupted, that impairs the important work they do.

By shining a spotlight on this issue and making sure Internet users and public interest groups knew what they stood to lose, we were able to empower them to speak up for themselves and make sure PIR and ICANN knew they were watching.



TAKING ON STALKERWARE

Working together to help stop tech-enabled intimate partner abuse

Eva Galperin
DIRECTOR OF CYBERSECURITY

Every day, I hear from victims of intimate partner abuse who are concerned about the security of their digital devices. Our digital devices contain a wealth of extremely personal information, which makes them tempting targets for stalkers, harassers, and abusive partners as well as governments and law enforcement. The close relationship between victims and their abusers makes it challenging to disentangle their digital lives. Frequently, partners share devices, share passwords, know enough about each other to answer login reset security questions, and have access to information through each others' friends and family. EFF's Surveillance Self Defense guide contains a wealth of advice about how to lock down your accounts, including using a password manager and enabling 2-factor authentication, but some of the worst and most persistent cases of abuse that came to me involved a class of apps commonly called "stalkerware."

Stalkerware is a category of commercially-available applications that can be surreptitiously installed onto a device and covertly send data from that device to the user. These applications are sometimes sold as tools for monitoring children or elderly parents, or "bossware" for keeping tabs on the activities of an increasingly-remote workforce. But they are also marketed explicitly as tools of abuse for "catching a cheating spouse."

Not all apps that allow remote monitoring of devices are stalkerware. The essential element is deception. These apps are designed to fool the user into thinking they are not being monitored.

Reports by members of the coalition, including Kaspersky and Malwarebytes, indicate that detection of stalkerware by their products has increased by more than 30% since they have begun tracking it. The anti-virus companies working with us are getting better at detecting stalkerware on your device, even as the use of stalkerware becomes more common.

In 2019, I spoke at TEDWomen about this class of applications and what can be done to limit their effectiveness, a talk that has been viewed by more than 2 million people. I also helped EFF to become a founding member of the Coalition Against Stalkerware, an organization that works to facilitate communications between those working to combat domestic violence and the information security community. The coalition continues to grow rapidly, bringing in new members. The coalition has produced a working definition of stalkerware, so that it can be better identified and studied, and facilitated sample-sharing among anti-virus companies in order to increase the detection of stalkerware by their products. Reports by members of the coalition, including Kaspersky and Malwarebytes, indicate that detection of stalkerware by their products has increased by more than 30% since they have begun tracking it. The anti-virus companies working with us are getting better at detecting stalkerware on your device, even as the use of stalkerware becomes more common.

EFF has advocated for Apple and Google to keep these applications out of their respective app stores, where such apps are already in violation of both companies' policies.

There is still considerable work left to do, from raising awareness of stalkerware to changing the norms around the use of these tools in an industry that has, up until recently, turned a blind eye to this kind of intimate partner abuse. I'm glad to see we are already making a huge difference against these deceptive and dangerous apps, with real impact for the victims of intimate partner abuse.

THE WOODHULL CASE

Defending the First Amendment rights of online speakers and challenging FOSTA

Aaron Mackey
STAFF ATTORNEY

When I think about my work at EFF fighting for Internet users, two users in particular come to mind: Alex Andrews and Eric Koszyk.

EFF is part of the legal team representing Alex, Eric, the Woodhull Freedom Foundation, Human Rights Watch, and the Internet Archive in a constitutional challenge to the Allow States and Victims to Fight Online Sex Trafficking Act, or FOSTA, a broad and harmful online censorship law passed in 2018.

FOSTA violates the First Amendment in multiple respects: it contains vague language that could sweep up protected speech, it targets any online discussions remotely concerning sex work, and it removes important legal protections for online platforms that host user-generated content. Under FOSTA's crushing liability, numerous online services censored their users' speech or shut down entirely.

The plaintiffs' challenge to FOSTA presses on today, thanks in large part to Alex and Eric. A federal appellate court revived the case in January, ruling that Alex and Eric had shown how FOSTA had injured them—in legal jargon, that they had standing. The decision reversed a lower court's 2018 ruling dismissing the case.

The appellate court recognized what Alex and Eric had said since Congress passed FOSTA: the law harmed both of them, as well as the large and diverse group of Internet users they represent.

For Alex, FOSTA has jeopardized her ability to maintain an online platform created to help sex workers. Alex is a sex worker advocate and ally who is on the board of directors of the Sex Workers Outreach Project USA. In 2015 she collaborated with other advocates and sex workers to create an online review website called Rate That Rescue.

