EFF

2018 ANNUAL REPORT

Since 1990, the Electronic Frontier Foundation has led the charge to protect our basic rights to privacy and free expression in the burgeoning world of technology. Increasingly, tech and the Internet are part of life whether you are texting a friend, navigating to a restaurant for lunch, applying for a library card, checking out test results from your doctor, or commenting on a cat video. The way we interact with the world has changed, and that presents as many challenges as opportunities. But along with over 30,000 dues-paying members around the world, EFF stands with you.

The EFF team is tireless in applying its deep understanding of law and technology to debates about civil liberties. We've earned our trusted voice in policy and legal debates thanks to a combination of unique expertise and decades of experience fighting for the users. This annual report features reflections from several EFF staff members about some of our most significant efforts in 2018, as well as financial information for the fiscal year ending in June of that year.

To learn more, read our Year in Review series:
https://eff.org/YearInReview2018

TABLE OF CONTENTS

A WORD FROM OUR EXECUTIVE DIRECTOR

Dear friends,

As people worldwide demand more control over their data and policymakers debate who gets to decide what's on the Internet, EFF remains a powerful force protecting the rights of technology users and small makers. Even in shifting political winds, our lawyers, technologists, and activists continue rising to the challenge with determination and unfailing dedication to preserving civil liberties. We have so much to be proud of, and I'm thrilled to share highlights from 2018 with you.

In this report you'll learn about how our team's deep expertise, creativity, and commitment to users made a difference in fights against censorship, surveillance, and government secrecy. We have excelled through adversity thanks to the support of motivated individuals like you from all over the world.

The digital horizon of 2018 was stormy. We saw the expansion of military-style surveillance tools applied domestically, broad-scale searches at the border, the rise of biased autonomous tools in criminal justice, and major setbacks to hard-won net neutrality protections. A growing climate of fear pervaded public discourse, leading to attacks on the free press and broader online censorship, too often silencing voices of those less powerful rather than the ones that are most pernicious. In a major blow to online speech and community, a coalition of the world's largest Internet companies helped pass FOSTA, the most extreme Internet censorship bill in over 20 years, which has predictably resulted in further injury to some of the most marginalized people on the Internet. Tension and further distrust of the companies that host our online forums were fueled by scandals including malicious bots sowing political division on social media and Facebook allowing Cambridge Analytica to violate user privacy at a massive scale. While the problems are clear, and increasingly recognized by the broader public, the responses proposed by many in power were often wrongheaded and dangerous.

Our team was relentless in both clearly explaining the issues and pushing back against bad laws, outdated Constitutional theories and bad policy. As our Surveillance Litigation Director Jen Lynch explains, the U.S. Supreme Court cited EFF's arguments in their ruling that the First and Fourth Amendments apply to government demands for location data. We now have 84 groups in the grassroots Electronic Frontier Alliance family, and last year we stood together with one in beating back a dangerous expansion of computer crime laws in Georgia. And that's just the start.

In turbulent times, when governments and companies put ideology and hunger for profits ahead of human rights, we don't rest and we don't back down.

In addition to the issues discussed in this report, we brought the fight against FOSTA to the courts. We won a major victory in our lawsuit challenging warrantless device searches at the border, beating back the government's attempt to have the case dismissed. We helped users avoid online tracking with a new release of Privacy Badger that detects and blocks a new class of evasive, pervasive third-party trackers. We continued to defend technologists and users against patent trolls, and finally killed off an outrageous podcast patent that threatened podcasters for years. These are just a handful of the ways in which EFF is making sure that technology users have an advocate in critical debates about how we will interact with one another and the world.

This work exemplifies our commitment to free expression, privacy, and the future of innovation. What's more, it shows what EFF is made of. In turbulent times, when governments and companies put ideology and hunger for profits ahead of human rights, we don't rest and we don't back down. EFF has embraced this tenacity and sense of duty since our founding nearly thirty years ago. The rights we secure today will define what lies ahead not only for technology users and makers, but for all who depend upon the basic right to explore ideas and have private conversations.

