

2017

ANNUAL REPORT





Electronic Frontier Foundation was founded in 1990 to protect the rights of technology users, a mission that expands dramatically as digital devices and networks transform modern life and culture. With nearly 40,000 dues-paying members around the world and a social media reach of well over 1 million followers across different social networks, EFF engages directly with digital users worldwide and provides leadership on cutting-edge issues of free expression, privacy, and human rights.

Our annual report features reflections from several EFF staff members about some of our most significant efforts, as well as financial information for the fiscal year ending June 2017.



TABLE OF CONTENTS

A Word from Our Executive Director, Cindy Cohn.....	4
Milestones in Digital Rights	6
Privacy at the Border.....	7
Alasaad v. Nielsen	8
Slippery Slope of Surveillance Tech	10
Protecting Innovation.....	12
Net Neutrality	13
Saved by Alice.....	15
Strengthening Our Community	17
Security Education Companion	18
Offline.....	21
Financial Report.....	23
Thank You	26
Become an EFF Member Today.....	27



A WORD FROM OUR EXECUTIVE DIRECTOR

Dear friend,

The pace of the news last year felt unprecedented, but it wasn't EFF's first rodeo. Our team of lawyers, technologists, and activists have been poised and ready at the fore-front of every critical battle in digital rights for 28 years and counting. In the following report, you will see why I have immense pride in our team. The challenges we navigated together demonstrated new boundaries of their intelligence, kindness, energy, and grit.

Your support transformed what could have been a difficult year into one that ignited powerful and effective change.

We have never been busier, but we aren't doing it alone. We partnered with other organizations in litigation, worked with hundreds of volunteer coders on our open source technology projects, and brought together more grassroots organizations through the Electronic Frontier Alliance. Most importantly, we felt the support of thousands of EFF members—close to 40,000 of you. The mutual respect shared by the EFF staff and EFF members is unique and we can't thank you enough. Your support transformed what could have been a difficult year into one that ignited powerful and effective change.

In 2017, technology played a role in nearly every public issue and conversation. Whether battling invasive searches of our devices at the U.S. border, fighting patent trolls, or training the next generation of security educators, we remained on the front-lines. We've continued to shine a light on secret governmental programs and pushed for more transparency for private systems that hold our communications and data. Our mission has always extended internationally, and last year we made critical efforts to release imprisoned bloggers and technologists around the world. EFF continues to serve as a fierce watchdog for your rights of free expression and freedom of association by rallying support for the open Internet. We have won net neutrality protections before, and we can win again.

This report is just the tip of the iceberg of our work last year, but it exemplifies the values we champion: freedom, privacy, and innovation. These pillars stand on the foundation of public service we laid down at the very beginning of the technological frontier. Going forward, EFF will continue to grow and build an even stronger ecosystem of projects and tools. Our bricks are strong encryption and security practices, transparent and accountable technologies, laws that encourage creativity and respect the user, and a community of empowered technology users who stand with us—people like you.

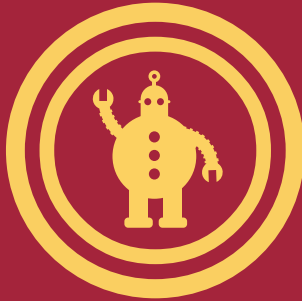
Thank you.

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

Cindy Cohn, Executive Director

Build with us. [Donate to EFF.](#)

MILESTONES IN DIGITAL RIGHTS



TECH

We brought together engineers and Internet pioneers to help restore net neutrality protections.

We released Privacy Badger 2.0 which currently has over 2 million active users.

We broadened Internet encryption through HTTPS Everywhere and Certbot.

We debuted our new, more accessible website which now features a Tech Tools section featuring projects like Panopticlick and Surveillance Self Defense.



ACTIVISM

We launched the Security Education Companion, empowering new audiences to train their communities.

We expanded Who Has Your Back with our partners globally.

Onlinecensorship.org launched a resource toolkit for journalists and expanded its reach on content moderation policy.

The Electronic Frontier Alliance grew to include 81 grassroots organizations in 27 states.



LAW

We battled against illegal search and seizure of digital devices.

We fought against industry groups who were abusing copyright law to control public access to laws and standards.

