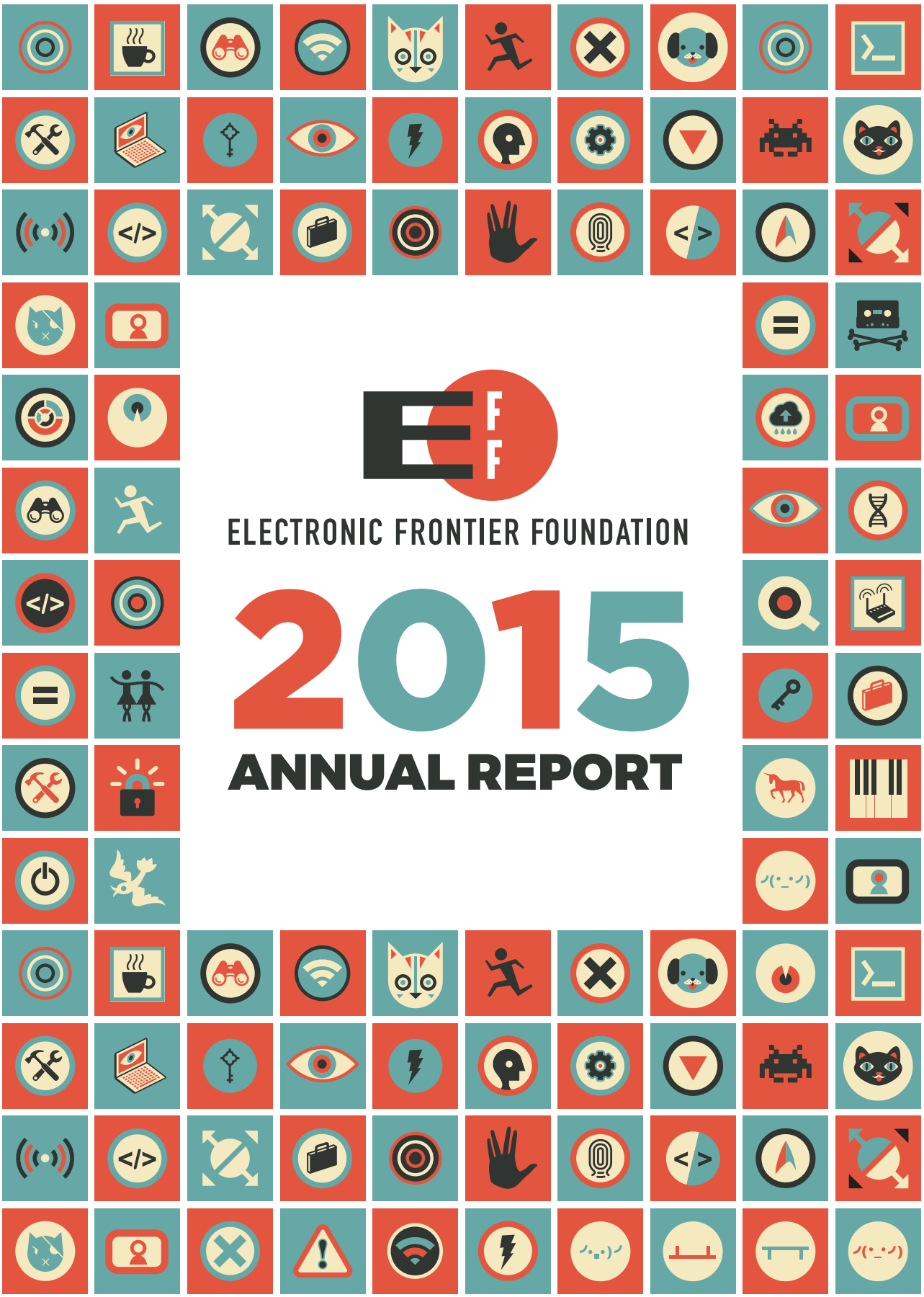
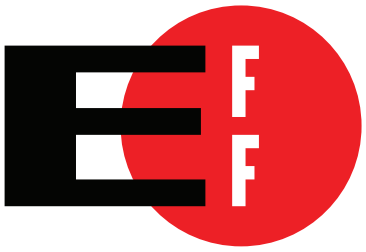


ELECTRONIC FRONTIER FOUNDATION

2015 ANNUAL REPORT



The 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 over 25,000 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 2015.

TABLE OF CONTENTS

A WORD FROM OUR EXECUTIVE DIRECTOR

Dear friends,

2015 was a year of big transitions at EFF. After 15 years as EFF's Legal Director, I took on the role of Executive Director last April, stepping into Shari Steele's shoes. Over the past year, I have found myself overwhelmed by support from both inside and outside of the organization, and newly galvanized as we set forth on this next phase in EFF's history.

Twenty-five years ago, EFF took the first steps toward what is now a global movement. We have watched this movement coalesce, uniting people around the world who embrace digital technology and all of its possibilities. We've grown alongside the Internet, taking strategic steps to maintain our role as the anchor of this ever-growing movement. We fight to make sure people have access to the speech platforms and privacy tools that help them take control of their world, innovate and grow, and bring their imaginations to life.

We know, too, that even as technology develops to more deeply enrich our lives, it also increases its potential to restrict our freedoms. EFF's fight is on this front, too: we have your back against overbroad surveillance, against the lockdown of the tools people use to communicate and bring their ideas to fruition, and against other corporate and legal attempts to use technology and law to limit our digital freedoms. In 2015, we busted the podcasting patent and fought for—and won—several key DMCA exemptions, including jailbreaking cell phones and other devices to run

third-party software, and repairing and doing security research on your own car. Based in part on our near decade of activism and legal work, Congress also passed the USA Freedom Act, the first real restrictions and oversight imposed on the NSA's surveillance powers since 1978.