Thank you for standing alongside EFF and making a better digital future possible.

Sincerely,

Cindy Cohn, Executive Director

MILESTONES IN DIGITAL RIGHTS

TECH

We renewed our efforts to secure the email ecosystem with the relaunch of STARTTLS Everywhere, a project that enables email server-to-server certificate authentication.

We improved Privacy Badger to block new kinds of tracking, including link tracking on Facebook, Twitter, and Google.

We saw HTTPS support continue to rise, and had over a million daily active users and over five million downloads of HTTPS Everywhere just in 2018.

We helped expand Internet encryption with Let's Encrypt, which is now trusted by all major computer programs.

ACTIVISM

We led campaigns opposing the use of surveillance technologies on communities.

We launched Who Has Your Back: Censorship Edition, to shine a light on content moderation practices at social media platforms.

We continued our work to restore net neutrality protections and relaunched the Net Neutrality Defense Guide.

We expanded our grassroots outreach, working with local groups across the country to defend digital freedom.

LAW

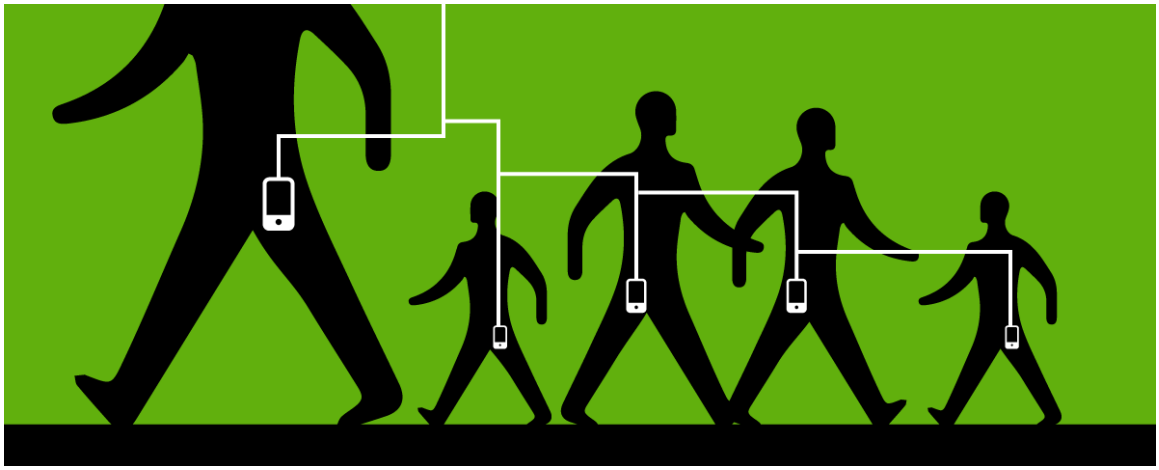
The U.S. Supreme Court cited EFF's amicus brief in Carpenter v. United States, a landmark decision holding that the Fourth Amendment protects cell phone location information.

We achieved final victory in our efforts to invalidate bogus podcasting copyright claims.

We defeated the government's attempts to dismiss our lawsuit challenging warrantless searches of electronic devices at the border and obtained discovery that bolstered our claims.

We continued to fight against Internet censorship and efforts to weaken innovation on the web.

PRIVACY



EFF AND THE CARPENTER VICTORY

Groundbreaking ruling recognizes our right to privacy in location data

Jen Lynch

SENIOR STAFF ATTORNEY

We've been fighting to protect people from the prying eyes of government for many years, but one of our longest-running battles is against warrantless police access to location data generated by our cell phones. In 2018, in a Supreme Court case called Carpenter v. United States, we had a huge victory. To link a defendant to a string of robberies, the government obtained 127 days' worth of cell tower data—without a warrant—to try to place him at the scene. The Court held definitively that the Fourth Amendment protects historical cell phone location information.