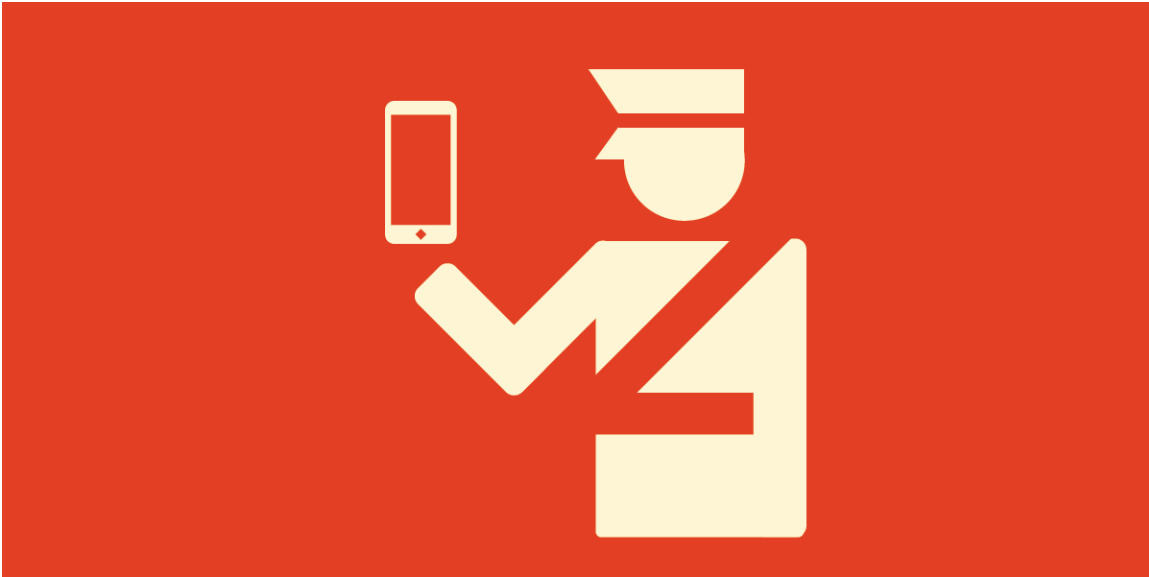
We exposed secretive government spying and surveillance programs.

With 59 amicus briefs, we weighed in on free speech and privacy issues, advocated for fair use and consumer rights, and championed the public interest in many other critical battles.



PRIVACY AT THE BORDER

The law trails behind our evolving use of digital technology, opening the door to unprecedented invasions of privacy. EFF fights hard to keep ordinary people safe from warrantless searches of their digital devices at our airports and land crossings and increased biometric surveillance.



Sophia Cope

SENIOR STAFF ATTORNEY

Alasaad v. Nielsen

Our groundbreaking lawsuit challenges invasive border searches of electronic devices.

When I was living in Washington, D.C.—a very international city—I remember more and more reports of border agents freely searching travelers’ cell phones, laptops, and other electronic devices at international airports and land crossings. As a civil liberties lawyer, that seemed like an egregious violation of privacy and free speech rights. As a frequent traveler overseas—to see family, for work, and for vacation—it was easy to imagine how violated I would feel by a government search of my smartphone.

When I interviewed at EFF in 2014, I enthusiastically declared that I wanted to work on border searches. It’s been four years since I started working here, I’m proud to say that this issue is a core part of my docket and EFF’s constitutional work.

We’ve filed several amicus briefs in appellate courts, written numerous blog posts, published a technical and legal guide for travelers, pushed for more protective federal legislation, and in September 2017, we filed a lawsuit against the Department of Homeland Security—one of our biggest projects yet.

In *Alasaad v. Nielsen*, we are representing 11 clients from all walks of life who had their electronic devices searched—some, multiple times—by officers from U.S. Customs and Border Protection (CBP) and/or Immigration and Customs Enforcement (ICE). We’re

partnering with the ACLU to challenge these unconstitutional intrusions into our clients' private lives—and those of all travelers to the United States. The plaintiffs include a NASA engineer, a military veteran, a business owner, students, journalists, and an artist. Several are Muslims or people of color. None were accused of a crime.