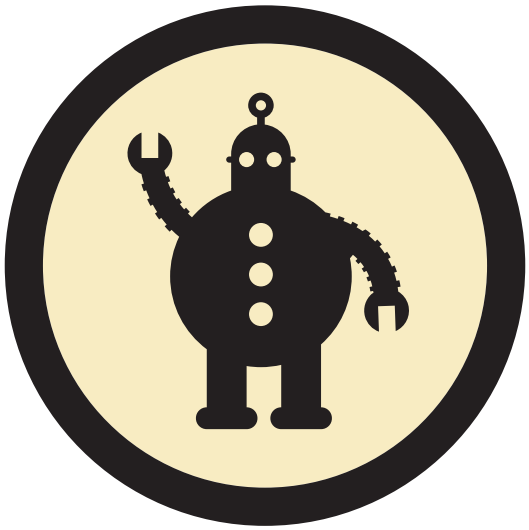
"As the line between our everyday lives and our digital lives fades into memory, EFF's role becomes even clearer."

Even as we fight these battles, however, we strive to educate and equip others to do the same. Our annual Who Has Your Back? report has gone global, with partners in Mexico, Colombia, and Peru publishing their own editions as they bring the battle for digital rights to their own turf. Let's Encrypt—a free, automated, and open certificate authority—brings HTTPS to the masses by making it easier than ever to set up a secure website. Street Level Surveillance breaks down how commonly-used surveillance technologies work and provides activists with the information they need to challenge the use of these technologies in their own communities.

As the line between our everyday lives and our digital lives fades into memory, EFF's role becomes even clearer. A strong EFF is vital to a strong Internet; as the Internet becomes vital to people's lives, so, too, does a strong EFF. As author and EFF Fellow Cory Doctorow puts it, there are no digital rights anymore—there are just rights. And it's not just digital freedom we're fighting for—it's freedom.

We're not at the threshold anymore. We've been fighting the good fight for 25 years, and we couldn't have done it without you. I hope you'll continue to ride along with us, because I can't wait to see what's next.

Cindy Cohn, Executive Director

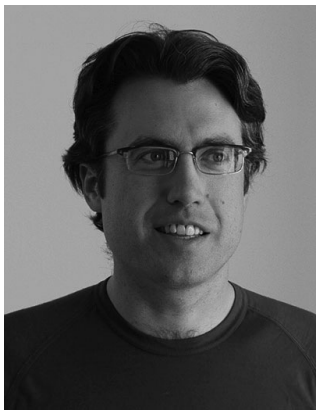


TECH

We build tools to increase the security, privacy, and censorship resistance of Internet protocols and delve into the technical details of the software and services that increasingly affect our digital rights.

LET'S ENCRYPT

A free, automated, and open certificate authority (CA), run for the public's benefit, puts a secure Internet within reach.



Jacob Hoffman-Andrews
SENIOR STAFF TECHNOLOGIST

Five years ago, I joined the movement to encrypt the Web. I was an engineer at Twitter at the time, and Firesheep had just been released, demonstrating just how easy it was for anyone to hijack people's accounts by sniffing cookies. The fix, HTTPS, was cheaper than ever, but was considered overkill for a social site. I began quietly fixing bugs in Twitter's nascent HTTPS support, and agitated for full encryption by default. Eventually I made HTTPS-by-default my full-time job, and within a year it was enabled for all users.

As a longtime EFF supporter, I had watched the first crypto wars with great interest. I ran workshops to teach my friends and neighbors how to encrypt email with PGP and chat with OTR, and I realized that to make the most of our right to encrypt, we need safe protocols that everyone can use—without even knowing they're using them. HTTPS is one of those protocols, and my biggest goal in my work is to bring safe, strong encryption to every person who uses the Web.

As an EFF Technologist, I make it my mission to find high-leverage ways of advancing our ideals of individual privacy and free expression. My biggest project at the moment is developing the free and automated certificate authority, Let's Encrypt. Let's Encrypt was developed behind the scenes for many years, and finally launched to the public in December. As a certificate authority (CA), it provides websites with certificates, a prerequisite to using HTTPS. For better or for worse, CAs act as gatekeepers

to the secure Internet. Until now, most CAs have been expensive, difficult to use, or both. With Let's Encrypt, we implement the same level of validation as other CAs, but we make it free for everyone, and are working to make it as easy as possible. If we are going to encrypt the Web, we cannot leave anyone behind. I strongly believe that money and technical skills cannot be a barrier to speech on tomorrow's safer Web.

"If we are going to encrypt the Web, we cannot leave anyone behind."

The first time I used Let's Encrypt to turn on encryption for a live website, it was magical. I can think of no other way to describe it. I'd spent months working on both the client and server code, issuing thousands of test certificates. But the first time I ran the command on a live server, then opened my browser to see that little "https:" in the URL bar, it all became really real for me. I thought, "We're really going to do it. The whole Web."

Let's Encrypt just issued its two millionth certificate. We're planning to issue billions more in the years to come. I can hardly wait.

Our browser extension, which automatically blocks hidden trackers that would otherwise spy on your web browsing habits, leaves beta.

Cooper Quintin
STAFF TECHNOLOGIST

Like many people who came of age after the launch of the World Wide Web, I practically grew up on the Internet. Rather than watch TV all summer, I spent hours every day browsing the early Web and exploring the Internet: reading text files and web forums, finding funny GIFs, learning interesting new things and talking to people from around the world. I gained knowledge, experiences, and friends that I never would have otherwise in my small northern California town. To me, the Internet represented a worldwide community; one more diverse, interesting, accepting, and free than any geographically-based community could have ever been. The Internet feels like my home, so it is of great importance to me that the Internet remain the open, free, and diverse place that I grew up with.

