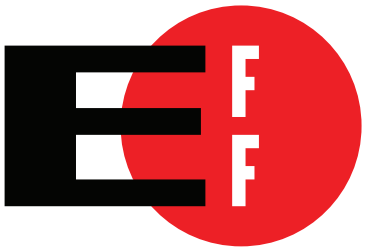

2016
ANNUAL REPORT



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 30,000 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 2016.

TABLE OF CONTENTS

A WORD FROM OUR EXECUTIVE DIRECTOR

Dear friends,

EFF, like the rest of the country and the world, entered a new era in 2016.

Early in the year we returned to our roots in the Crypto Wars, standing with Apple as it resisted the FBI's attempt to make the company weaken the security it offered to users. We also continued to combat bad patents, including putting pressure on universities to stop selling to patent trolls. We saw strong growth in the Electronic Frontier Alliance, which helps spreads EFF's core values locally by bringing together groups at universities and communities across the nation to share ideas and strategies for protecting the Internet. We fought hard to protect the balance between copyrights, publicity rights, trademarks and free speech.

The 2016 election, however, ushered in new challenges and revived some old ones. Our full-page ad in Wired put the technology community on notice: "Your Threat Model Has Changed." After a dramatic increase in demands to search devices at the border, as well as demands to turn over social media passwords and other cloud credentials, EFF quickly turned to update our border search white paper, with sections on processes, law and technology that call upon our broad range of expertise. We included a pocket guide with key issues that travelers can carry with them, and solicited stories for a potential test case. We fought and then responded to the rollback of ISP user privacy protections enacted by the FCC and continue to push back on the effort to repeal the hard-won network neutrality rules.

When civil liberties come under threat, we challenge the powerful—from those in high office to those in big business—to establish limits and protect people. We know that freedom and justice aren't automatic or made inevitable by technology. If we want our technologies—which today are woven throughout our communities, our laws, our culture, and our very lives—to support freedom and justice, we have to fight. Hard. We may even need to refight some battles to protect our past victories. But EFF has fought for 26 years to build a free and fair future. EFF has countered abuses of power through four presidential administrations so far, and we know how to fight a battle uphill.

We're also as strong as we've ever been, thanks to you. This has always been work that we do together, and our members have kept EFF a powerful watchdog for digital rights since our first case in 1990.

In 2017, we will fight for encryption, challenge the reckless deployment of state-sponsored malware, oppose mass surveillance of our digital communications, defend network neutrality and the freedom of the press, protect online creativity and innovation, and push back against government and private surveillance and censorship of social media. Attorneys will bring lawsuits, technologists will encrypt the web, and activists will organize, share, and engage. EFF will be there.

Stand with us. Donate to EFF.

Cindy Cohn, Executive Director

Featured Story: Apple v. FBI

A Dangerous Precedent

David Greene
CIVIL LIBERTIES DIRECTOR

I was on an airplane with spotty wifi, returning to San Francisco from a deposition, when the news broke: A judge had issued a preliminary order requiring Apple to create vulnerabilities in iOS so that the FBI could disable security features and get access to the San Bernardino attacker's iPhone. By the time I reached the EFF office, our lawyers, technologists, and activists had already sprung into action.

The danger posed by the FBI's request was obvious. By requiring Apple to weaken the security of its operating system, the court's approval of the FBI's request set a precedent for similar requests in the future. And the FBI's request in many ways brought to light the ongoing nature of the Crypto Wars—the failure of law enforcement to see cryptography as broadly necessary, even if it made it marginally more difficult for them to get information in investigations.

It was an easy decision to file an amicus brief supporting Apple's motion to vacate the order. But figuring out what we would say was more difficult.

I like bringing First Amendment free speech arguments where they might not be immediately obvious, and this seemed like a great opportunity to do so. The First Amendment not only protects against limitations on one's right to speak, but it also sharply limits the government's ability to require one to speak. This "compelled speech" doctrine applied here, because the order to write new code required Apple to speak in two ways: first, to write the code; and second, to certify that the new code was authentic.

We also had to figure out whom we would be representing with the brief. Although many times we will simply file a "friend of the court" brief on behalf of EFF, this time we had a unique opportunity to represent a group of "friends" with a particularly relevant expertise. So we gathered 46 cryptographers, researchers, and technologists—including pioneers in digital signature technology—and explained to the court on their behalf why the court's order compelling coding was, in this case, compelling speech.

The FBI's request generated a ton of interest. Ours was one of 22 amicus briefs filed, and we spent days fielding press requests.

The FBI ended up withdrawing its request before the court had to rule on it. Instead, the FBI purchased a vulnerability that, the FBI maintains, allowed it to bypass the security features without Apple's assistance. A few of us were in the airport on our way down to the hearing when that happened—we fielded the first round of press calls from an airport lounge.

Although the court never had a chance to rule, I am confident that our brief was influential and will remain so for years to come. We articulated an argument that the government had not likely fully considered; they'll have no choice but to consider it in the future.

Set good precedent. Donate to EFF.

Defending Encryption Against Bad Legislation

Rainey Reitman
ACTIVISM DIRECTOR

When I read the first draft of the legislation, I was stunned. The bill being floated by Senators Dianne Feinstein and Richard Burr was terrifyingly vague and wide-ranging, raising as many questions as it answered. It seemed to require technology companies anywhere in the country to decrypt data for the government. In essence, it would bar future tech companies from offering truly secure end-to-end encryption as a consumer product.

As an advocate for digital rights working with coalitions around the globe, I use end-to-end encryption for sensitive conversations every day. Would basic tools I use everyday—like Signal, PGP, and WhatsApp—be banned or undermined?

I called one of the attorneys on staff who was also reviewing the bill. "Is this as bad as I think it is?" I asked.

"It's worse," he confirmed.

The draft bill was floated in April 2016, in the wake of a heated battle about whether Apple could be forced to defeat its own security tools in response to a court order. Even as our attorneys were fighting in court, EFF supporters were speaking out in defense of encryption, many even taking to the streets for public demonstrations. I got on the phone and began reaching out to other advocates, beginning to build a coalition to fight this new proposal.

But things got worse. Even as we began reaching out to contacts on the Hill and began writing publicly to draw attention to the Burr-Feinstein bill, the California legislature began to move a similar proposal. The Assembly Privacy and Consumer Protection committee held a hearing on a bill that would have banned the sale of any phone that could not be decrypted.

Now we were fighting on two fronts. On state and federal levels, elected officials were trying to create a backdoor into our digital lives. And that would leave us all less secure.

The next few months were a whirlwind of campaigning. EFF engaged tens of thousands of people in learning about this issue and speaking out through social media and online campaigns. We launched a petition to Obama that garnered over 100,000 signatures demanding he oppose backdoors. EFF convinced dozens of major tech companies—including Amazon, Apple, Dropbox, Facebook, Google, Twitter and WhatsApp—to publicly speak out against backdoors. Encryption backdoors were even featured in John Oliver's Last Week Tonight.

In 2016, thanks to countless people who took the time to speak out online and call their members of Congress, we won. We stopped the government officials who wanted to make all of us less secure by forcing tech companies to build backdoors into their products.

I'm worried about the future. I'm worried that right now, we're at a lull in the fight, and that we'll be facing an even tougher battle over the right to encryption next year. But thanks to the awareness we've built and the community of resistance we've cultivated in the last 12 months, we're in a better position than ever to defend digital security against future attacks.

Defend encryption. Donate to EFF.

Crypto Wars 2.0

Seth Schoen
SENIOR TECHNOLOGIST

I was 13 when I first heard about the Crypto Wars. A spate of press coverage of cypherpunks and privacy advocates struggling to get privacy tools into the public's hands was followed by news that the government was proposing its own data security alternative, the Clipper chip, with a backdoor to allow the government access to people's phone calls.

That summer brought electrifying news. A mathematician named Daniel J. Bernstein had been told by the government that he couldn't publish his encryption software on the Internet—they regarded it as a "munition" subject to export controls, and publishing it online was deemed to be an "export." Everyone at my math camp seemed to be talking about it. How had math become front-page news? Could the government really stop people from publishing their research?