There is no question that police officers working in the interior of the country generally have to follow strict rules under the Fourth and First Amendments to safeguard constitutional rights to privacy and free speech. The problem is that at the border, Supreme Court precedent has granted border agents essentially unfettered access to personal belongings. The Court reasoned, in decades-old cases, that travelers' privacy interests in luggage are low, and the government's interests in border security—for example, intercepting contraband such as drugs or weapons—are high.

But the Supreme Court's historical reasoning doesn't work when it comes to cell phones, laptops, or tablets. Travelers' privacy interests in the vast amounts of digital data their electronic devices contain are unprecedented: a suitcase can't hold what a 256-gigabyte smartphone can.

The vast amounts of personal data we generate on a device—our emails; text messages; voicemails; photos and videos; social media, shopping, transportation and other apps; contacts; calendar entries; and web browsing histories—paint a near-complete picture of our lives. That data can reveal an individual's political affiliation, religious beliefs and practices, sexual and romantic life, financial status, health conditions, and family and professional associations—much more so than what a typical suitcase, purse, or backpack ever could. EFF argues that no border agent should be able to access such sensitive personal information without first getting a warrant from a judge based on probable cause.

We're heartened by the Supreme Court's more recent decisions recognizing the immense privacy interests people have in their cell phones. In *Riley v. California* (2014), the court held that the police need a warrant before searching the cell phone of someone they arrest. And in *Carpenter v. U.S.* (2018), the court held that the government needs a warrant to access a person's cell phone location history.

Our constitutional rights don't end in the digital world, and they shouldn't end at the border.

I'm happy to report that we successfully fought the government's attempt to dismiss our complaint in *Alasaad*. We're now on to discovery, the fact-finding part of the case that will help us prove our legal arguments. Our constitutional rights don't end in the digital world, and they shouldn't end at the border. Together, we need to push privacy laws into the 21st century. With your help, I'm optimistic that EFF will help us get there.

Keep border agents out of your personal data. [Donate to EFF.](#)



Jennifer Lynch
SENIOR STAFF ATTORNEY

Slippery Slope of Surveillance Tech

The increased use of biometric surveillance of travelers threatens privacy at mass scale.

My son is nine. He's been traveling on planes since he was only a few months old, and now that he's older, we've started to travel out of the country together. My goal is to take him to a different country every year for as long as I can (or as long as I can afford it). But traveling internationally means he needs his own passport. It also means the federal government now has an excuse to collect and track him with his biometric data. As a mom, this really worries me.

In 2016 and 2017, the Department of Homeland Security (DHS) ramped up its plans to collect face images and iris scans from travelers on a nationwide scale. In pilot programs in Georgia and Arizona in 2016, Customs and Border Protection (CBP) used face recognition to capture pictures of all travelers boarding a flight out of the country and walking across a U.S. land border and compared those pictures to previously recorded photos from passports, visas, and "other DHS encounters." But what began as a pilot program with the stated goal of using face recognition to screen foreign travelers morphed, without congressional authorization, into screening of U.S. citizens, too. The agency plans to roll out the program to all international flights and border crossings, and will retain photos of U.S. citizens and lawful permanent residents for two weeks and information about their travel for 15 years. It retains data on "non-immigrant aliens" for 75 years.

This won't be limited to international flights. In 2017, CBP and TSA announced plans to vastly expand this biometric screening and tracking program to cover domestic flights as well. The agencies want to create a "biometric" pathway that would use face recognition to track all travelers—including U.S. citizens—through airports from check-in, through security, into airport lounges, and onto flights. And they want to partner with commercial airlines and airports to roll this out. DHS has said that the only way we can ensure that our biometric data isn't collected when we travel is to "refrain from traveling."

DHS is laying the groundwork for a vast surveillance and tracking network that could impact all of us for years to come.

These programs threaten privacy on a mass scale. By collecting and retaining face recognition data and partnering with private companies that face no restrictions on data sharing, DHS is laying the groundwork for a vast surveillance and tracking network that could impact all of us for years to come. These programs also allow DHS to build a database large enough to identify and track all people in public places, without their knowledge—not just in places the agency oversees, like airports, but anywhere there are cameras.

Police are already abusing their access to facial recognition by using it on public streets and at political protests. During the 2015 protests surrounding the death of Freddie Gray while in police custody, Baltimore Police ran social media photos against a face recognition database to identify protesters and arrest them. Many have proposed linking face recognition to police body-worn cameras so that officers can identify people in real-time.