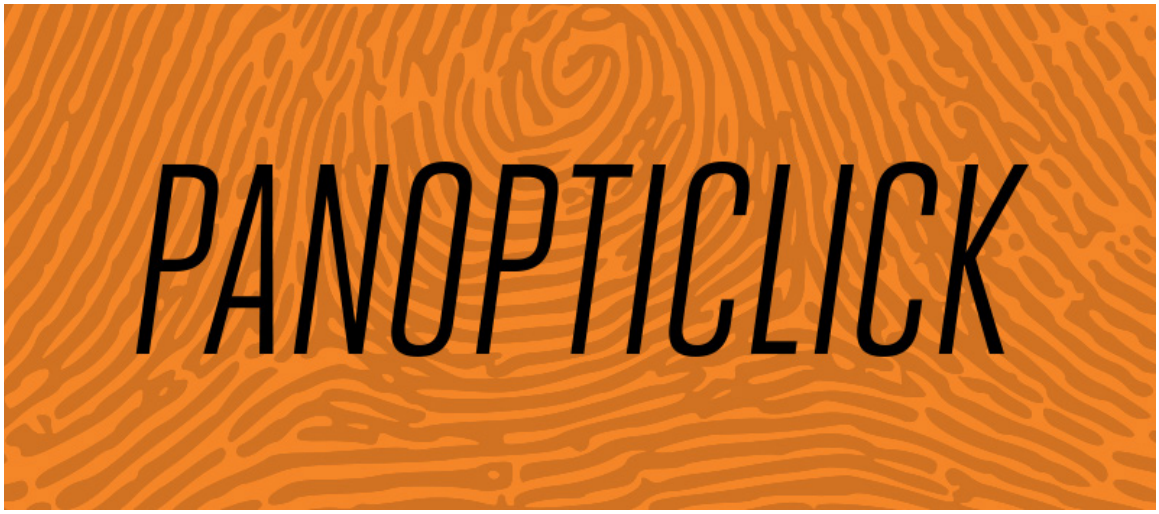
I have long felt that non-consensual tracking is one of the greatest threats to Internet freedom. Unfortunately, third-party tracking has become the main business model of the Web. I have seen the privacy and anonymity that I love so much about the Web—the cornerstones of freedom of speech and freedom of thought—erode due to web-based tracking. So of course I was thrilled to start work on Privacy Badger, a tool to stop non-consensual tracking on the Web. I'm far from alone in my enthusiasm for the project: Privacy Badger has been downloaded by over 500,000 people since alpha launch in 2014.

But shepherding an open source project is not always easy. With any creative endeavor, it can be intimidating to put so much effort into a piece of work and then release it into the public; Privacy Badger is no exception. As a software developer, most of the feedback you get on your projects is in the form of bug reports and complaints, which can be discouraging for many open source developers. It can be difficult to remember that most of the people who use your software actually like it.

Sometimes, though, I'm reminded that people actually do rely on—and love—Privacy Badger. I once struck up a conversation on BART with a person wearing an EFF shirt. I mentioned that I work on Privacy Badger. "Oh, Privacy Badger! I use that every day," he responded. "I love it!" Another time, I was wearing my Privacy Badger shirt when a man shouted at me—from across the street—that he and his dogs love EFF and Privacy Badger! And a couple of weeks ago, when I was talking to a friend, it turned out that she had been using Privacy Badger for months as her primary tracker blocking extension, and was very happy with how it had made her browsing experience feel safe again.

"Every time I make Privacy Badger better, I feel like I am making the Web just a little bit more private and a little bit more free."

It's moments like this that make me really appreciate the work that I get to do. With every new release, I get the joy of knowing that my code is running on more than half a million computers. If I write good code, hundreds of thousands of people get better protection from tracking, malvertising, and surveillance. Every time I make Privacy Badger better, I feel like I am making the Web just a little bit more private and a little bit more free. Maintaining Privacy Badger is a big responsibility, and it can be intimidating at times, but when I meet people that tell me how much they like Privacy Badger, and how thankful they are for the work that EFF does, it makes all of the hard work worthwhile.



The latest version of our tracking and fingerprinting detection tool includes new tests, updating its ability to uniquely identify browsers with current techniques.

William Budington
SOFTWARE ENGINEER

In the last few decades, the web browser—the most widely-used Internet platform for the free flow of information—has been transformed by advertisers and trackers into a place where user data is now brokered and exchanged freely without user consent—or even knowledge. What's worse, there is no limit to the invasive methods trackers can use to learn the intimate details of our activities, identities, and behaviors. Panopticlick fights back against these trackers by providing you with information about what your browser divulges about you and suggests tools to protect yourself against trackers.

We originally launched Panopticlick in 2009 in response to the widespread problem of web tracking. The site, used by hundreds of thousands, allowed users to determine just how unique—and fingerprintable—their browsers were. Last year, we launched Panopticlick 2.0, a new iteration that improved the site by giving it a new design, adding additional fingerprinting metrics, and detecting how well your tracking protection is working.

I was very excited to spearhead a project with such a large impact: the revamped site has provided over 9 million results to users across the globe. But this was a team

effort, bringing together designers, technologists, and developers to make it happen, and the process of pulling it all together gives a great picture of EFF in action.

The site design was brought to you by our art director, Hugh D'Andrade. The new logo, color scheme, and background image are all a result of his keen eye. Our design contractor, Chris Antaki, wrangled our templating engine and brought Hugh's design to life. The responsive design views that you see on the site are a result of Chris' hard work.

"Panopticlick fights back against these trackers by providing you with information about what your browser divulges about you and suggests tools to protect yourself against trackers."

While Hugh and Chris tackled the design and layout aspects of the site, I converted the older Panopticlick codebase to Python/Flask, incorporating bits of code from projects like Aloodo and Fingerprint2 and working on adding additional tests for our fingerprint and blocker detection tools. We developed in parallel—Chris in a styling branch and myself in a development branch—eventually merging them to make sure everything was in tip-top shape for launch. In the meantime, activism team lead Rainey Reitman, General Counsel Kurt Opsahl, and Chief Computer Scientist Peter Eckersley finessed the language to appear on various pages of the finished site.