Rate That Rescue works like many other online review website: it lets users share information about the growing number of organizations whose stated missions include assisting or rescuing sex workers. And much like some of the Internet's most popular platforms, Rate That Rescue grew into something else when its users started reviewing a variety of other services that they rely on, such as Twitter, and payment processors such as PayPal. It has become a go-to platform to share practical and important information on a variety of topics, including healthcare and housing.

I continue to fight for Alex and Eric because I want the Internet to continue to be a place for all Internet users to organize, to find community, to build their business, or to seek the social change they desire.

FOSTA imperils Rate That Rescue's ability to serve as a forum for the sex worker community. Rate That Rescue was explicitly designed to support sex workers and make their lives easier. Yet because FOSTA creates new federal criminal liability for any online services that promotes or facilitates prostitution, the review site's very existence could be considered illegal. And because FOSTA repealed legal protections for online platforms, it's possible that Rate That Rescue could be liable for specific content its users post that could be construed as promoting or facilitating prostitution.

For Eric, FOSTA has taken away his ability to use the Internet to make a living. Eric is a licensed massage therapist who for more than a decade advertised his business on Craigslist. Prior to FOSTA, Eric's use of Craigslist was an Internet success story: advertising on Craigslist allowed him to decide when and how often he worked, flexibility he relished through cross-country moves, putting himself through graduate

school, and caring for his small children. Craigslist's ubiquity nonetheless allowed Eric to work frequently enough to supplement his family's income.

In the days after Congress passed FOSTA, Craigslist took down Eric's most recent ad and shut down the section of its site that allowed massage therapists to advertise. Eric has not been able to advertise on Craigslist since. In a public statement about FOSTA, Craigslist said it took down certain parts of its website because the law created too much risk to host certain user-generated content.

Eric's business has never recovered. Despite looking for new platforms to advertise on, and even setting up his own personal website, Eric has not been able to connect with the same audience of customers he previously found on Craigslist. His business' revenue the last few years is about half of what he made in 2017.

Alex and Eric's experiences show FOSTA's far reaching and comprehensive censorship. The law has made the Internet less open, and less free for Alex, Eric, and so many other Internet users.

I continue to fight for Alex and Eric because I want the Internet to continue to be a place for all Internet users to organize, to find community, to build their business, or to seek the social change they desire. After all, EFF will always fight for the users.

FINANCIALS

Contributions from more than 30,000 dues-paying members from around the world form the backbone of the Electronic Frontier Foundation's financial support.

EFF MEMBERS MAKE A BETTER DIGITAL FUTURE POSSIBLE

Aaron Jue
DEVELOPMENT DIRECTOR

Faced with undeniably tough times for the world and for technology users, EFF and its supporters are resilient. Today over 35,000 EFF donors stand together to protect crucial rights and freedoms online. We are proud that the majority of EFF's funding comes from individuals, and 74% of that funding consists of donations under $10,000. Direct contributions from businesses of any size comprised only 6% of our total public support in fiscal year 2019. Find full financial details in the following chart.

EFF has received a top four-star rating—and 100/100 for transparency and accountability—from the nonprofit rating website Charity Navigator for seven years in a row. This rating means that EFF "exceeds industry standards and outperforms most charities in [our] cause." For fiscal year 2019, we put 74% of all funds toward programs. In other words, the majority of donations went directly toward EFF's work including litigation, legislative analyses, and development of free privacy-enhancing technology including Certbot and Privacy Badger.

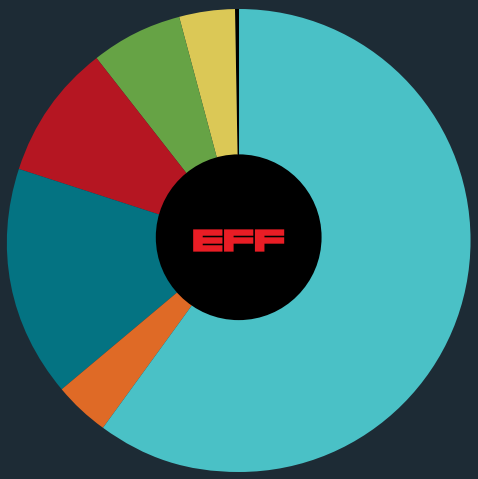
We care deeply about honoring your generosity and making the most out of every donation. The bottom line of this year's financial report is that EFF has continued to keep its fundraising and administrative costs low so we can focus on what matters most: ensuring that the Internet continues to connect, inspire, and uplift all of us. Thank you for believing in EFF's mission and for allowing us to keep fighting.