I don't want my son to grow up in a world like this. I work at EFF so I can defend his and everyone else's constitutionally-protected right to privacy, right to travel, and right to anonymous association with others. With my colleagues at EFF, I push lawmakers, agencies, and the courts to restrict the government's ability to use surveillance technologies like face recognition.

Don't Panic. [Donate to EFF.](#)



PROTECTING INNOVATION

EFF defends fair use, open access, net neutrality, and your freedom to tinker. Internet giants should not get to decide what content you have access to, nor should trolls get to abuse outdated copyright laws.



Ernesto Falcon

LEGISLATIVE COUNSEL

Net Neutrality

Schooling the FCC on how the Internet works.

Technical facts can be instrumental to legal decisions. The FCC’s vote to repeal the 2015 Open Internet Order was based on a flawed understanding of how the Internet works and which entities provide which services. In order for its legal conclusions to hold water, the FCC had to mindfully misinterpret what is and is not broadband Internet access.

An explanation of the Internet’s architecture became EFF’s central thrust to overturn the FCC’s decision to abandon popular net neutrality rules.

The origins of this approach date back to May 2017 when the agency invited public comment on its proposal to eliminate net neutrality and privacy protections for broadband subscribers. I was sitting in my office reading through the text when our senior technologist Jeremy Gillula came by, a bit flummoxed. “Why does the FCC think that broadband companies do social media?”

“Well, because they have to argue how they are not telecommunications services, but rather are information services that process services,” I responded. “They have to make that argument in order to legally justify the repeal.”

“But it is just completely wrong,” Jeremy said while shaking his head.

This is the core of EFF’s strength: we shine when we work together. By bringing together the expertise of engineers, lawyers, and activists, one group’s strengths can cross-pollinate with

another's. Jeremy noticed a critical weakness in the FCC's argument and I was able to explain the legal ramifications of attacking that weakness. There was one caveat—based on Supreme Court precedent where the agency gets deference from the courts—to the FCC's ability to reclassify broadband and void net neutrality rules: if it could be shown that the agency was so wildly wrong on the facts, a federal court might throw out the decision on the grounds that it was an unreasonable act (arbitrary and capricious in legal jargon).

To get that result, we needed to have the FCC's record contain an authoritative document that states categorically technical facts about the history, structure, and evolving nature of the Internet. If we could show that the FCC's misinterpretation was fundamentally wrong, then we might have a chance. I asked him, "Would other engineers read what the FCC produced and come to the same conclusion as you?"

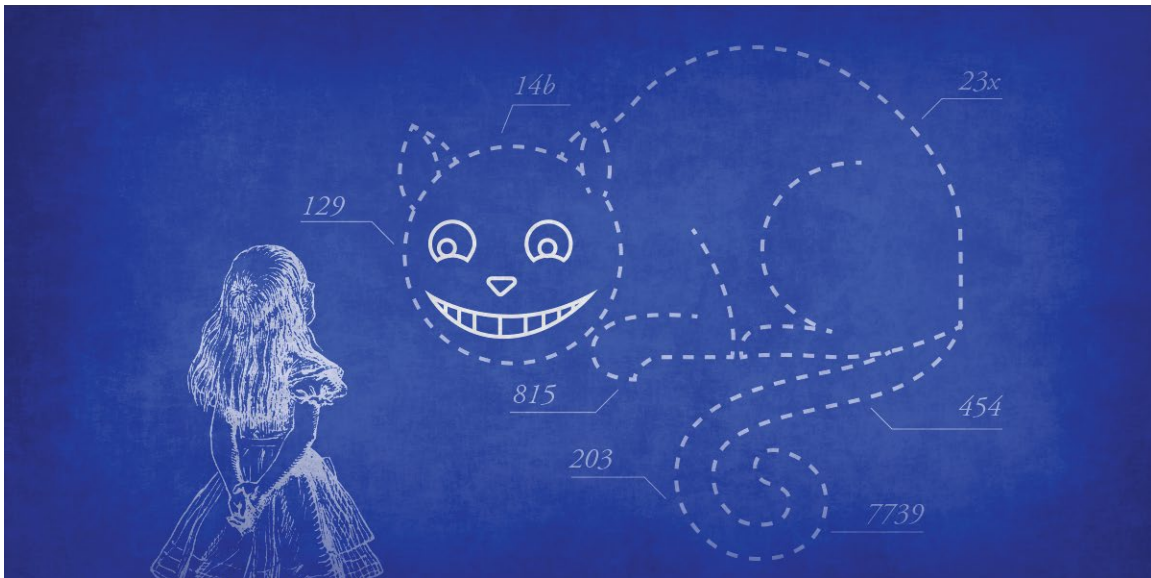
"I would think so," Jeremy responded.