With so many elements in flux, we were worried about bringing them all together in time. Our web development team lead, Max Hunter, was able to coordinate all the moving parts and make sure they operated as a well-oiled machine.

Panopticlick embodies the coordination we see on various projects at EFF, bringing together different skills, mindsets, and sometimes even combatting opinions. In the end, our collaboration ensures that we create a great product that benefits the people it's our mission to defend: you, the user!

ACTIVISM

We inform the press and public about digital rights issues and provide meaningful avenues for change, distributing tools and techniques to protect essential freedoms worldwide.

After more than two years of work in the wake of the Snowden revelations, this bill's passage marks the first significant reform on NSA surveillance in over 30 years.

Rainey Reitman
ACTIVISM DIRECTOR

My friend Peter jokes that I should have a bulletin board with all the bills I've killed.

In six years at EFF, I've lost track of how many times I've crossed swords over flawed legislation that would undermine our rights. Whether bills are trying to force tech companies to store data on their users, increase penalties related to computer crimes, ratchet up surveillance on the local level, or push online platforms into acting as censors—I've faced a lot of bad legislation. We don't win every battle, but we win a lot of them.

But one thing is a lot harder than stopping bad bills: passing something good.

This year is different. This is the year we passed the USA Freedom Act. It's the first time in over thirty years that Congress put real restrictions and oversight on the NSA's surveillance powers.

The law does a few things. It limits the bulk collection of phone records by the NSA, effectively ending the mass surveillance of telephone metadata in the United States. It adds new levels of transparency to the surveillance practices of the NSA and gives companies greater ability to report on surveillance requests. Perhaps most importantly, the law creates a special amicus position in the FISA Court: a legal expert to argue for

privacy and civil liberties before the secret court that approves domestic surveillance programs by the NSA.

Those changes are vital to reforming mass surveillance. But for me, this bill was more than just changes in the law. It was also a turning point for our advocacy.

"It's the first time in over thirty years that Congress put real restrictions and oversight on the NSA's surveillance powers."

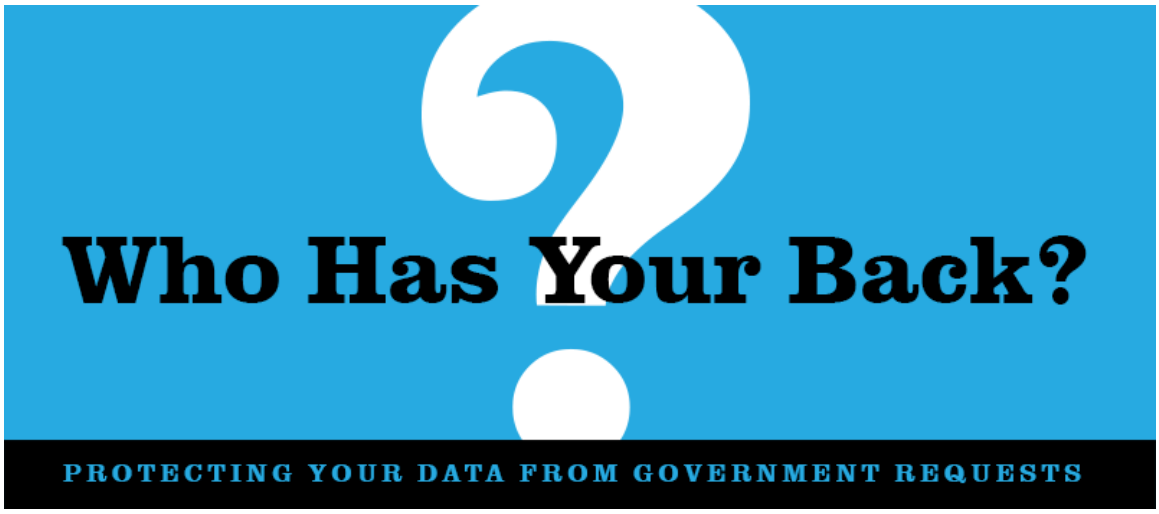
Passing positive legislation is just plain hard. It takes sustained pressure from the public, a massive publicity campaign around a central issue, continuous engagement with the media, deep connections to lawmakers, and the coordination of diverse groups from across the political spectrum. It takes years, and there's no guarantee of success.

I dedicated a few years of my life to passing the strongest version of the USA Freedom Act possible, and I'm glad for it. Lots of that time was mundane: early morning conference calls, editing blog posts, reviewing bill text. Even on the long days, I was happy for it because defending rights is my life's work, and there's no place I'd rather be.

Other moments were life-changing. I'll never forget watching a blimp glide over the NSA data center in Utah at dawn, announcing our new website grading legislators on their votes to reform NSA surveillance. I'll always smile to think of how we wrangled celebrities like John Cusack and Maggie Gyllenhaal for a video against mass spying. There was one day we rallied 90,000 people into calling Congress demanding an end to mass spying. And I cherish the memory of walking through a crowd of thousands in Washington, D.C., looking up at sunlight glinting through cloth banners with the words of the First and Fourth Amendments bright against the sky.

I believe the USA Freedom Act is the first step to reining in mass spying by the NSA. To really end unconstitutional surveillance, we need to keep passing positive legislation. And this year, we proved we can do that.

We've still got a long road ahead of us, but we're definitely headed in the right direction.



Our yearly report—which documents the practices of major Internet companies and service providers, judges their publicly available policies, and highlights best practices—goes global.

Katitza Rodriguez
INTERNATIONAL
RIGHTS DIRECTOR

I'm writing this in Lima, the city where I grew up. I still remember the street protests during the presidency of Alberto Fujimori, a time when it was difficult to engage in political activism without fear of retaliation. Fujimori is now serving 25 years in prison for corruption and crimes against humanity. I remember it as if it were yesterday. It was then that I came to realize that no matter how democratic a government is, realities change. Power corrupts, and when it does, surveillance equals control.

It was then that I learned, firsthand, the value of privacy.