Part of EFF's core mission is to maintain the civil rights that we've always had in the offline world in an era when technologies like cell phones, computers, activity trackers, or smart home devices capture more personal details about us than ever before. These modern conveniences have made it easier for us to connect with family and friends, find our way around the world, and do so much more. But they have also made it easier for companies, governments, and especially law enforcement to track us and learn intimate details about our lives.

I believe it's vital that the government not be able to track us everywhere we go, and equally important that we benefit from new technologies. If we know that the government has access to records of our sensitive information, we may be less likely to use those tools. More importantly, we may be less likely to participate fully in society

when we know the government is watching. This chilling effect is especially true for communities that are already over-policed or marginalized. For example, when the NYPD was surveilling Muslim communities in New York and New Jersey, community members reported they were less likely to talk to people they didn't know, shopkeepers changed television channels to avoid Arabic language programs, and parents encouraged their children not to speak out against the government.

Part of EFF's core mission is to maintain the civil rights that we've always had in the offline world in an era when technologies like cell phones, computers, activity trackers, or smart home devices capture more personal details about us than ever before.

As far back as 2005, we've challenged law enforcement's warrantless access to location data—sometimes at the invitation of judges when there wasn't even a defendant yet—explaining cell phone technology to the courts and arguing the Fourth Amendment requires a warrant for location data. On the other side, the government has argued that we have no reasonable expectation of privacy in this data because it is collected by and shared with a "third party"—the phone company. As cases started going up to appellate courts, we kept losing one case after the next with the courts feeling hamstrung by earlier Supreme Court opinions. Despite these setbacks, we carried on because we believed the courts were wrong and that they were setting dangerous precedents, not just for cell phones, but for all the other data we share with companies as a byproduct of how many technologies now operate.

Finally Carpenter made it up to the Supreme Court. We filed an amicus brief urging the Court to take another look at how the Fourth Amendment should apply to the vast amount of data collected by third parties like cell phone companies and by other technologies we rely on every day.

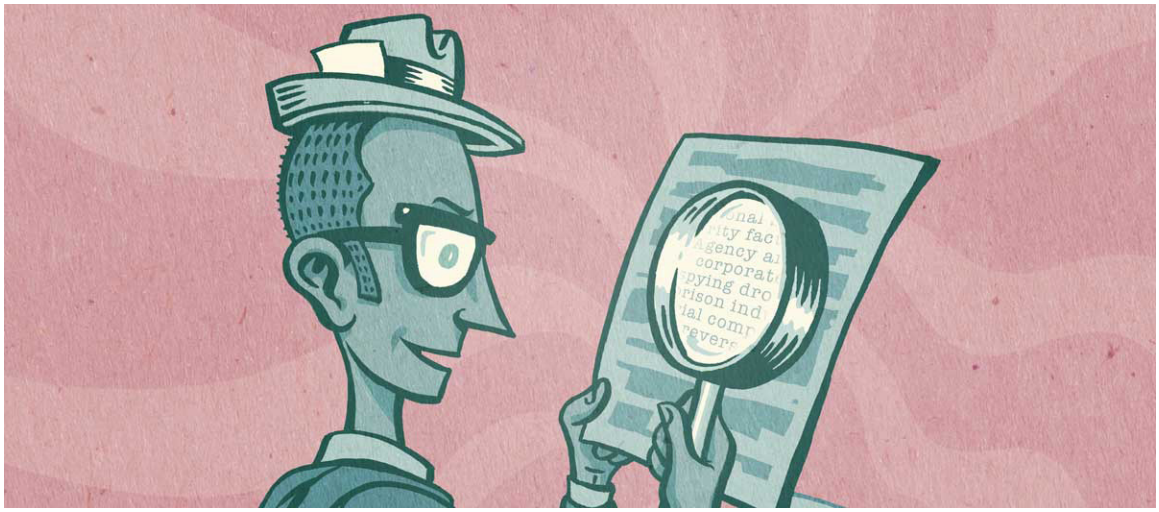
In its landmark 5-4 opinion, the Court agreed with our arguments, even citing our amicus brief. The Court held the Fourth Amendment protects data, even when shared with or collected by a third party. The Court recognized that location information creates a "detailed chronicle of a person's physical presence compiled every day, every moment over years." As a result, police must now get a warrant to access it.