More than 190 Internet engineers filed comments categorically stating that the FCC's interpretation of the Internet was factually wrong.

It was this and many subsequent conversations between our lawyers and engineers that resulted in EFF's FCC filing. More than 190 Internet engineers filed comments categorically stating that the FCC's interpretation of the Internet was factually wrong. It was followed by our amicus filing to the D.C. Circuit, with a chorus of engineers reiterating those points, and explaining the harmful impacts of the repeal on speech and innovation.

We will likely find out next year if the collective effort organized by EFF will be enough for the judiciary to put a stop to the FCC's repeal. We are also challenging the repeal in the states and we're making progress – 36 states have proposed bills with 9 having passed laws or executive orders. EFF's efforts in our home state resulted in California passing the strongest net neutrality bill of any state. No ISP should be able to dictate what kind of Internet we have. EFF will continue to join forces for an Internet that is fair and open, and the fight is far from over.

Free the Internet. [Donate to EFF.](#)



Daniel Nazer

SENIOR STAFF ATTORNEY
AND MARK CUBAN CHAIR TO
ELIMINATE STUPID PATENTS

Saved by Alice

Gallant tales: how small businesses and innovators defeat patent trolls.

EFF defends true innovators from patent trolls. A big part of our job is to protect creators from abstract patents on software ideas. This is why we welcomed the Supreme Court's decision in *Alice v. CLS Bank*, which held that an abstract idea does not become eligible for a patent simply by being implemented on a generic computer. This 2014 decision has significantly reduced the harm caused by vague and overbroad software patents.

Unfortunately, the *Alice* decision is under attack. A few powerful lobbyists have been asking Congress to undo the Supreme Court's ruling through legislation. To counter this, we launched a project called *Saved by Alice*, collecting stories of innovators who used the *Alice* ruling to save their business. You can learn more about this important work at eff.org/alice.

Our *Saved by Alice* project includes the story of an EFF client, Ruth Taylor. Ruth runs a photography website, *Bytephoto*, as a hobby. Her site hosts user-submitted photos and runs weekly competitions, decided by user vote, for the best. She never expected that her hobby would get her sued. But one day, a lawyer called her out of the blue to tell her she had been sued for patent infringement.

Ruth didn't understand how someone could patent online contests. It seemed like a scam.

Ruth didn't understand how someone could patent online contests. It seemed like a scam. But a few days later, a process server arrived at her house to formally serve the complaint. A company called Garfum.com Corporation accused her of infringing U.S. Patent No. 8,209,618 – which essentially patented the idea of online competitions. Ruth then knew the threat she faced was real.

EFF agreed to represent Ruth for free. Without pro bono legal help, Ruth would have been in a tough position. Defending a patent suit can cost hundreds of thousands of dollars. Since Bytephoto was just a hobby, Ruth had never incorporated it. This meant she was personally on the hook for the company's debts and liabilities. She faced the choice between paying a settlement and paying even higher litigation costs to clear her name.

Fortunately for Ruth, her lawsuit arrived after the Supreme Court's decision in *Alice v. CLS Bank*. Many judges have allowed challenges under Alice to be filed early in the case rather than waiting for discovery (since the patent itself is the key evidence). We filed a motion asking the court to hold the patent invalid under Alice. A few days before the court heard arguments on that motion, Garfum voluntarily abandoned its suit against Ruth.

While it was great to be able to defend Ruth and defeat the lawsuit against her, we want to ensure that other creators are protected from patents on abstract ideas. We hope that the stories collected in Saved by Alice will help convince legislators that the Supreme Court got it right: abstract software patents hurt innovation and should remain in the dustbin.

Protect Creators. [Donate to EFF.](#)



STRENGTHENING OUR COMMUNITY

EFF empowers technology users around the world. We educate the public on how to protect themselves and others and advocate for imprisoned bloggers and technologists.