A year and a half later, in 1995, I first heard of Cindy Cohn (now EFF's executive director). Cindy signed on as Daniel Bernstein's lawyer and was defending her client's right to publish his ideas online—making the pioneering claim that "code is speech." I looked up to Cindy and her colleagues for their creative (and successful) defense of what crypto could mean for everyone.

The Bernstein case was just one of the conflicts in the 1990s around the right to publish and use encryption tools. It's easy to forget how software developers avoided encryption features then, entirely because of threats of criminal penalties for developers who published crypto without a license. The government also pursued other angles to prevent strong crypto from becoming mainstream. It pushed Clipper and other "key escrow" approaches with backdoors the government could use. Some companies even agreed to

deliberately weaken their crypto implementations to avoid running afoul of the government, a decision that's still causing harm today.

EFF fought hard on all these issues. By the turn of the millennium, the Crypto Wars were seen as ending in a victory for privacy advocates. The government liberalized its rules and stopped threatening researchers and software developers; encryption was rolled out as a basic part of technology infrastructure. "The code rebels beat the government," Steven Levy said in a 2001 history: The conflict was apparently over.

But in 2010, the FBI's general counsel presaged a new round in the Crypto Wars with a speech complaining that ubiquitous encryption was harming law enforcement, and calling on technology companies to figure out how to let the government get around it. Since then, officials have seemed to call for mandatory back doors. Once again, they've asked that our tools be intentionally weakened to give the government access to spy on us—a demand the government had backed down from a decade earlier.

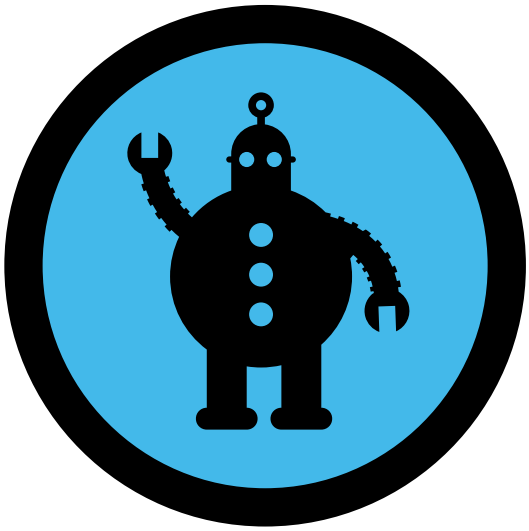
Since then, EFF has been fighting the second Crypto Wars, standing up for technologists' right to make the most secure tools they know how, and the public's right to access those tools.

Back at my math camp, I'd never have expected to see these fights from the inside. The EFFers and crypto community fighting them seemed like mythic figures I might never meet, let alone work alongside. Yet as an EFF staffer since 2001, I've been a part of it, whether writing code or testifying to the National Academies. I've been able to lend a hand to many of these efforts in ways I couldn't have dreamt of.

At the same time, it came as a shock for me to realize that these battles had to be fought again. These conflicts didn't, in fact, end in the clear victory they'd once seemed to.

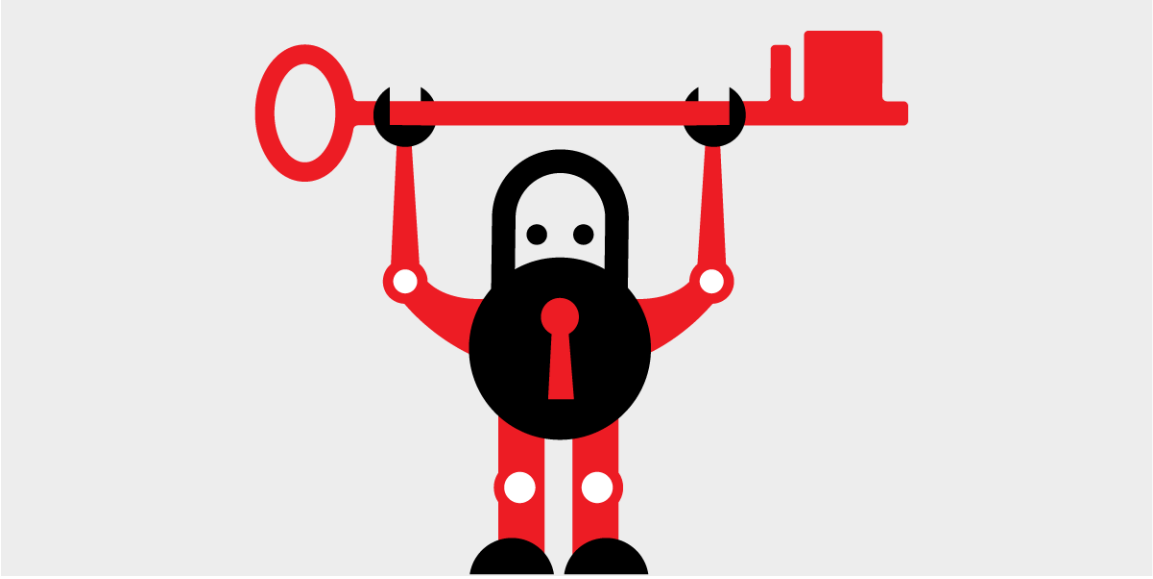
But after a quarter-century of experience, defending strong crypto is deep in EFF's DNA. We helped start the Let's Encrypt project, which has enabled tens of millions of web sites to offer secure encrypted connections. We're pushing companies to keep rolling out crypto and not to compromise on privacy and security. We're in court arguing that the government can't make technology makers like Apple weaken their security. We're teaching people from all walks of life how to protect themselves with encryption. We're working to understand clandestine government efforts to weaken and subvert crypto. We're letting everybody know what's at stake, and we'll do it as many times as we need to.

Do the math. Donate to EFF.



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.



Certbot

Noah Swartz
STAFF TECHNOLOGIST

When I first started at EFF nearly two years ago, I had no idea how to get an SSL certificate or enable HTTPS on my website. I had put sites up on the web, and I knew the security benefits, but I had never jumped through the hoops required to set up HTTPS. I knew that encryption was important, but didn't think that my websites were important enough to warrant the time or cost of getting them a certificate.

I remember one of my co-workers filming me trying to get a certificate, to show in her Defcon talk about Certbot. Four hours later, despite being someone who could whiteboard out how the underlying encryption actually worked, I still hadn't managed to complete the process. I knew that with Certbot this would get easier, but after that day I was convinced that we were solving a worthwhile problem.

Shortly after my dreadful certificate acquiring failure, I joined the Certbot team, excited to work on the tool that'd solve my and so many other people's problems. While I was laboring away at my computer fixing bugs and adding features, the world noticed its usefulness as well. Every bug report fixed was another site that could enable security for its visitors. Soon my websites were encrypted and I was getting emails from

friends and strangers to help them with their own sites. With a tool like Certbot there was no reason that any site shouldn't have HTTPS enabled.

Last year we watched as the web crossed the line of having more than half of all page loads done over HTTPS—in large part due to tools like Certbot. By the end of 2016, about 25 million sites were serving certificates obtained through us. I kept running into people who had used Certbot but had never heard of the EFF!

The responses were unanimous and positive. At conferences, the mere mention of Certbot would get me surrounded by people wanting to share stories about how much they liked it. Systems administrators gushed about how easy it had made their jobs, and people who maintained their own personal websites thanked me for how much money it was saving them, and how easy it was to use the first time. The most common response I got when I asked how the process of getting a certificate had been—"It just worked!"—was much different than my own four-hour debacle. The biggest complaint I heard was that people had already bought a certificate from another provider before hearing about Certbot. Pretty soon I didn't even have to evangelize it—merely mentioning its name would lead someone to jump up and sing its praises to anyone around who hadn't heard of it.

Sometimes the work we do at EFF can take a long time to show results. Even if we get the perfect case in court, it can take years to be decided; a victory in blocking a bad bill can be the first of many such fights. Certbot has provided me with a way to see immediate and impressive results. Being able to sit with someone for less than a minute and watch a green lock icon appear next to their URL is a constant source of joy.

We hope for Certbot to become the gold standard in HTTPS enabling technology. Every day I feel like we're one step closer to removing any last excuses for not using HTTPS.