Over the last five years, EFF's "Who Has Your Back?" project has successfully persuaded US companies to adopt voluntary user protection standards to safeguard against government access demands. By adapting these voluntary measures to local laws and realities in Peru, Colombia, Mexico, Brazil, Chile, and Paraguay, I thought, we could help our allies in those countries stand up to protect users' privacy rights.

Working with digital rights and privacy groups across the continent, we devised "Quien Defiende Tus Datos," a project to compare phone companies and Internet service providers in Latin America to see which stand with their users when responding to government requests for personal information. Each report examined publicly

posted information, including privacy policies and codes of practice, from the biggest telecommunications access providers in each country. Each was customized and targeted based on what we knew were the greatest threats and opportunities.

"By adapting these voluntary measures to local laws and realities in Peru, Colombia, Mexico, Brazil, Chile, and Paraguay, I thought, we could help our allies in those countries stand up to protect users' privacy rights."

It hasn't been easy. "Who Has Your Back?" was hard enough in the United States, where companies like Google, Twitter, and Facebook already face constant media scrutiny for their practices. In Latin America, political conditions, media concentration, and a long tradition of big corporations voluntarily assisting law enforcement with their surveillance demands make it even harder.

What has made it a joy is partnering on the ground with activists who—with few resources—have undertaken to speak truth to power on an extremely challenging topic. Groups like InternetLab, Fundación Karisma, Red en Defensa de los Derechos Digitales, Derechos Digitales, and TEDIC jumped at the chance to learn and build upon some of the strategies we've developed to put pressure on companies and governments. By working with activists around the world, we amplify our message. We also learn more about the realities of surveillance from those who face it every day.

I've been traveling throughout Latin America for more than 16 years. I see many here who suffer the most harrowing effects of compromised security, from kidnappings to contract killings. As in the rest of the world, this violence is used to intensify people's fear. The people become willing to compromise their freedom in order to feel safe, to embrace new security measures under the misconception that they will lead to greater safety. We can't let that impulse to authoritarianism rule the Net.

With work like "Quien Defiende Tus Datos," with our many sister organizations across the world, and with your support, we work to ensure the digital world is free—in Peru, across the Americas, and anywhere and everywhere we can make a difference.

Our new Web portal is loaded with comprehensive, easy-to-access information on police spying tools like license plate readers, biometric collection devices, and "Stingrays."

Jennifer Lynch
SENIOR STAFF ATTORNEY

How can we help the people who are most impacted by domestic surveillance technologies? Whether it's Muslims targeted by Automated License Plate Readers in New York, defense attorneys trying to figure out how the cops located their client inside his girlfriend's apartment, or migrant workers in Georgia rounded up by ICE and coerced into providing biometric data, that's the problem we were trying to solve when we launched our Street Level Surveillance project.

This is not a new problem for EFF. Just before I started working here, Department of Homeland Security (DHS) launched a program called "Secure Communities" or "S-Comm" that mandated biometric and biographic information sharing among local law enforcement officers, the FBI, and DHS. S-Comm resulted in almost 230,000 people being taken into ICE custody and identified for deportation, including approximately 3,600 U.S. citizens—and many of these people were originally arrested for extremely minor offenses. This controversial program made people fearful of reporting crime to their local law enforcement agencies. Because S-Comm relied in part on biometric data sharing—something I've worked on quite a bit while at EFF—immigrant and minority rights organizations reached out to us for help. In 2011, we partnered

together to host a large conference about the intersection of surveillance technology, domestic law enforcement, national security, and immigration enforcement, and that provided the perfect forum to meet with groups whose clients were feeling the impact of surveillance firsthand.

"...sometimes we forget that some of the most vulnerable in society are feeling the impact of surveillance on a day-to-day basis from their local cops, not the NSA."

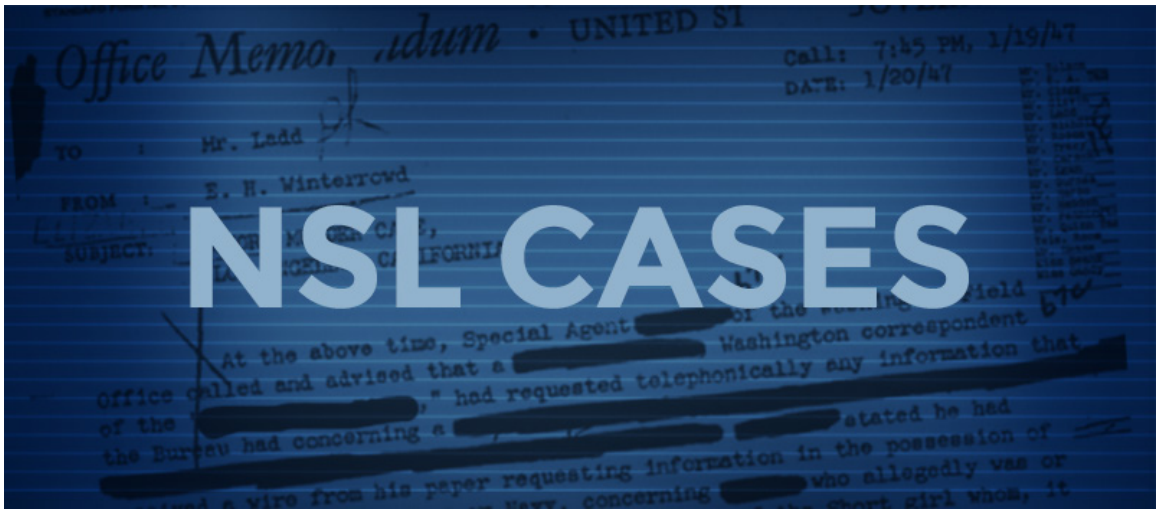
After that conference, lawyers and activists at EFF continued to work with, help, and learn from these community organizations, but the work was piecemeal, and our limited time meant we weren't able to help as many people as we wanted to. We decided to create a central portal on our website where we could direct people so that they could learn about specific surveillance technologies and find resources to use in their own work.