For your online rights,

Aaron Jue

EFF Director of Member Engagement

FY 2019 PUBLIC SUPPORT



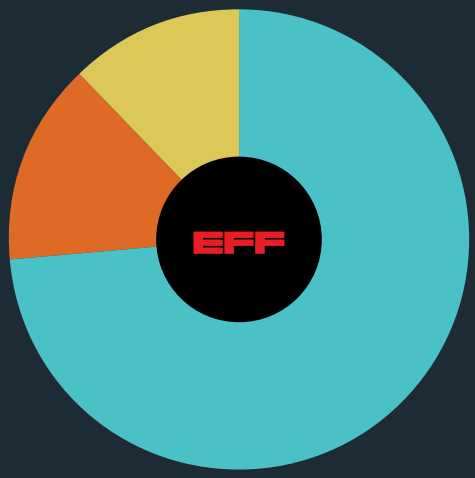
PUBLIC SUPPORT

Individual	$ 7,950,942
Individual through Foundation	513,958
Foundation	2,132,492
Employee & Customer-Directed Gifts*	1,236,206
Corporate	855,912
Cy Pres	507,443
In-kind Legal Services	15,848
Total Public Support	**$13,212,801**

EXPENSES

Program	$ 10,678,031
Administrative	2,048,208
Fundraising	1,764,024
Total Expenses	**$14,490,263**

FY 2019 EXPENSES



INCOME

PUBLIC SUPPORT

Individual Contributions	
Individual Contributions over $50,000	$1,125,546
Individual Contributions $10,000-$50,000	$910,883
Individual Contributions under $10,000	$5,914,513
Total Individual Contributions	$7,950,942
Individual Contributions through Foundations	
Individual Contributions through Foundations Over $50,000	$345,000
Individual Contributions through Foundations Up to $50,000	$168,958
Total Individual Contributions through Foundations	$513,958
Foundation Grants	$2,132,492
Cy Pres Awards	
Ashley Madison Customer Data Security Breach Litigation	$28,828
Ossola, et al. v. American Express Company, et al.	$84,467
Cottage health Settlement	$239,170
Opperman et al. v. Kong Technologies Inc. et al	$154,977
Total Cy Pres Awards	$507,443
Corporate Contributions	
Employee and Customer-Directed Gifts*	$1,236,206
Other Corporate Contributions	$855,912
Total Corporate Contributions	$2,092,118
In-kind Legal Services	$15,848
TOTAL PUBLIC SUPPORT	**$13,212,801**

REVENUE

Net Investment Income	$1,502,216
Attorneys' Fees Awarded	$204,957
EFF Event Income, net of expenses	-$10,214
Miscellaneous	$133,250
TOTAL REVENUE	**$1,830,210**

TOTAL SUPPORT AND REVENUE $15,043,011

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

EXPENSES

Salaries & Benefits	$11,808,659
Legal & Professional Fees	$681,474
Membership Expenses	$533,080
Amortization & Depreciation	$277,078
Building Expenses	$216,463
Planning & Development	$211,521
Travel Expenses	$183,033
Office Expenses	$160,594
Corporate Insurance	$119,646
Litigation Expenses	$116,820
Furniture & Equipment Expense	$104,815
Awareness Events	$26,751
Other Administrative Expenses	$24,644
Intern Expenses	$23,636
Fundraising Expenses	$2,049
TOTAL EXPENSES	**$14,490,263**

NET INCOME $552,748

THANK YOU

For 30 years, members have joined EFF to defend freedom of expression, protect encryption, battle with patent trolls, stand up for the freedom to tinker, and so much more. Because of you, our values live in the law, in code, and in the way we defeat threats and champion progress. Whether in the courts, in the streets, or appearing before Congress, we're proud and humbled by our members' passion for freedom and for the future that ought to be. Thank you.

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)
$ _____
- ☐ Stickers
- ☐ Shirt

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

Titanium: ($250-499)
$ _____
- ☐ Stickers
- ☐ Shirt
- ☐ Hat
- ☐ Hoodie
- ☐ Stickesr, shirt, & hat

Rare Earths ($500-999)
$ _____
- ☐ Stickers
- ☐ Shirt
- ☐ Hat
- ☐ Hoodie
- ☐ Stickers, shirt, & hat

Major Donor ($1000+)
$ _____
- ☐ Stickers
- ☐ Shirt
- ☐ Hat
- ☐ Hoodie
- ☐ Stickers, shirt, & hat

SHIRT/HOODIE SIZE:

Classic Fit: ☐ XS ☐ S ☐ M ☐ L ☐ XL ☐ 2XL ☐ 3XL **Slim Fit:** ☐ XS ☐ S ☐ M ☐ L ☐ XL

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