Keep it simple. Donate to EFF.

Security Trainings

Soraya Okuda

PROJECT MANAGER,
SECURITY EDUCATION

"Can I have a sticker?" is a request I'm very familiar with.

Before my life as designer for the digital rights community, I was a fledgling elementary school teacher, rewarding collective good behavior with stickers at the end of class.

It's hard being a new teacher, but thankfully there are resources: networks of teachers in similar districts teaching the same subject matter, websites where you can download, remix and share materials, and places where you can review alternative ways of structuring lessons. When I didn't find the resources I needed, I made my own, and found that I loved creating and sharing educational games, slides and handouts.

I went to an education master's program to immerse myself in the practice of making free, accessible learning materials for groups in need. After hearing many intelligent people disclose that they felt defeated when learning privacy-protecting tools, I focused on making digital security approachable for non-technical audiences. Designing security educational materials led me to EFF's Surveillance Self-Defense (SSD), and I'm excited to be giving back by expanding SSD as a resource hub for security educators.

In 2016, EFF received a flood of digital security requests: from groups asking for trainings for their communities, to EFF members and civil society groups seeking guidance about how

to teach digital security. Though EFF provides trainings on a limited basis, the solution was not to send more staffers to train. We decided to expand our educational materials in SSD for those who want to help their communities learn digital security.

Teaching is an art that requires mindful facilitation, a thoughtful layering of content, trust, and a deep sensitivity to the implicit needs and concerns of the audience. The additional challenge of teaching a topic like digital security is to factor in learners' varying levels of fear, distrust, personal safety, linguistic and technological fluency, and contexts. Moreover, each person's relationship to their devices directly affects their learning experiences, including what machines they use, how they interact with social networks, their daily workflows, their attitudes towards adopting new tools and practices, and their comprehension of various risks. What people learn—or don't learn—has real repercussions.

Nobody knows this better than digital security trainers working within movements and with at-risk groups around the world, and we've been tremendously fortunate to learn from their expertise. We've interviewed dozens of U.S.-based and international trainers about what learners struggle with, their teaching techniques, the types of materials they use, and what kinds of educational content and resources they want. We're working hard to ensure this is done in coordination with the powerful efforts of similar initiatives, and we seek to support, complement, and add to that collective body of knowledge and practice.

The project also requires frequent critical assessment of learners and trainers, with regular live-testing of our workshop content and user testing evaluations of the SSD website. It's been humbling to observe where beginners have difficulty learning concepts or tools, and to hear where trainers struggle with using our materials. With their frustrations fresh in mind, we continue to iterate on the materials and curriculum.

Expanding SSD for trainers is a cross-organization initiative requiring interdisciplinary expertise. It's been amazing to project plan with Kim Carlson, Jillian York, Eva Galperin, Noah Swartz, Bill Budington and Danny O'Brien, and collaborate with Elliot Harmon, Camille Ochoa and Shahid Buttar to meaningfully incorporate Electronic Frontier Alliance participation and U.S. trainers' concerns into the process. I've learned so much from our adviser Carol Waters, whose work on the state of trainings for journalists and the security curriculum for LevelUp first inspired me.

It's been a dream to collaborate with the training community on improving learning outcomes. I'm moved by our shared vision for sustained impact, and how these efforts will help people to be safer. Together, we can improve as security educators and help communities in need learn about digital safety.

Earn a sticker. Donate to EFF.

Standing Rock

Stephanie Lacambra

CRIMINAL DEFENSE STAFF ATTORNEY

Law enforcement is very good at deploying its most disturbing digital surveillance techniques strategically, so as to minimize public outrage. In particular, the government knows that if it starts with unsympathetic or marginalized groups, the broader public may be slow to realize the impact. The FBI's use of malware to hack into the private computers of countless individuals all over the world is a good example. As long as it was done in the name of apprehending suspected traffickers of child pornography, many would be reluctant to condemn it. We saw the same phenomenon in the use of cell site simulators (commonly known as stingrays) to track the location or disrupt communications of political protestors, from Black Lives Matter to the water protectors at Standing Rock.

More broadly, we know that our criminal justice system disproportionately impacts the poor and communities of color. I was first drawn to criminal defense work because I wanted to be a champion for the most vulnerable and disenfranchised in our communities who needed our help the most. Focusing on the surveillance tools used to marginalize these communities seemed like a natural next step.

As a newbie to EFF last year, I was thrilled to get the chance to travel out to Standing Rock, North Dakota to investigate suspicions of law enforcement interference with water protectors' digital communications. EFF had received many distressing accounts of pipeline protes-

tors experiencing bizarre cell phone behavior and unusual interruptions in their live streaming and posting abilities while on the ground at Oceti Sakowin, the main water protector camp.

When I arrived at Standing Rock, the weather conditions were frigid and the Internet connectivity was sparse. Press volunteers braved the freezing temperatures on the highest elevation at camp, dubbed "Facebook Hill," to attempt to publish their firsthand accounts of law enforcement actions as they unfolded.

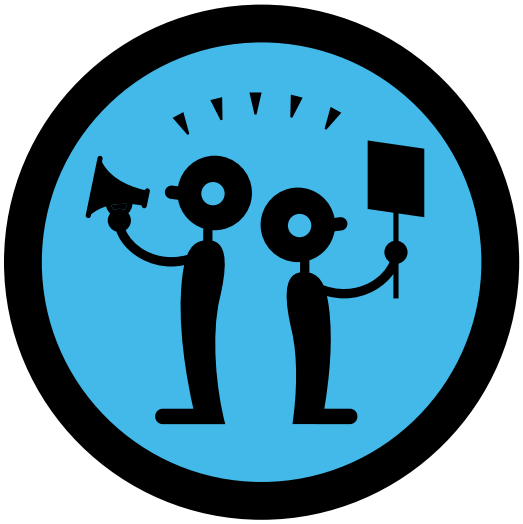
Many water protectors complained of strange behavior in their digital devices: sudden and unusual battery drainage, weird echoes or background noises during their phone calls, Facebook post threads disappearing completely, cell cameras and microphones mysteriously turning on and recording. People's suspicions were only exacerbated by the omnipresent, low-flying helicopters and biplanes circling the camp hourly, day and night.

I spoke with everyone—journalists, activists, technologists, and other volunteer lawyers—about their digital communication experiences at Standing Rock. One activist noticed their cell phone spontaneously sharing their location with one of their contacts without their permission. Others reported cell phones surreptitiously turning on and recording the activity around them, an issue of particular concern for the legal volunteers trying to conduct confidential interviews with their clients. I received so many reports while on the ground that we set up a web portal for witnesses to continue to report even after I left.

We're still reviewing the readings from the IMSI catcher detection applications and analyzing the logs, but our preliminary examination seems to indicate unusual interference with digital communications of water protectors at Standing Rock. But the real work is discerning the causes for these interruptions and whether they can be attributed to a specific body or organization. Unfortunately, the nature of cell site simulator technology—and the current state of cell site simulator detection software—makes it very difficult to drill down and identify those who deploy it. EFF put out a call to technologists this year to develop more precise anti-surveillance software, specifically cell-site simulator detection applications. We hope this will help us get some answers and further the fight against government surveillance and intimidation of protestors.

Transparent accountability is an essential safeguard against abuse of power. In a perfect world, I'd want law enforcement to protect the dignity and humanity of ALL Americans–especially communities that have been historically targeted—and embrace judicial and public oversight of their acquisition and use of surveillance technologies. In the meantime, I'm proud that we're able to combat misconduct by public officials entrusted with safeguarding our freedoms and safety, even if just by letting them know that we're watching.

Police the police. Donate to EFF.



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.

Electronic Frontier Alliance

Shahid Buttar
DIRECTOR OF GRASSROOTS ADVOCACY

When EFF was invited to visit a library in Silicon Valley one weeknight in early 2017 to speak with a group of women interested in online privacy, I could never have predicted where that meeting would lead.

We learned, from the invitation, that a small group of women had been organizing monthly events to inform their neighbors about policy issues. We scheduled a phone call to learn more about their work, and learned that even though they had only begun organizing in the wake of the 2016 presidential election, they had already held several events, most recently pulling together 75 neighbors spanning three generations who, before leaving the room, wrote letters to their legislators following up on their discussions.