The Street Level Surveillance project brings together resources for community members, defense attorneys, organizations, lawmakers and judges, and includes infographics explaining how specific surveillance technologies work, "know your rights" information, litigation briefs, presentations, case summaries, and blog posts about the most important issues arising in domestic surveillance technologies today.

EFF has long been widely known and highly regarded for its work on national-security related surveillance, but sometimes we forget that some of the most vulnerable in society are feeling the impact of surveillance on a day-to-day basis from their local cops, not the NSA. Through the Street Level Surveillance project, we can offer resources about surveillance technologies and how they're being used—and remind people that they have the power to question the use of these technologies in their own communities and to put pressure on lawmakers and agencies to change.

LAW

We defend digital rights through impact litigation, "friend of the court" participation in pivotal US court cases, policy analysis, and answering questions about technology law for the press and public.



EFF fights unconstitutional gag orders on behalf of clients forced to remain anonymous.

Kurt Opsahl
DEPUTY EXECUTIVE DIRECTOR
AND GENERAL COUNSEL

For the last five years, I've had the honor of representing the two unnamed service providers defending a Federal court's decision holding the National Security Letter statute unconstitutional on its face. A statutory gag prevents our clients from publicly acknowledging even the mere fact of receiving the NSLs. We're fighting for their right to speak.

The danger of national security powers being abused increases exponentially when the law operates in the shadows. Sunlight is, as Justice Louis Brandeis put it, "the best of disinfectants." If our clients could fully participate in the wide-ranging public debate on this controversial NSL power—and its documented history of misuse—they could open the shutters and bring sunlight where it is needed most.

In addition to our courageous clients' efforts, service providers big and small are now publishing transparency reports. Spurred on, in part, by EFF's Who Has Your Back rankings, which give "gold stars" to providers who issue transparency reports, the release of these reports lets customers (and the public) know more about the kinds of legal demands that service providers are receiving—and how often they are receiving them. Yet the gag orders that accompany NSLs are a problem here too. Because of these gag orders, my clients cannot publish honest and complete reporting for their customers. If we are successful in striking down the gag orders, we'll not only help our

clients to speak truthfully, we'll also be helping everyone who wants to hear. Knowing how often the government comes seeking information from our service providers is important not only for people who want to protect their privacy, but for us as a society to judge whether we're comfortable with the decisions government is making in seeking that information.

"Sunlight is, as Justice Louis Brandeis put it, 'the best of disinfectants.'"

Thank you for the support that makes this important work possible. With your help, we've been able to fight to preserve the vibrancy of our constitutional rights, for transparency and justice, and, of course, for sunlight.

EFF successfully challenged the bogus podcasting patent owned by Personal Audio LLC.

Daniel Nazer

STAFF ATTORNEY AND MARK CUBAN CHAIR TO ELIMINATE STUPID PATENTS

As fans of the Internet and free speech, EFF loves podcasting. Some of our favorite episodes include:

- This American Life on patent trolls
- ReplyAll on the Computer Fraud and Abuse Act
- Note to Self on Stingrays
- The WTF episode where Marc Maron calls EFF (and Moon Zappa)

Almost as much as we love podcasts, we hate patent trolls. But our patent fights are often difficult for nonlawyers to understand, since they are steeped in the particular language and jargon of patent law and involve obscure legal processes. So in early 2013, when we learned that a patent troll was going after podcasting, we knew we had to jump in and use this horrible situation not only to protect podcasting, but to broaden the public's understanding about the problems patent trolls cause for all of us. While patent trolls often use jargon and gibberish to obscure their claims and make cases hard to understand, this one presented a clear injustice. The context was dramatic: a troll called Personal Audio had sued Adam Carolla in the Eastern District of Texas and was loudly threatening to sue other podcasters.

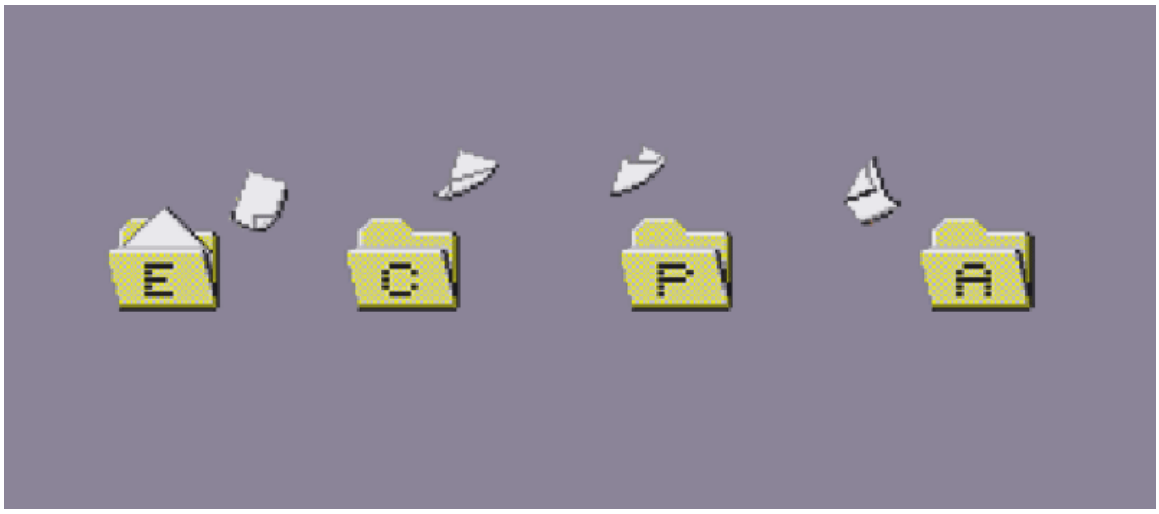
We decided to use one of those obscure legal processes, called "inter partes review," to challenge the patent at the patent office. We've done versions of this plenty of times,

using previous processes at the Patent and Trademark Office (PTO), but this time we decided to ask the public to help fund our challenge. This was in part because the application fee alone was over $20,000. The public response was overwhelming and gratifying: we quickly raised the funds and filed our challenge in October 2013. The reach of this campaign was much broader than our usual EFF fundraising, thanks in part to podcasters themselves explaining the situation to their listeners. Our petition cited the Geek of the Week internet radio show from the early 1990s, an MIT masters thesis, and a CBC online radio pilot program.