Security Education Companion



Nathan Sheard

GRASSROOTS ADVOCACY
ORGANIZER

Keeping pace with the security needs of growing communities.

815 Eddy Street, on the edge of San Francisco's Tenderloin District, is a special place. While the people who work here do not often wear capes (we have been known to from time to time), their dedication to protecting civil liberties, and upholding the most fundamental of promises enshrined in the Bill of Rights, is nothing less than heroic. In a culture that lionizes entertainment and sports figures, you're unlikely to find kids on a playground emulating EFF's most dramatic wins, but there is no team more dedicated than the people that assemble each day within this building's walls.

In July of 2017, I received the call that I liken to the moment a college athlete finds out they have just been chosen in the draft to represent the top team in the league and asked to play alongside the most dedicated professionals in the field. As EFF's Grassroots Advocacy Organizer, I get to work alongside community members, organizers, and technologists that are passionate about ensuring privacy and fundamental rights for all.

... it became necessary for many of us to become versed in ways we could work with supportive attorneys to push back on these violations, and become better acquainted with tools that would provide security where legal protections were lacking.

Government surveillance is not a phenomenon born of the digital age. However, with each new innovation in technology, federal and local law enforcement agencies, and their commercial suppliers, have pushed for new ways to invasively monitor the public, often with disproportionate impact on activists as well as ethnic and religious minorities. My own path to understanding this reality better came as a result of working with activist communities in New York and later in cities throughout the country. As an activist in New York City, surveillance by the NYPD and other agencies was a regular occurrence. As these agencies began to use cell-site simulators and more advanced tools of surveillance that pushed the boundaries of warrant requirements and the Handschu decree (itself resulting from the NYPD's history of unconstitutional surveillance of First Amendment protected activity), it became necessary for many of us to become versed in ways we could work with supportive attorneys to push back on these violations, and become better acquainted with tools that would provide security where legal protections were lacking.

“As I developed the skills to assure that my data and my community’s information was secure, something happened... Others began coming to me for support in securing their own digital communications.”

One resource I came to rely upon was EFF’s Surveillance Self-Defense Guide (SSD). As I developed the skills to assure that my data and my community’s information was secure, something happened that I’m sure many EFF supporters can relate to. Others began coming to me for support in securing their own digital communications.

At the same time, many communities (especially activist ones) were growing more concerned with the security of their communication and devices. With increasing regularity, their phones were being seized as they entered the country, and community gatherings and religious institutions were being monitored. In North Dakota, where I was working before joining EFF, we learned that our concerns about protecting the information of hundreds of Water Protectors were well-founded. Reports revealed that law enforcement agencies worked directly with the mercenary firm Tiger Swan to surveil and infiltrate protest camps.

As you might expect, many other groups began to contact EFF for guidance on how to support and protect their neighbors and loved ones. It would not be practical or responsible for EFF or any national organization to respond individually to the overwhelming breadth of calls from such a wide range of concerned communities, facing a variety of immediate and potential threats. Luckily, the remarkable folks I now count as colleagues and friends did what they do with remarkable consistency. They developed a solution.

Days into joining EFF, I was overjoyed to get hands-on with resources that would become the Security Education Companion (SEC). I had become part of a cross-disciplinary team of activists, technologists, design professionals, and attorneys, working with the support of many outside educators and organizations, united to maximize their support for communities everywhere. Building on the lessons learned in the development of SSD, the SEC was designed

to help that person who has—perhaps unintentionally—become the de facto trainer within their community. SEC provides solid training to build pedagogical skill and to assure the information they’re delivering is accessible to everyone in the room.

Like me years before, many who find themselves thrust into the role of digital security trainer for their community do not have the experiences of both teaching and assessing security technology. The SEC helps bridge that knowledge gap. Additionally, rather than having professional experts parachuting into communities where they lack first-hand knowledge of the concerns and threats, and with whom the development of trust takes time, EFF teaches members of a community how to help each other.

I’ve worked closely with members of over 70 grassroots allies across the country and watched organizers who initially called me with concern in their voices, grow confident in their ability to walk new learners through understanding encryption, securing their accounts, threat modeling, and more.