When I visited the library, we shared an hour together exploring the contemporary debate on mass surveillance, unpacking the history of politicized targeted surveillance in the U.S., the rationale for why privacy enjoys constitutional protection, and the metastasis of the surveillance state from national security agencies to local police departments. We also discussed local reforms sweeping the country that, where successful, could force transparency on the widely overlooked local dimensions of unconstitutional mass surveillance.

A conversation following the formal event included a student organizer from another Electronic Frontier Alliance group on the opposite end of the country who learned of the event while in town on spring break. He and the local organizers were able to trade notes about their respective projects.

That conversation also offered a chance to further inform the group's coordinators about a related state bill. Introduced by the state assembly member representing that district, it nodded towards our concerns but was unfortunately poised to undermine local campaigns around the country by setting an artificially low ceiling on reform.

Before the week was out, they took action. Acting independently on information shared both by our team and other grassroots allies across the Bay Area to whom we introduced them, the group's coordinators reached out to their state assembly representative and met with him in person to convey their concerns.

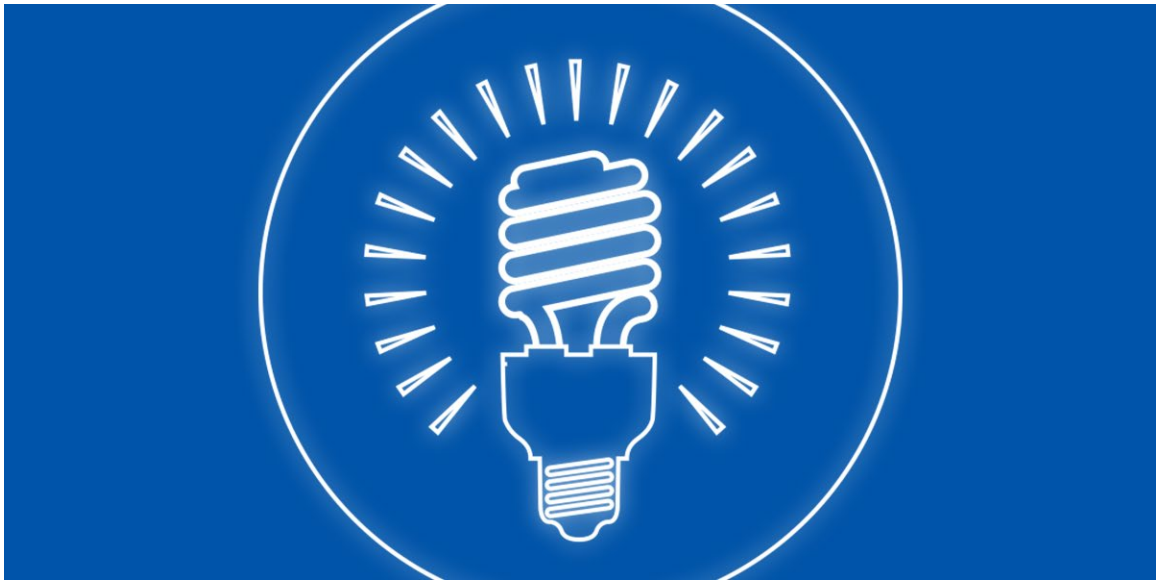
They proved persuasive. Within days, the legislator introduced amendments acknowledging concerns that EFF and other allied organizations had raised previously to no avail. Our expertise gained seemingly immediate traction once it was amplified by organized constituents, and helped prompt several rounds of amendments that took the bill from one we initially opposed to one we could consider enthusiastically supporting.

This story could repeat itself in ten thousand cities and towns across America. In fact, it must repeat itself (in at least many of those cities) before the national policy debate will seriously contemplate constitutional limits on mass surveillance.

While EFF fights digital dystopia in institutions like courts and Congress, the grassroots activists working in local communities under the banner of groups in the EFA do so at the same dinner tables where we won the movement for marriage equality.

Every time I watch someone grow inspired to raise a new voice in support of digital rights, I remember why popular sovereignty matters. Beyond being the basis for democratic legitimacy, it is the constitutional key to preserving liberty in a time of crisis. Building the EFA feels like a calling, an opportunity to help millions of other Americans join the struggle to champion timeless values like freedom of expression, access to knowledge, and creativity.

Raise your voice. Donate to EFF.



Reclaim Invention

Elliot Harmon
ACTIVIST

On February 22, 2013, the White House Office of Science and Technology Policy released a memo requiring every federal agency that funds scientific research to adopt an open access policy, ensuring that the research it funds is available to the public after an optional embargo period. For a lot of us in the open access world, the White House memo represented a massive victory, one we'd been working toward for years. It wasn't perfect—in the fast-moving world of scientific research, a one-year embargo period is far too long. But it was, at long last, a meaningful step in the right direction.

I was working at Creative Commons, one of EFF's allies in the fight for open access. The best way to describe the vibe in the office that day is, we won. I remember thinking that a chain of events had been set in motion that could not be stopped. Embargo periods would go down. Publishers would have to turn to open access or go out of business. It would be just a year or two before all academic research was available to the public the moment it was published, when a teenager on a Native American reservation in South Dakota would have access to the same body of knowledge as a postdoc researcher at Stanford. I remember saying to a colleague, "Well, time to find a new cause."

A couple years later, I was working at EFF in our fight against patent trolls, companies

that do nothing but hoard patents and use them to threaten real, practicing companies with expensive lawsuits. As I was getting up to speed on our patent work, I kept coming back to one question: where do trolls get their patents in the first place? Some notorious trolls have thousands of patents in their portfolios; they're surely not sitting around filing all of those patent applications themselves, right?

Many of the ways trolls get patents didn't surprise me much—they buy or license them on the cheap from inventors who never got their inventions off the ground or from companies that went out of business. But one source floored me: universities.

It's common practice today for universities to file patents on inventions that arise in the course of their research. The reasoning make sense: they want to find a company to bring that invention to market, and some partners might demand the surety of an exclusive license. But when a university licenses to a troll, the logic breaks down: trolls don't bring anything to market. Keep in mind that most of that scientific research is funded by the U.S. government. I thought back to the 2013 White House memo. Why did we go through the work of securing research outputs for the public if they were just going to be fodder for abusive litigation? If the purpose of an open access policy is to stimulate innovation, then some universities' patenting practices undermined that purpose.

In 2016, EFF launched Reclaim Invention, our new initiative to encourage universities to rethink their patenting practices. Since then, thousands of students, faculty members, and others in the university community have signed petitions demanding that their institutions pledge not to sell patents to trolls. As I write this, the Maryland legislature is considering a bill inspired by our work, a bill that would bar state universities from selling to trolls. And we hope to see more states do the same.

This campaign has made me realize something: access to knowledge is never finished. If Congress passed the perfect open access bill tomorrow, patent trolls would still find ways to use that publicly funded research against the public. And if we solve that problem, there'll be a new one. Don't get me wrong: we've had plenty victories, but the fight is never really over.

That's why I'm proud to work at EFF. Protecting privacy, free speech, fair use, and innovation at the same time requires thinking and moving fast. As we work to push back the latest constraint on your digital rights, we always have one eye on the horizon, watching for the next threat.

School patent trolls. Donate to EFF.

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.

National Security Letters

Andrew Crocker
STAFF ATTORNEY

Imagine this: You're forced to keep a secret. You wonder whether you should have to keep it secret at all. In fact, staying quiet feels almost dishonest. But you have no choice.

Years pass. You keep the secret so long that it feels like second nature. One day, all of a sudden, it's not a secret anymore. What does it feel like to share this secret that you never wanted but you've lived with for years?

For me, that's a window into how national security letters operate. Companies that receive NSLs are forced to stay silent, to the point that they cannot even say that they've received an NSL. For years, EFF has represented NSL recipients that know firsthand that these gag orders distort the public conversation about national security. The leaders of these companies deeply want to participate in this conversation, but the simple fact that the FBI served them with an NSL stops them from doing so. It stops even me, as their lawyer, from engaging in full public advocacy about NSLs.