Although the Supreme Court explicitly tried to limit Carpenter to historical cell phone location information, the language in the opinion is so sweeping that we think it would apply easily to other technologies.

We are now pushing the limits of Carpenter by urging courts to apply it to other data stored with third parties and to other instances when law enforcement collects location information without a warrant. One technology we're focusing on is automatic license plate readers (ALPRs)—cameras mounted on utility poles, police cars, and even vehicles operated by private contractors that scan all license plates that cross their paths and record the time, date, and location of the scan. Law enforcement and surveillance companies are building databases of billions of plate scans from ordinary people who've committed no crimes. We've now filed amicus briefs in several federal and state appellate court cases challenging warrantless access to this data. So far, the lower courts have ruled that law enforcement don't need any kind of legal process at all to access it.

Law enforcement likes to make the argument that when you're driving in public, you can't expect privacy over your license plate because anyone can see your car, and you should know you are being watched. But one thing I've found in my work is that most people don't agree at all with this argument. When people find out that police and private surveillance companies are tracking their location they find it surprising and often really creepy.

It is creepy. And it goes against the Constitution and the democratic principles on which the United States was founded. With your help, we'll keep fighting to protect your data and your location from the government's prying eyes.



THE STRANGER CASE

Shedding light upon law enforcement's data access and surveillance capabilities

Aaron Mackey
STAFF ATTORNEY

It has long been easy for U.S. law enforcement to find out who people communicate with, where they travel, and what they believe. Using technology like pen registers—electronic devices that record metadata like all numbers called from a particular phone line—and other tools, police can collect an abundance of data on anyone who uses the Internet or a mobile phone, including who they call and what websites they visit. Government's use of these powers has also long been secret.

Federal laws such as the Pen Register Act, Stored Communications Act, and Wiretap Act give law enforcement the authority to obtain this information. The vast majority of these cases are filed under seal and remain that way indefinitely. The secrecy surrounding these orders is further heightened by the varying docketing practices of federal courts across the country, which means there's often not even a public docket for such materials—making it impossible to know basic facts and when and how frequently government requests this data.

As a result of EFF's work on behalf of the Pulitzer Prize-winning newspaper The Stranger, the public will get access to basic facts about law enforcement's use of these powers in Seattle. In 2018, EFF represented the newspaper to file a petition with a

Washington state federal district court aimed at ending secrecy surrounding electronic surveillance orders. The petition asked the court to make public historically sealed electronic surveillance orders while also requesting that the court adopt procedures to ensure greater transparency moving forward. EFF was proud to represent The Stranger because the newspaper is committed to government transparency and has a distinct history of reporting on law enforcement surveillance capabilities.

This is problematic because without public scrutiny, law enforcement can aggregate power to itself and too often, judges fail to check that growing power.

The amount of information that law enforcement is able to obtain without a warrant right now is already invasive. In addition to just being able to obtain info that details private info about us, we know that law enforcement are increasingly pushing the boundaries of these authorities to try to use them in new ways. This is problematic because without public scrutiny, law enforcement can aggregate power to itself and too often, judges fail to check that growing power. And given the secrecy, neither the public nor Congress has enough information to actually protect individual privacy and limit law enforcement.

For example, the blockbuster Supreme Court case U.S. v. Carpenter, which ruled that police must get a warrant before obtaining historic cell-site location information, originated from a Stored Communications Act order issued in 2011. It took seven years for the case to wind its way through the courts. And it was only because a criminal defendant who was actually charged with a crime challenged the order that we are able to enjoy these new protections.
The secrecy also limits courts and lawmakers from meaningfully developing the law to protect individual privacy. So many of these surveillance orders are issued and the target whose emails or communications metadata are collected doesn't learn of that invasion because they are never prosecuted or are not the target of the criminal investigation.