The array of skills, expertise, and evident desire to look at a situation from every angle and work toward the best solution is what first enamored me with EFF’s work. A year has passed since I first walked through the doors of EFF’s HQ. Yet, I still come to work every day with the same excitement to work alongside this superhero team. Each day is a cherished challenge and an opportunity.

Train the Trainers. [Donate to EFF.](#)



Jillian York

DIRECTOR FOR
INTERNATIONAL FREEDOM
OF EXPRESSION

Offline

Around the world, bloggers and technologists are targeted and imprisoned.

When I first met activist and free software developer Alaa Abd El Fattah ten years ago, he was the loudest voice in the room. Passionate about the free and open Internet, and firm in his politics and principles, he stood out, and we soon became fast friends.

Alaa was beaten and arrested without a warrant by now-President Sisi's interim government in 2013. His friends rallied to his defense. We organized a letter urging the Egyptian government to immediately release him, and were joined by more than forty international organizations. We also worked with our allies at the Media Legal Defence Initiative to submit a petition to the UN Working Group on Arbitrary Detention; the Working Group ultimately ruled in Alaa's favor. Alaa is currently serving five years in prison.

In 2015, EFF launched Offline, a project advocating for detained or persecuted bloggers, citizen journalists, and technologists. Alaa's was among the first cases we highlighted, along with those of Canadian-Iranian technologist Saeed Malekpour and prominent Ethiopian journalist Eskinder Nega, among others. We hope that by shining a light on these cases, we can help secure a speedier release or better treatment for those imprisoned. We cannot let these important voices, though silenced, be forgotten.

Around the world, the number of individuals in prison for online speech is on the rise. In 2017, the Committee to Protect Journalists found that more than 70% of imprisoned journalists were arrested for activities conducted online, and a 2018 Reporters Without Borders report counted 141 incidents of imprisoned citizen journalists.

Poet Dareen Tatour spent several years under house arrest for a poem she read on YouTube before being sentenced to five months in prison.

Today, Offline features seven active cases. There's Wael Abbas, an award-winning Egyptian journalist arrested earlier this year without a warrant and held in continuous pre-trial detention. Amal Fathy is a mother and activist whose viral video about sexual harassment in Cairo landed her in prison. Poet Dareen Tatour spent several years under house arrest for a poem she read on YouTube before being sentenced to five months in prison. These, and the other featured cases, show us that governments will do anything to silence powerful voices—and that we must fight globally for the right to freedom of expression.

While we carry sorrow and outrage for these individuals, we have also been able to share some victories: Nega and his fellow countrymen, the Zone 9 Bloggers, were freed earlier this year. This fight can seem like an uphill battle, but EFF is tenacious. We must continue to raise awareness of the plight of those around the world who bravely contribute to innovation and raise their voices against injustice.

Shine a light. [Donate to EFF.](#)



The Electronic Frontier Foundation team is deeply grateful to grassroots members like you who keep our lights on, ensure our laptops are firing, and give us the strength to stare down the Internet's biggest foes with confidence.

The following financial report details EFF's fiscal year from July 2016 to June 2017.

EFF's fight for online privacy, free expression, and the future of innovation depend on support from nearly 40,000 active donors around the world. We are proud that the majority of EFF's funding comes from regular individuals, and more than 80% of that funding consists of donations under \$10,000. Direct contributions from companies comprised less than 5% of our total public support. Thanks for ensuring that EFF's work will always remain fiercely independent.

EFF has a four-star rating (the highest possible) and scores a perfect 100 in accountability and transparency from watchdog Charity Navigator, a non-profit organization dedicated to providing an unbiased, objective, and numbers-based assessment of over 9,000 charities.

(chart on next page)

FY 2017 PUBLIC SUPPORT



PUBLIC SUPPORT

Individual	\$7,203,354
Individual through Foundation	\$1,075,615
Employee & Customer-Directed*	\$1,644,029
Corporate	\$819,127
Foundation	\$3,027,866
Cy Pres	\$3,061,754
In-kind Legal Services	\$289,437