Our clients have been fighting NSLs since 2011 and 2013, respectively. They embarked on this legal battle precisely because they disagree with a law that gives the FBI

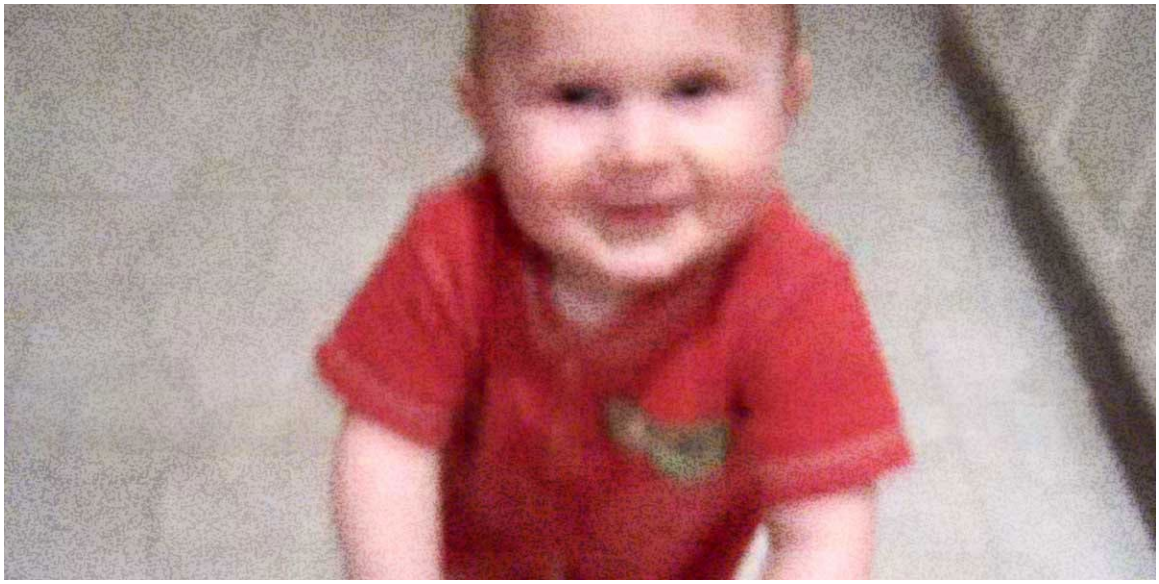
the power to gag them, potentially permanently, without ever going to a court. As the years passed, though, they couldn't help but get used to the secrecy that had been imposed on them. Every conversation we had, whether it was supposed to be about the case or not, had to grapple with this unwelcome duty. If they signed a letter in support of surveillance reform, would they be seen as tipping their hats? What about an amicus brief? And how coy did the answers to a certain reporter's questions have to be?

That's what made it such a strange moment when, in late 2016, I was able to call up our clients, CREDO Mobile and Cloudflare, and tell them they could finally identify themselves. As I explained what had happened, I was struck by how foreign it felt to be discussing a public statement in the companies' own names. It took real time to sink in.

It has been a privilege to represent these clients in standing up for their customers and for the principles of transparency that are at EFF's core. When they took on this fight, they had no assurance that a day of public recognition would come, and they did so nonetheless.

Of course, there's more to do. As of this writing, we're still seeking a ruling from the court of appeals that NSLs are unconstitutional. But I savor the feeling of telling our clients that those gags had been lifted.

Speak out. Donate to EFF.



Lenz v. Universal

Corynne McSherry
LEGAL DIRECTOR

Many of my friends know that I've been a huge Prince fan since I was a kid. I've seen the movie Purple Rain at least 5 times, and know every word of every song on the album—as well as many other Prince songs. When Prince died I cried, along with the millions of other fans who treasure his music. I do a mean air guitar of the "Let's Go Crazy" solo.

What many of my friends don't know is that I've been involved for close to a decade in a legal battle that started with that very song. Way back in 2007, my client, Stephanie Lenz, made a little video of her kids dancing in the kitchen and posted it on YouTube so her mother could see it. As it happens, they were dancing to "Let's Go Crazy." As it also happens, Prince was not fond of having his music online in almost any context that he couldn't control. His representatives at Universal Music sent a notice to YouTube accusing Lenz of copyright infringement. And YouTube took the video down.

Most people would just accept this kind of takedown. Stephanie Lenz is not most people. She was outraged at having her video silenced and she decided to fight back. She turned to EFF for help. We were glad to do it.

A big part of EFF's mission, and a part that means a lot to me, is to defend online fair

uses. We know that fair use is an essential part of our copyright system, because it helps make sure that copyrights don't block new creativity and innovation. For years we've seen copyright owners abuse the copyright system to take down fair uses. Under a law called the Digital Millennium Copyright Act, service providers have strong incentives to take down any content that is identified as infringing—including perfectly legal content. We think that's a problem.

As we argued in court, however, the DMCA also provides that copyright holders have an obligation to pause and consider whether uses they target are actually lawful, and come to a reasonable conclusion on the question. If they fail to do that, they can be liable for damages, including attorneys' fees. That provision is crucial to ensuring a balance between the rights and needs of copyright holders, service providers, and users. UMG didn't do that. If it had, it would have realized immediately that Lenz's video was a lawful fair use.

UMG disagreed. It claimed copyright holders don't have to consider whether a use is fair unless and until the user takes them to court. But if that's the rule, then the DMCA basically upended the balance between copyright and the First Amendment, giving any copyright holder the ability to take down lawful speech, without fear of consequence.

After years of litigation, we finally got a ruling, and it was a good one. The Ninth Circuit Court of Appeals stood with the users, holding that fair use is an affirmative right that copyright holders cannot ignore. But the court also said that even unreasonable conclusions about fair use might pass muster. We asked the Supreme Court to correct that error, but unfortunately, the Supreme Court decided not to take the case. We're disappointed, but proud that we stood with Ms. Lenz and helped clarify that the DMCA requires copyright holders to consider whether material they don't like is a nonetheless protected by law—before they send a DMCA notice that could take down a lawful fair use.

I've had people ask me, more than once, why EFF made such a 'big deal' about a little home video. Why not focus on political speech, for example, or news commentary, or a sophisticated and clever remix? But fair use isn't just for politicians, journalists and artists. It's for everyone—including stay-at-home moms. In a world where copying is ubiquitous, and everyone can create and share all kinds of works, we all need fair use protections. It's my job, and my privilege, to make sure we get them—even if it means I have to get in a fight with Prince.

Go crazy. Donate to EFF.

Hemisphere

Adam Schwartz
SENIOR STAFF ATTORNEY

I grew up reading books like 1984 and watching movies like Minority Report. So real-world government surveillance programs alarm me. I went to law school to learn to fight high tech spying, and I have been lucky to do so ever since, first at the ACLU and now at EFF.

Hemisphere is the dystopic spy tech that scares me the most.

Police across the country routinely use this secretive AT&T database to spy on our phone calls. Hemisphere may be the largest reservoir of telephone metadata every created. It grows by four billion records every day, and contains records dating back to 1987. On behalf of police, AT&T conducts complicated phone call pattern analysis to map our social networks, learn who speaks to whom, find multiple phones used by a single person, and track where people are when they make calls.

For many years, the police and AT&T hid Hemisphere from scrutiny by elected officials, the courts, and the general public. They did so with what police call "parallel construction," and what EFF calls "evidence laundering." That is, after police use Hemisphere to identify an investigative lead, they bury that lead. Then police recreate

the lead with a less controversial investigative tool, and disclose only that tool to the courts and the accused. That way, police dodge questions they don't want to answer about the legality of the Hemisphere program.

In 2013, the New York Times published a government record about Hemisphere, which for the first time brought the vast spying program to the public's attention. But many questions about the program remained unanswered.

So EFF sued the federal government to force it to answer those questions. In this and countless other cases, when the government tries to hide its high tech spying programs in the shadows, we use the Freedom of Information Act to expose the program to the light of public debate.