After EFF filed the petition for The Stranger, the federal court in Seattle agreed to track and docket warrantless surveillance orders and requests, and then publicly disclose them twice a year. The agreement requires that, beginning in 2020, the court will publicly post a list of the cases involving these requests and orders that will include basic information about them, such as when they were sought and what crimes police were investigating.

Providing greater transparency will help everyone learn sooner how law enforcement is using its surveillance powers, which will hopefully allow people to more proactively challenge those powers, either in court or by passing new laws.

FREE EXPRESSION

SANTA CLARA PRINCIPLES

Keeping companies transparent and accountable for online censorship

Jillian York

DIRECTOR FOR INTERNATIONAL FREDOM OF EXPRESSION

As a lifelong digital rights advocate, I have seen careless moderation of online content lead directly to broad censorship. Though originally intended to protect users from offensive or illegal content, companies have increasingly added complexity to their public-facing rules, internal guidelines, and content moderation practices, silencing many forms of expression.

Inconsistent and overbroad content moderation has a negative impact on all kinds of individuals and groups, from political protestors in Egypt or Poland to businesses both small and large. I've seen overly complex policies and moderation errors harm LGBTQ+ organizations, bra companies, Catalan independence activists, poets, religious figures, and many others.

While many of these policies are unfairly restrictive, EFF believes in a company's right (guaranteed by CDA 230) to moderate their own platform. But we also believe that they should be transparent and communicative about what they remove, and accountable to their users when they make wrong decisions by offering a means for them to appeal. No one is immune from overbroad content moderation, which is why one remedy is to ensure that all users are treated fairly and offered consistent tools for recourse.

For many years, EFF has been a leader in advocating for transparency and accountability. Through our Who Has Your Back project, we've pushed for companies to produce regular transparency reports and inform their users about the decisions they make—but with platform censorship on the rise, we knew we needed to do more. In February of 2018, we convened digital rights and free speech-focused groups and academics alongside a conference in Santa Clara, California to determine what needed to be done.

No one is immune from overbroad content moderation, which is why one remedy is to ensure that all users are treated fairly and offered consistent tools for recourse.

From that meeting emerged the Santa Clara Principles on Transparency and Accountability in Content Moderation, which serve as a starting point for companies. The principles outline a minimum set of standards for companies for reporting on transparency; providing notice to users on content takedowns and account deactivations; and supplying users with an appeals process when their content has been wrongly removed.

Last year, along with more than one hundred organizations from all over the world, we penned an open letter calling on Facebook CEO Mark Zuckerberg to incorporate the Santa Clara Principles into Facebook's practices. To our surprise, Facebook responded publicly. The company committed to providing users with an expanded appeals process, and shortly after receiving our letter, published their first report offering transparency around content moderation decisions. While their commitments fell short of our demands, the company further pledged to engaging more robustly with the global digital rights community.

The process of collaboration amongst so many disparate groups has also led to the creation of a loose global coalition of organizations concerned with the policies and practices of content moderation. The coalition holds regular learning calls and has planned meetups at upcoming events.

I'm looking forward to conducting more advocacy campaigns directed at tech companies whose policies fall short of the Santa Clara Principles, and even adapting or

expanding the principles as time goes on to keep up with new trends. By working together, I know we can ensure that more tech companies operate with transparency and accountability to respect their users.

PETA v. TEXAS A&M

Defending your right to question and criticize government entities

Camille Fischer
FRANK STANTON FELLOW

Social media can be a powerful tool for government to connect directly with citizens, but it can also be ripe for abuse. All too often, elected officials and government entities encourage constituents to engage with them on social media, but when that engagement leads to criticism, they react by shutting down their opponents. And when a public entity shuts someone out of a discussion forum because they don't like what the person has to say, it is illegal viewpoint discrimination.