Total Public Support **\$17,121,183**

FY 2017 EXPENSES

EXPENSES

Program	\$8,578,311
Administrative	\$1,559,585
Fundraising	\$1,545,519

Total Expenses **\$11,683,415**



INCOME

PUBLIC SUPPORT

Individual Contributions		
Individual Contributions over \$50,000	\$547,540	
Individual Contributions \$10,000 - \$50,000	\$774,470	
Individual Contributions under \$10,000	\$5,881,344	
Total Individual Contributions		\$7,203,354
Individual Contributions through Foundations		
Individual Contributions through Foundations Over \$50,000	\$525,000	
Individual Contributions through Foundations Under \$50,000	\$550,615	
Total Individual Contributions through Foundations		\$1,075,615
Foundation Grants		\$3,027,866
Cy Pres Awards		
Capital One TCPA Litigation	\$1,726,379	
Fraleigh v. Facebook, Inc.	\$846,771	
Bank of America TCPA Litigation	\$187,212	
McCabe, et al. v. Six Continents	\$125,870	
Stanley Nader v. Capital One	\$83,559	
Chapa v. TruGreen Inc.	\$82,550	
Wheelock v Hyundai Motors of America	\$9,413	
Total Cy Press Awards		\$3,061,754
Corporate Contributions		
Employee and Customer-Directed Gifts*	\$1,644,029	
Other Corporate Contributions	\$819,127	
Total Corporate Contributions		\$2,463,156
In-kind Legal Services		\$289,437
Total Public Support		\$17,121,183

REVENUE

Net Investment Income	\$1,710,119	
Attorneys' Fees Awarded	\$22,500	
EFF Event Income, Net of Expenses	-\$16,242	
Miscellaneous	\$226,354	
Total Revenue		\$1,942,732

TOTAL SUPPORT AND REVENUE

\$19,063,915

EXPENSES

Amortization & Depreciation	\$251,462
Building Expenses	\$203,860
Corporate Insurance	\$114,922
Fundraising Expenses	\$1,945
Furniture & Equipment Expense	\$63,883
Intern Expenses	\$23,342
Legal & Professional Fees	\$931,993
Litigation Expenses	\$95,811
Membership Expenses	\$537,761
Office Expenses	\$109,307
Planning & Development	\$69,231
Salaries & Benefits	\$9,080,273
Travel Expenses	\$185,498
Other Administrative Expenses	\$14,127

TOTAL EXPENSES

\$11,683,415

NET INCOME

\$7,380,500

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



THANK YOU

For 28 years, members have joined EFF to defend freedom of expression, protect encryption, battle with patent trolls, stand up for the freedom to tinker, empower users with technical tools and knowledge, 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.

BECOME AN EFF MEMBER TODAY!

The Electronic Frontier Foundation (EFF) is the leading organization defending civil liberties in the digital world. We guard free speech online, fight illegal surveillance, 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.

TO BECOME A MEMBER, SIGN UP AT EFF.ORG/ARCY17, OR FILL OUT THIS FORM & MAIL TO EFF:



815 Eddy Street
San Francisco, CA, 94109, USA

CONTRIBUTE TO DEFEND DIGITAL FREEDOM:

- ☐ Super Major Donor (\$2,500+).....shirt, hat & stickers
- ☐ Major Donor (\$1,000+).....shirt, hat & stickers
- ☐ Rare Earths (\$500+).....shirt, hat & stickers
- ☐ Titanium (\$250+).....shirt, hat & stickers
- ☐ Gold (\$100+).....shirt ☐ or hat ☐
- ☐ Copper (\$65+).....shirt
- ☐ Silicon (\$25+).....multisticker sheet
- ☐ Other \$ _____

☐ No gift, please.

\$ _____
Donation Amount — Thank you for supporting EFF!

Credit Card Number (AmEx, Discover, MC or Visa)

Signature Exp. (MM/YYYY)

(_____) _____
Phone Number — In case of transaction issues only.

CHOOSE YOUR SHIRT STYLE AND SIZE:

☐ Slim ☐ Classic ☐ XS ☐ S ☐ M ☐ L ☐ XL ☐ 2XL ☐ 3XL

CONTACT INFORMATION:

First Name Last Name

Address

City State/Province

Postal Code Country

☐ Yes, I have supported EFF before.

☐ Yes, I want EFF's online newsletter & Action Alerts.

Email address

Donate via credit card, check (payable to EFF), or at eff.org/ARCY17
EFF is a 501(c)(3) nonprofit, US federal tax ID 04-3091431.
Your gift is tax-deductible as allowed by law, less the value of premiums received.
We do not sell, swap, or share your information. Contact us at membership@eff.org
ARP17