After we filed our lawsuit, the government gave us a document that I found especially memorable. This email, shared broadly among police officials, called Hemisphere "Google on steroids" and a "super search engine." This is very disturbing. People should be able to call their friends and family without having to worry that police officers, years later, will "Google" their phone records to learn their social relationships.

Of course, exposing Hemisphere is just a start. The next step is to abolish it. The database is incalculably large. The search engines are immensely powerful. Whoever holds the keys to this massive surveillance tool can pore over the minutiae of our social, political, and religious relationships, going back for decades. Among other things, Hemisphere can expose when we called a criminal defense lawyer, a newspaper reporter, a psychiatrist, a former romantic partner, a political dissident, or a reproductive healthcare facility. Yet police officers commonly use this tool with no judicial oversight.

We continue to prosecute our FOIA lawsuit. We hope to win access to hundreds of additional records about the abusive Hemisphere telephone spying program. Then we hope to end it. Mass surveillance technologies like Hemisphere might make a good sci-fi plot, but they should have no place in our free society.

Fight dystopia. Donate to EFF.

Respublika

Jamie Williams
STAFF ATTORNEY

As an organization dedicated to protecting online speech, EFF is not a fan of censorship. And that's putting it mildly. Efforts to censor, intimidate, and harass the independent media are particularly troubling. A free press is necessary to a free society; censorship of the press enables manipulation of public opinion, chills public debate, breeds conformity, and stifles dissent. As Thomas Jefferson famously said, "Were it left to me to decide whether we should have a government without newspapers, or newspapers without a government, I should not hesitate a moment to prefer the latter."

At EFF, we feel the same way. As an undergrad studying journalism, learning about cases in which the First Amendment prevailed over efforts to stifle the free press inspired my interest in law. It also instilled in me a conviction that a society is not truly free if its press is not free. That's why I'm happy to work at an organization that stands up for the rights of independent newspapers—not just in the United States but around the world. As a U.S.-based legal non-profit, we aren't able to easily challenge the legality of censorship efforts by oppressive regimes on their turf—where there's usually no such thing as the First Amendment. That's why we jumped into action when heard that Kazakhstan—a country notorious for its efforts to silence independent newspapers—was trying to use the United States' court system as a tool to censor independent newspaper Respublika. Not on our watch.

Respublika originally came to us with a small request—help them deal with their U.S.-based webhost, who was taking down their content in response to requests from Kazakhstan. The articles relied on documents and emails—all relevant to the public interest—that had been somehow leaked from the Kazakhstan government. Kazakhstan claimed they were hacked and that the webhost needed to take them down pursuant to a court order obtained in a Computer Fraud and Abuse Act (CFAA) lawsuit in New York.

We saw a bigger problem than simply dealing with the webhost. Namely, Kazakhstan was trying to use a "Doe" injunction—an injunction against the unknown "hacking" defendants—to censor an unnamed third party, Respublika. To us, Kazakhstan's blatant abuse of the injunction made the entire lawsuit look like a strategic attempt to censor Respublika.

We immediately decided to get involved—and to represent Respublika in challenging the underlying injunction in New York. We asked the court to clarify that the preliminary injunction could not be used to censor Respublika. The judge agreed with us, in a win for free speech. The court held that neither Respublika, nor anyone else not directly involved in the purported theft of the documents, could be barred from publishing emails, the "stolen materials." The judge also found that the preliminary injunction as applied against Respublika was an unconstitutional prior restraint on speech, in violation of the First Amendment.

But Kazakhstan did not stop there. It next subpoenaed Facebook for the names, email addresses, IP addresses, and MAC addresses of the users associated with Respublika's and another user's Facebook accounts. This concerned us, given the country's history of intimating, harassing, and arresting journalists. EFF filed an opposition to Kazakhstan's motion to compel Facebook to turn over the data. Facebook also opposed the motion for information about its users.

The First Amendment prevailed again. The magistrate judge ruled in favor of Respublika and Facebook. The judge recognized that "[t]he proposed discovery from Facebook, which involves Respublika, a news organization, raises significant concerns regarding the reporter's privilege and the First Amendment." The judge said it was "implausible that broad and essentially undefined expedited discovery with respect to Respublika and affiliated persons remains" was authorized in the case, especially in light of the New York judge's holding.

In January 2017, the clock ran out on Kazakhstan's lawsuit and the government dismissed the case. The closing score: First Amendment: 2; Kazakhstan: 0. We hope this score sends a clear message to anyone thinking about using the U.S. court system as a tool for online censorship: we are watching and ready.

Keep the press free. Donate to EFF.

INTERNATIONAL

We collaborate with program staff and with other groups throughout the world to share knowledge and explore solutions to challenges outside of the United States.

Onlinecensorship.org

Jillian York

DIRECTOR FOR INTERNATIONAL FREEDOM OF EXPRESSION

My first experience with online censorship was in 2005. I was living in Morocco and created a blog to write about my experiences. A few months after I arrived, the platform that I was using was blocked in the country. That experience led to meeting bloggers and anti-censorship advocates in the country and broader region, and eventually to my previous job at the Berkman Klein Center for Internet & Society at Harvard, where I researched online censorship.

I was thrilled to join EFF in 2011 and to take on an advocacy role. I was familiar with EFF's legal work, and joined our then-small international team as Director for International Freedom of Expression. I love that EFF fights for freedom of expression for everyone, everywhere—in my time here, I've advocated for jailed bloggers to the United Nations, written about censorship in dozens of countries, and worked with our allies in various countries to protect free speech.

One project I'm excited about right now is Onlinecensorship.org, which seeks to encourage social media companies to operate with greater transparency and accountability toward their users as they make decisions that regulate speech. In 2014, On-

linecensorship.org was among the winners of the Knight News Challenge, enabling us to grow our team and build the project.

We started Onlinecensorship.org at a time when social media users had just begun campaigning for freedom of speech on platforms like Facebook and Twitter—today, it's an issue that affects an increasing number of users and makes the news almost every day. These giant companies generally have the legal right to decide what speech they want to host, but we believe that they have a responsibility to their users to ensure that the spirit of free expression is protected.

The project collects voluntary data from users through a survey. Our team then analyzes the anonymized data and produces reports and recommendations for both companies and users. Because the project is a partnership with another organization, Visualizing Impact, I get to work with a fantastic team that spans more than five countries (and time zones!)—I believe that the diversity of our team enables us to better understand the impact that censorship has on different individuals and societies.

We've begun to see the influence of our work on other advocacy groups, on individuals, and on how online censorship is reported in the media. I'm excited for the work we have planned for the next year too, from speaking about Onlinecensorship.org at RightsCon to finding new ways of telling user stories through visual advocacy. It's amazing what a small team of people can do to create change!

Express yourself. Donate to EFF.

Shadow Regulation

Jeremy Malcolm
SENIOR GLOBAL POLICY ANALYST

When laws and policies that would harm user expression and privacy are developed in public, EFF has a great track record of engaging with policymakers and improving or defeating these measures. But when such policies are developed away from public scrutiny, it's much harder for us to share our insight and expertise in an effective way.

This problem has been a driving force behind quite a lot of my work at EFF, such as our opposition to closed, opaque trade deals such as the now-defeated Trans-Pacific Partnership agreement (TPP). But for all its many faults, even the TPP, as a formal intergovernmental negotiation, was more open and accountable than some of the informal arrangements that affect the rights and freedoms of Internet users.

These sorts of informal private agreements go by various names. For example, rightsholders and search engines agree on "codes of conduct" to demote links associated with copyright infringement, law enforcement agencies and social networks conclude "memoranda of understanding" to censor "hateful" speech, and pharmaceutical companies and payment processors push "guidelines" to cut off payments to online pharmacies.

Despite their disparate subject matters, these deals share a tendency to exclude users from participation in their development, and to operate with low levels of openness and transparency. This is especially problematic when governments are involved, promoting such deals in the name of self-regulation yet failing to ensure that the resulting agreements are inclusive, balanced, and accountable.