I've always been interested in the tools that people use to speak up for themselves. In fact, it's why I went to law school. And after the Snowden disclosures broke during my second year, I chose courses that focused on civil remedies for government abuses. I loved law school, and upon graduation, I was the recipient of the presidential management fellowship, which is a pathway for post-graduate students to go directly into government jobs. I began my career working in the Department of Commerce, but soon moved into the National Economic Council in the Obama White House, working as the civil and consumer rights point-person for the administration's policies regarding police access to people's data.

At the time I thought that working for the government would be the best way to protect a person's rights. But seeing how the power balances within government frequent-

ly tip towards national security and secrecy interests frustrated me, and so when I saw the Frank Stanton Fellowship opportunity at EFF, I knew it was the next logical step. My work with EFF has allowed me to counter government abuses of power head on.

Texas A&M is the second largest public university in the country, and receives significant amounts of federal funding. The university is also home to a lab in which dogs are bred to develop muscular dystrophy and subject to experiments in the hopes of finding treatments or a cure for the degenerative disease.

PETA (People for the Ethical Treatment of Animals) has been among the lab's loudest critics, using various platforms—including Facebook—to spread their message. The university responded by setting keyword filters for its Facebook page that prevented comments with words including "PETA," "lab", and "cruel" from being posted to the page, and also manually deleted comments expressing views critical of the dog lab.

So, in this case, we have this critic of one of the largest public universities in the country, and the university is doing everything possible to shut them down. The kind of criticism that PETA was engaging in, especially because they are running a campaign centered on petitioning and protesting, was exactly what the First Amendment was written to protect.

The kind of criticism that PETA was engaging in, especially because they are running a campaign centered on petitioning and protesting, was exactly what the First Amendment was written to protect.

PETA submitted a Texas public records request to see what the Facebook settings were on Texas A&M's page to figure out why they were being blocked. When they got the results, we got proof that Texas A&M had used page admin tools to use automated keyword filters to specifically target PETA. And in the litigation, Texas A&M admitted to manually and automatically filtering or taking down PETA's speech from their Facebook page.

The university filed a motion to dismiss, arguing that their Facebook page wasn't a public forum. But we successfully challenged the motion. After a few months of unproductive discovery discussions, EFF filed a motion for summary judgement this March. The motion is currently stayed while the parties try to settle the case.

This case is core to free speech and isn't the only one of its kind: Three federal courts of appeals have already ruled that when government officials delete comments or block people on social media they are engaging in illegal viewpoint discrimination. The case against President Trump in particular—Knight First Amendment Institute v. Trump—should serve as a warning sign to elected representatives across the country that when they want to operate a social media page to engage with the public and get all of the benefits of this new type of direct engagement, they must abide by the Constitution and allow all people to share their voices and opinions, regardless of viewpoint.

SECURITY

SECURING EMAIL COMMUNICATIONS

Leveraging our web encryption success to make secure email a real-

Sydney Li
STAFF TECHNOLOGIST

The journey to a more secure email ecosystem has had a lot of twists and turns, making it both challenging and exciting. We moved closer to our goal of securing email delivery in 2018 with a renewed focus on STARTTLS Everywhere, EFF's initiative to make secure email a reality.

This work wouldn't be possible without the great strides we've made in encrypting the entire web. Let's Encrypt continues to hit milestone after milestone. As of today, according to Mozilla, over 75% of web pages worldwide are loading over HTTPS. It's time we use this momentum to secure the rest of the Internet.

STARTTLS Everywhere is the continuation of work that began in 2014 to push for identity authentication in server-to-server email delivery, as well as web browsing. To accomplish that, we worked to create a list of email servers and their security information so that other servers can be sure the messages they're getting are coming from a trusted source and haven't been hijacked or tapped by an on-path attacker.