"While patent trolls often use jargon and gibberish to obscure their claims and make cases hard to understand, this one presented a clear injustice."

As well as working on the fine technical and legal details of the case, we got to reach new audiences. Former staffer Julie Samuels was a guest on Adam Carolla's lively show. And I got to go on my favorite podcast: WTF with Marc Maron (something I never thought would happen without having a second career as a standup comic).

In April 2015, we learned that our hard work had paid off: the Patent Office granted our petition and struck down all the challenged claims. Just days later, Chairman Bob Goodlatte cited our challenge favorably at a congressional hearing on patent reform. The case is now on appeal at the Federal Circuit. If the ruling stands—as we are optimistic it will—it should prevent Personal Audio from suing any more podcasters. But in addition, this case helped raise the broader problem of patent trolls, as well as the need for patent reform, in the large and growing community of people who, like us, love podcasts.



California is now the largest state to adopt digital privacy protections including both the content of messages and location data.

Dave Maass
INVESTIGATIVE RESEARCHER

As we shift to a paperless society, our devices have shrunk, their storage capacity has grown, and cloud services have begun hosting more of our information. Our laws, however, haven't caught up yet: while law enforcement needs a warrant to search through our filing cabinets and drawers, law enforcement often claims it doesn't need to follow the same rules to access our digital information.

We needed a way to ensure that police get a warrant for our electronic records, including emails and locational data, regardless of whether they're held on a device or by online service providers. New technology may address a lot of contemporary challenges, but problems with the law can often only be solved by the same age-old system: the legislative process.

Near the end of the 2015 California legislative session, Gov. Jerry Brown signed what Wired magazine dubbed "the nation's best digital privacy law." Before that, the bill went by many names: S.B. 178, the California Electronic Communications Privacy Act, and CalECPA. However you refer to it, we call it a victory. Except in rare life-or-death emergencies, law enforcement in California now need to get a warrant before they can access your digital records, whether it's on your cell phone or stored by an online service provider.

This victory didn't come easily: it was the third time the legislature sent a bill of this nature to the governor's desk. But the last two times, the bill died with a flick of the governor's veto pen. This time around, however, the equation changed. It started with a bipartisan team of authors: Sen. Mark Leno, your traditional San Francisco Democrat, and Sen. Joel Anderson, a Southern California Tea Party Republican. EFF, the ACLU of California, and the California Newspaper Publishers Association formed the core of the activism movement. But what was different this time was that the tech companies joined the cause en masse. Through careful negotiations, the coalition was even able to get the state's major law enforcement agencies to go neutral on the bill.

EFF was involved in every step of the bill's passage. Senior staff attorneys Lee Tien and Hanni Fakhoury were up to their elbows in legal analysis and negotiation. Activist Adi Kamdar, and later I, Dave Maass, mobilized the grassroots. We generated thousands of emails to the legislature and the governor. EFF Technologist Cooper Quintin helped deliver 100,000 signatures generated on a dot matrix printer to the governor's office. Through what they called a "hard sell," we convinced the San Diego Police Officers Association—one of the largest local peace officer unions in the state—to throw its support behind the bill. It became a key ally when an anti-child-exploitation organization began circulating misleading, alarmist propaganda at the eleventh hour. This could have threatened the 2/3 vote we needed to pass a suppression remedy.

"EFF was involved in every step of the bill's passage."

Despite the opposition, the bill passed 34-4 in the Senate and 57-13 in the Assembly. Gov. Brown then signed the bill, along with several other measures regarding surveillance transparency. As we anticipated, we are currently working with the author and the law enforcement community on a series of small amendments that will clear up uncertainty in the language. However, we are also vigilantly observing how law enforcement applies the law, keeping a careful eye on how prosecutors and judges apply CalECPA in parole and probation cases.

Our laws have previously failed to reflect the privacy protections enshrined in the Constitution: the guarantee that people be free from unreasonable searches and seizures. California has led the way—as in so many things—in treating data with respect for its constituents' privacy and dignity. We are optimistic that others will follow its example.

In the U.S. Copyright Office's latest triennial rulemaking, EFF requested—and secured—6 anti-circumvention exemptions in 4 different categories.

Kit Walsh
STAFF ATTORNEY

In 2015, EFF defended your right to repair your own car and replace the software on your phone. We also worked to ensure that independent researchers could evaluate and improve upon the code controlling these devices, exposing security flaws or software that undermines your privacy or the environment. To do this, we worked through a rulemaking process run by the Copyright Office. The process takes place every three years, and lets us address some of the problems caused by Section 1201 of the Digital Millennium Copyright Act while we work for a broader solution.

Last year, we called on the public for help explaining the broad and varied impact of 1201 on vehicle repair and tinkering. We heard from from independent mechanics who had to subcontract out computer work to the dealers and a programmer who wanted to reprogram her car's locks after the dealer broke the software. We heard about family traditions of tinkering with cars in the driveway, encouraging curiosity about how things work and teaching the ability to be self-reliant. We heard from innovators trying to make tools and software that keep cars in better repair, reduce fuel consumption, and protect the environment. We heard from an Alaskan who had to tune his car to optimize for cold-weather performance and from performance tuners who lawfully modify cars for off-road racing.

"...we called on the public for help explaining the broad and varied impact of 1201 on vehicle repair and tinkering."