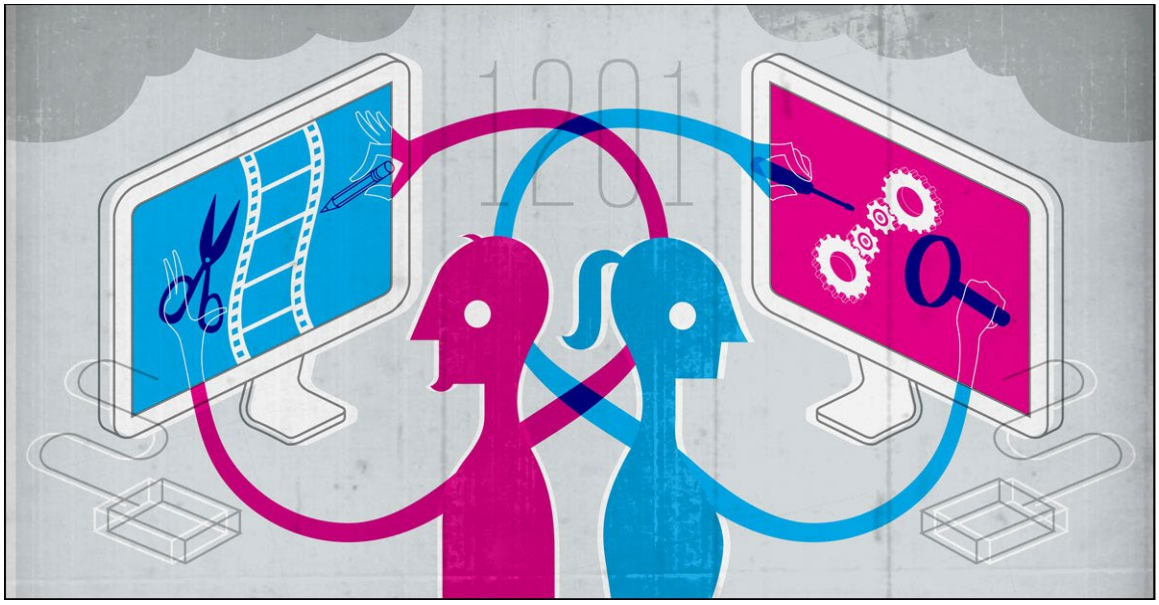
Although these agreements are nothing new, most people still don't know about this increasingly popular form of de facto Internet regulation and the systemic problems it creates. Our answer was to launch a campaign highlighting these secretive deals under the name Shadow Regulation, with an evocative graphic that illustrates how such seemingly innocuous private agreements can have sinister effects on users.

I touched a real nerve when EFF published a Deeplinks post of mine exposing how the pharmaceutical industry uses Shadow Regulation to pressure Internet and payment intermediaries to censor foreign websites that sell genuine pharmaceuticals to U.S. consumers for personal use. The CEO of one of the companies criticized in that post launched an all-out attack on our reporting via Twitter and his corporate website. This was a wake-up call to me about just how sensitive our adversaries can be when our reporting calls them out, and how important it is for us to stand firm when we know that we are right.

Light it up. Donate to EFF.

SPOTLIGHT: SECTION 1201

Since the Digital Millennium Copyright Act (DMCA) took effect in 2000, its "anti-circumvention" provisions have jeopardized fair use, impeded competition and innovation, and chilled free expression and scientific research. EFF is currently challenging Section 1201 in court as an unlawful restraint on speech.



Green v. DOJ

Kit Walsh
STAFF ATTORNEY

Imagine that you are a security researcher and you hear rumors that there are vulnerabilities in the technology people count on to keep financial transactions safe. So you buy one of the industrial-strength security modules used to encrypt such transactions, and you try to figure out if it can be hacked. It's your hardware, and it's not being used to handle anyone else's private data, so you should be able to open it up, right?

The government and big entertainment companies think otherwise.

Now imagine that you are a remix video enthusiast and you want to make your own art by mashing up video samples from high-quality video. Or you want to contrast two videos to show similarities or differences between them. Or a thousand other valuable activities that require you to manipulate high-quality video. Finally, imagine that you want to create a technology to let others do so. If copyright law allows people to make remixes within the bounds of "fair use," you should be able to give them the tool to make that right a reality, right?

Again, the government and entertainment companies don't think so.

What these scenarios have in common is that both types of activities are threatened by Section 1201 of the Digital Millennium Copyright Act. The law was supposed to prevent

infringement that could result from bypassing digital locks, but in practice its effects are primarily felt by those who are trying to engage in legitimate research and expression.

The Constitution doesn't allow those kinds of threats. So in 2016, EFF sued the government on behalf of a security researcher and a multimedia innovator, asking the court to vindicate the public's speech rights by striking down Section 1201. The case is captioned Green v. Department of Justice, and is pending in the District Court for the District of Columbia.

As we explain in our briefs, Section 1201 impermissibly represses free speech in several forms. First of all, it blocks all kinds of legitimate speech that rely upon remix of copyrighted works that are locked down by Digital Rights Management (DRM) technology. This includes educational speech, remix videos, documentary film, journalistic speech—anything that requires the ability to access locked-down content for reuse. It also blocks research into software and publications of research findings. Further, it directly prohibits the publication of software code—which is itself speech—that is capable of bypassing DRM. This further impacts the ability of security researchers to collaborate, teach, and verify one another's findings, which leaves us all less safe. After all, malicious hackers who discover and share vulnerabilities in pursuit of illegally exploiting them are not deterred by Section 1201.

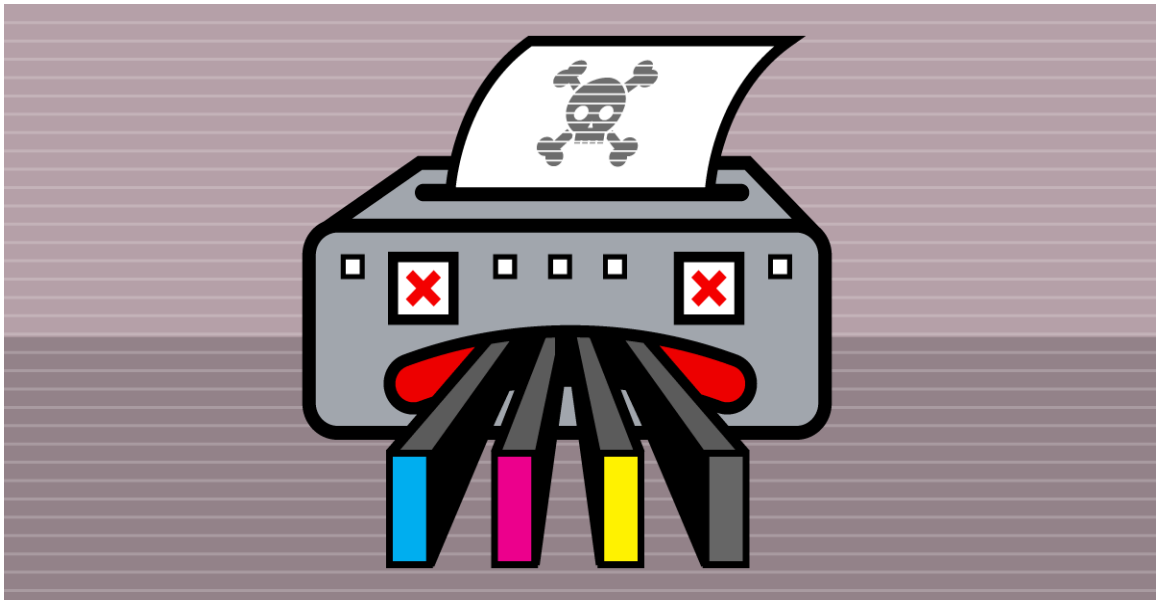
The law also creates a regime for licensing particular kinds of speech, something that is strongly disfavored in First Amendment law and needs to include strict safeguards that are not present in Section 1201. This regime is known as the "triennial rulemaking," conducted once every three years, at which members of the public can go and ask the Librarian of Congress for permission to engage in circumvention for particular purposes. The regime renders Section 1201 unconstitutional because the Librarian's discretion is not adequately bounded by firm standards of decision, and the procedure takes far too long and does not provide for judicial review. In our lawsuit, we also explain how the government strayed from the law in the way it conducted the most recent rulemaking and impermissibly denied or narrowed exemptions to which the public was entitled.