Email relies on something called the Simple Mail Transfer Protocol, or SMTP, which is technical language email servers use to communicate with each other. It was developed decades ago, without encryption or authentication in mind, as the trust model on the Internet today is starkly different from what it was in the 70s. So the machines that deliver emails can read their contents, as can anyone watching the traffic the ma-

chines send and read. It's like your post office or postal carrier can read the what you write on a postcard—the text is not inside an envelope or written in code.

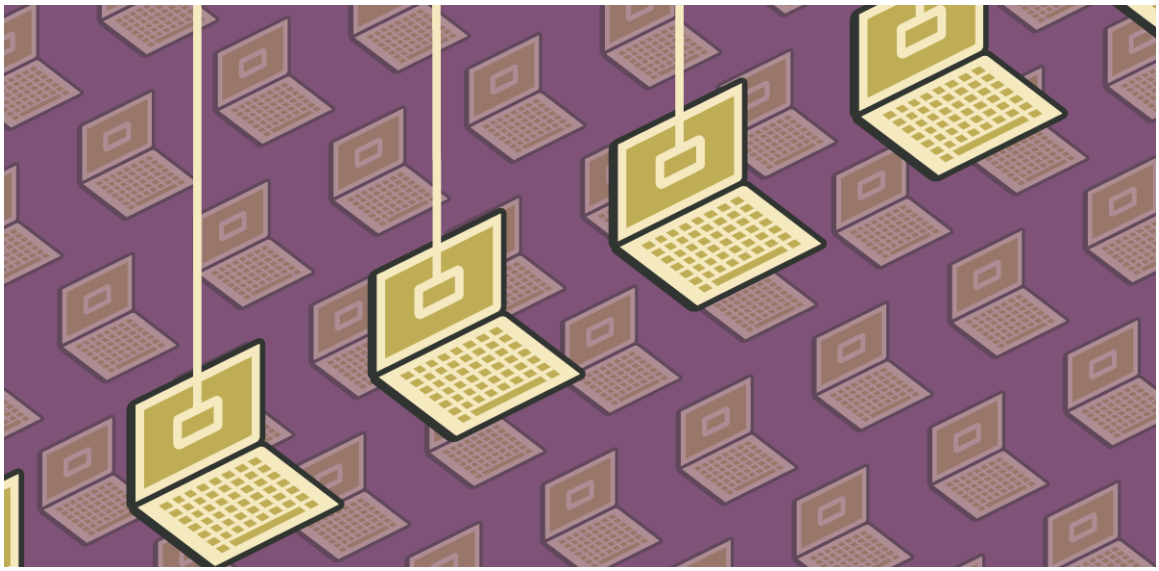
That means that without encryption, just like the web, government agencies that perform mass surveillance, like the NSA, can easily sweep up and read everyone's emails—no hacking or breaking encryption necessary. STARTTLS is an addition to SMTP, which allows one email server to say to the other, "I want to deliver this email to you over an encrypted communications channel." The recipient email server can then say "Sure! Let's negotiate an encrypted communications channel."

That means that without encryption, just like the web, government agencies that perform mass surveillance, like the NSA, can easily sweep up and read everyone's emails—no hacking or breaking encryption necessary.

In 2018, I took on STARTTLS Everywhere to scale the list we created in 2014 and re-launch the project. We developed tooling and software to help smaller mail server operators integrate it into their email server software, and provided a web interface for opting into the list and double-checking your email domain's security configuration. If the configuration is secure, email server admins can preload their domain to our index of high-security email domains so servers have another point of reference to discover that you support STARTTLS.

STARTTLS Everywhere is one prong of our two-step plan of attack to secure email messaging. We are first encouraging larger e-mail companies to adopt MTA Strict Transport Security (MTA-STS), a more scalable standard that was developed under the auspices of the Internet Engineering Task Force (IETF), and finalized in late 2018. It's not perfect, and can be complex to implement, but STARTTLS Everywhere and MTA-STS can cover each other's weaknesses. We're currently working on updating the STARTTLS Everywhere project such that the two technologies can complement each other.