These stories were powerful, not just at the Copyright Office, but for us at EFF, too. When someone writes to you explaining how your work impacts their life, that they want to change the world and don't know how, and that they count on you to take their story and use it effectively to protect their freedoms and everyone else's, that's tremendous. It's one thing to say, "we're EFF and we have 25,000 members." It's quite another to tell the actual stories of varied and amazing people who care deeply about the freedoms at stake.

Title II reclassification drew bright-line rules to protect the open Internet.

Jeremy Gillula
STAFF TECHNOLOGIST

"Who the fuck are you, anyway, EFF? Why are you stirring up so much trouble, and who pays you?"

–T-Mobile CEO John Legere, in response to an EFF tweet

It's not every day the CEO of a major telecommunications company curses at you via Twitter. But when one does, it might be a sign that whatever you're working on has an impact.

Since joining EFF, I've provided technical expertise for our net neutrality work, explaining things like the end-to-end principle or the network stack, writing blog posts about how important ISP transparency is to Internet innovators, and gathering signatures from computer scientists for our amicus brief. The work comes in bursts, with a huge push in early 2015 when we urged the FCC to issue regulations to protect and promote a neutral and open Internet by both creating some bright-line protections and refraining from claiming broader authority to regulate the Internet. While we won that battle—the FCC published its Open Internet Order in March 2015—our fight didn't end there: when the telecom companies subsequently challenged the FCC in court, we filed an amicus brief in support of the FCC's position, even as we continued to watch closely to prevent FCC overreach under the new rules. The latest burst

came when we decided to see what exactly ISPs were trying to get away with, now that fast lanes and paid prioritization are banned—and that's where T-Mobile's Binge On program came in.

We first heard about Binge On when it launched in November, but it wasn't until we read stories suggesting that T-Mobile was throttling all video traffic for Binge On users that we thought to look into it. In classic EFF style, I performed a thorough technical investigation on a shoestring budget. My test setup consisted of a pre-existing EFF server, a CC-licensed video (Sita Sings the Blues, if you're curious), and a co-worker's T-Mobile phone. Armed with these and some technical know-how, I was able to take enough data to confirm that T-Mobile was indeed throttling video—not optimizing it in any rational sense of the word—and that the only way to prevent the throttling was to turn off Binge On or use HTTPS. Data in hand, I got confirmation from a T-Mobile employee and wrote a blog post describing my findings.

"In classic EFF style, I performed a thorough technical investigation on a shoestring budget."

It didn't take long to get T-Mobile's attention. CEO John Legere announced a Twitter Q&A to clear up any misunderstandings about how Binge On worked, so EFF asked him to come clean about whether Binge On was just throttling in exchange for zero-rating, or if it actually did any sort of optimization (as T-Mobile continues to claim in all its public documentation). As for his response… well, the rest is history.

The press picked up his comments, and a flood of EFF supporters tweeted at Legere to explain just who we are, and why they pay us. One of my coworkers even got me an official EFF Stirrer of Trouble (a *molinillo*, a beautiful wooden whisk used to prepare Mexican hot chocolate). Now, whenever I have doubts about the importance of what I'm working on, I see the Stirrer of Trouble and remind myself that that's what we're here for: to stir up trouble for anyone and everyone who threatens a free and open Internet.

FINANCIALS

The financial report below gives details for the Electronic Frontier Foundation's fiscal year from July 2014 to June 2015.

EFF has a four-star rating (the highest possible) from watchdog Charity Navigator, a non-profit organization dedicated to providing an unbiased, objective, and numbers-based assessment of over 8,000 charities.

Contributions from more than 25,000 dues-paying members from around the world form the backbone of the Electronic Frontier Foundation's financial support.

FY 2015 INCOME

INCOME

- Individual: $4,724,024
- Individual through Foundation: $4,234,586
- Humble Bundle*: $1,533,635
- Foundation: $998,659
- Corporate: $784,734
- Cy Pres: $3,743,826
- In-kind Legal Services: $237,464

Total Income: $16,256,928

EXPENSES

- Program: $7,153,752
- Fundraising: $1,150,243
- Administrative: $1,120,915

Total Expenses: $9,424,910

FY 2015 EXPENSES

INCOME

PUBLIC SUPPORT

Corporate Contributions		
*Humble Bundle Contributions**	$	*1,533,635*
Other Corporate Contributions	$	*784,734*
Total Corporate Contributions	$	2,318,369
Foundation Grants	$	998,659
Individual Contributions Through Foundations	$	4,234,586
Invididual Contributions	$	4,724,024
Cy Pres Awards	$	3,743,826
In-kind Legal Services	$	237,464
TOTAL PUBLIC SUPPORT	**$**	**16,256,928**

REVENUE

Net Investment Income	$	254,711
Attorneys' Fees Awarded	$	95,306
EFF Event Income, net of expenses	$	- 14,521
Miscellaneous	$	169,622
TOTAL REVENUE	**$**	**505,118**

TOTAL SUPPORT & REVENUE $ 16,762,046

EXPENSES

Amortization & Depreciation	$	197,867
Building Expenses	$	178,744
Corporate Insurance	$	106,274
Fundraising Expenses	$	1,914
Furniture and Equipment Under $5,000	$	83,837
In-Kind Legal Services	$	243,693
Intern Expenses	$	24,162
Legal and Professional Fees	$	626,998
Litigation Expenses	$	212,404
Membership Expenses	$	323,894
Office Expenses	$	85,712
Salaries & Benefits	$	6,877,716
Staff and Board Enrichment	$	190,635
Travel Expenses	$	240,303
Other Administrative Fees	$	24,007
TOTAL EXPENSES	**$**	**9,418,160**

NET INCOME $7,343,886

* Individuals specify a portion of their payments for games, books, and other digital content through Humble Bundle to go to EFF. For more information: https://www.humblebundle.com.

THANK YOU

For 25 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.

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/ARP15, 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+) ..... sticker pack
- ◯ 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/contribute.
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.
ARP15