The lawsuit remains at an early stage, waiting for the judge to rule on initial motions.

Believe it or not, this summary has only scratched the surface of the harms done by Section 1201 and the reasons it has to go. We keep a collection of some of the worst abuses in our Unintended Consequences whitepaper.

EFF will continue to fight to ensure that technology enhances the ability to express oneself and learn about the world around us, rather than inhibiting it. One crucial step is getting Section 1201 out of the way.

Mix it up. Donate to EFF.



HP DRM

Cory Doctorow
EFF SPECIAL ADVISOR

In March 2016, HP pushed out a "security update" to millions of OfficeJet and OfficeJet Pro printers. But it wasn't a real security update: it was a booby-trap on a time-delay fuse, a piece of software that counted down in secret until September 2016, when it went off and triggered a hidden feature in all those printers, which allowed them to block third-party ink cartridges.

The result was chaos: people threw away their printers, assuming they'd broken down, they flooded third-party ink cartridge sellers with complaints, and gradually pieced together a picture of what HP had just done to them.

EFF swung into action with an open letter to HP CEO Dion Weisler, signed by tens of thousands of EFF supporters, calling on HP to admit what it had done, promise not to do it again, and make it right.

We won—kind of. HP did offer a patch that users could install to roll back the third-party ink blocker, and they did promise not to do this specific thing again, and they did apologize, in a roundabout way (think: "We're sorry you're angry at us").

The real issue here isn't just dirty tricks from hardware companies, it's the laws that enable them. Section 1201 of the DMCA has been used to intimidate and persecute anyone who reconfigures a software-enabled device to act in its owner's interests (accepting third-party ink!) and not in the interests of the device's manufacturer. If the dead hand of the manufacturer lies on your property after you've paid for it, ready to smack you any time you commit the sin of failing to arrange your affairs to benefit a distant group of shareholders, then you don't have property at all—you are merely leasing your smart devices, and that's not smart at all.

For me, HP is a canary in the Internet of Things coalmine. If they can coerce you to field-patch your "smart" printer to reject third-party ink, why couldn't your smart car patch to require one brand of gas (handshaked with the gas-nozzle), or your smart meter to work with only one kind of solar panel? We've already seen Philips patch its light-sockets to reject third party bulbs—just add a vision system to your toaster and it could reject third-party *bread*. If the DMCA protects any of this, it protects ALL of it.

That's why we filed a federal lawsuit last July to invalidate Section 1201 of the DMCA, and, in so doing, restore the balance that says, once you lawfully acquire a piece of property, it's YOURS. Yours to use as you see fit—as Blackstone wrote in the 18th century: property rights are the "sole and despotic dominion which one man claims and exercises over the external things of the world, in total exclusion of the right of any other individual in the universe."

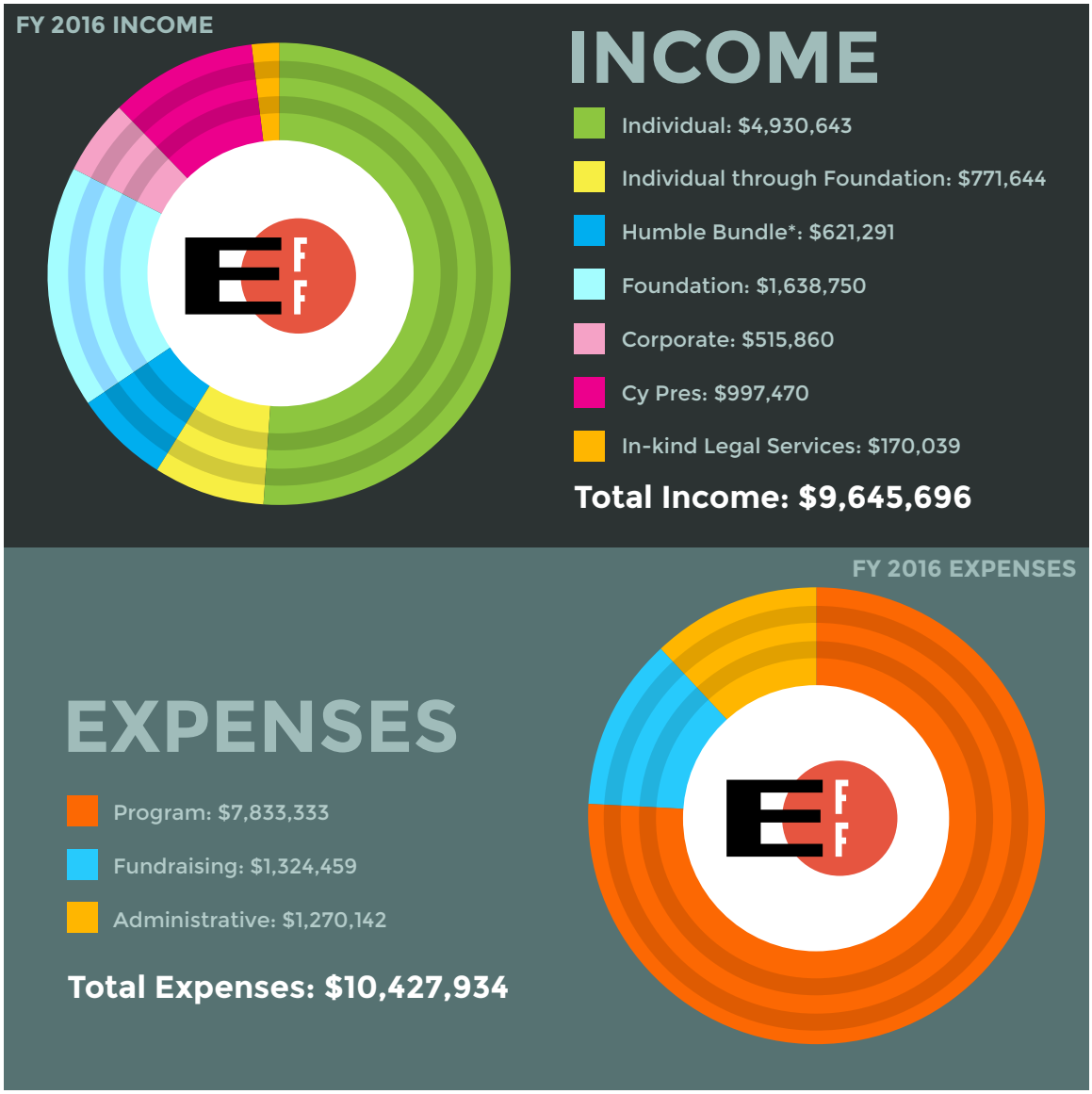
Own it. Donate to EFF.

FINANCIALS

The financial report below gives details for the Electronic Frontier Foundation's fiscal year from July 2015 to June 2016.

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



INCOME

PUBLIC SUPPORT

Corporate Contributions	
Humble Bundle Contributions*	*$621,291*
Other Corporate Contributions	*$515,860*
Total Corporate Contributions	$1,137,151
Foundation Grants	$1,638,750
Individual Contributions through Foundations	$771,644
Individual Contributions	$4,930,643
Cy Pres Awards	$997,470
In-kind Legal Services	$170,039
Total Public Support	$9,645,696

REVENUE

Net Investment Income	-$858,685
Attorneys' Fees Awarded	$89,475
EFF Event Income, net of expenses	$20,450
Miscellaneous	$84,465
Total Revenue	-$664,295

TOTAL SUPPORT AND REVENUE **$8,981,402**

EXPENSES

Amortization & Depreciation	$249,503
Building Expenses	$236,353
Corporate Insurance	$112,271
Fundraising Expenses	$1,845
Furniture & Equipment Expense	$109,920
Intern Expenses	$41,458
Legal & Professional Fees	$827,862
Litigation Expenses	$80,094
Membership Expenses	$344,567
Office Expenses	$123,192
Salaries & Benefits	$8,044,960
Staff & Board Enrichment	$90,593
Travel Expenses	$142,382
Other Administrative Expenses	$22,932

TOTAL EXPENSES **$10,427,934**

NET INCOME -$1,446,533

* 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 26 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/ARP16, 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.
ARP16