So the first prong is pushing companies to implement and adopt MTA-STS—Gmail is the first large email provider to adopt it, which is huge step in the right direction—and then adopt our list. The combination of these two things will finally secure email. In 2019 the game is to advocate for MTA-STS adoption by large email providers, and encourage smaller email server operators to update their encryption practices.



GEORGIA BILL S.B. 315

Bennett Cyphers
STAFF TECHNOLOGIST

Security researchers play a crucial role in protecting digital information, including people's personal data held by third parties. Even the most secure computer systems can be hit by breaches, and unfortunately, important public infrastructure often runs software that is not properly configured or not up-to-date. The best way to prevent people from abusing software vulnerabilities to steal data is to find and patch those vulnerabilities first. That's why EFF is such a strong supporter of the individuals who find and expose security holes in critical systems like voting machines, medical devices, and government databases. These researchers—rather than those who operate the systems—are often the first to spot holes in the security net and notify maintainers about the problem.

Unfortunately, federal law can be used to punish the very researchers who help keep us safe. The Computer Fraud and Abuse Act (CFAA) is a vague and overbroad anti-hacking statute used to hamper security research and prosecute people who have caused little or no economic harm. Worse, some states have taken the CFAA as a template and tried to pass their own overbroad anti-hacking laws. These laws threaten to treat researchers like criminals for alleged "unauthorized" access to computer systems, like landing on a URL that's not publicly listed.

Last year, the Georgia legislature introduced just such a bill, called S.B. 315. The bill was introduced after a security researcher uncovered a dangerous and embarrassing glitch that exposed a huge trove of voter and election data on the web. S.B. 315 adopted the worst parts of the CFAA, criminalizing "unauthorized access" without giving adequate exceptions for legitimate security research. Then it went even further, authorizing "hack back" measures for businesses which could have allowed them to target innocent users with malware if they were suspected of violating any parts of the proposed law. During my time studying computer science in college, I saw friends threatened with legal action for benign tinkering, and I saw EFF stand up for them. So when, two months after I joined EFF, S.B. 315 reared its ugly head, I jumped at the chance to tackle the issue head-on.

S.B. 315 was brought to EFF's attention by digital rights group Electronic Frontiers Georgia (EFGA), and we joined forces with them to fight it. The dogged work of EFGA drew national attention to the industry-wide implications of the measure. With EFF's support, EFGA members mobilized at every stage of the legislative process to defeat the bill. Meanwhile, EFF set up an action page for readers to send emails to Georgia lawmakers urging them to vote against the bill.

Despite our efforts, a modified—but still awful—S.B. 315 was approved by Georgia lawmakers in March 2018 and sent to the governor's desk. We had one more chance to stop the bill: we needed to convince the governor to veto it. EFF put together a letter outlining, once again, the potential ramifications of the bill, signed by 55 top cybersecurity researchers and professionals from around the country. The bill created new liability for independent researchers, and opened the door for companies to spy on them, the letter said.

EFF put together a letter outlining, once again, the potential ramifications of the bill, signed by 55 top cybersecurity researchers and professionals from around the country.

On the same day the letter from the experts was published, both Microsoft and Google announced their opposition to the bill as well. The unified opposition from advocates, researchers, and industry made state news, and it finally caught the governor's attention.

On May 8, 2018, Gov. Nathan Deal vetoed S.B. 315. It was a major victory for Electronic Frontiers Georgia, EFF, security researchers, and the people of Georgia. The odds were against us, given that the bill passed with a huge majority, but the effort payed off.

That's not to say the battle is over. Because a majority of lawmakers voted for the bill, we're aware that it could come around again. EFF and our supporters around the country are ready to fight bills like these wherever they arise.

FINANCIALS

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

EFF MEMBERS MAKE A BETTER DIGITAL FUTURE POSSIBLE

Aaron Jue

DEVELOPMENT DIRECTOR

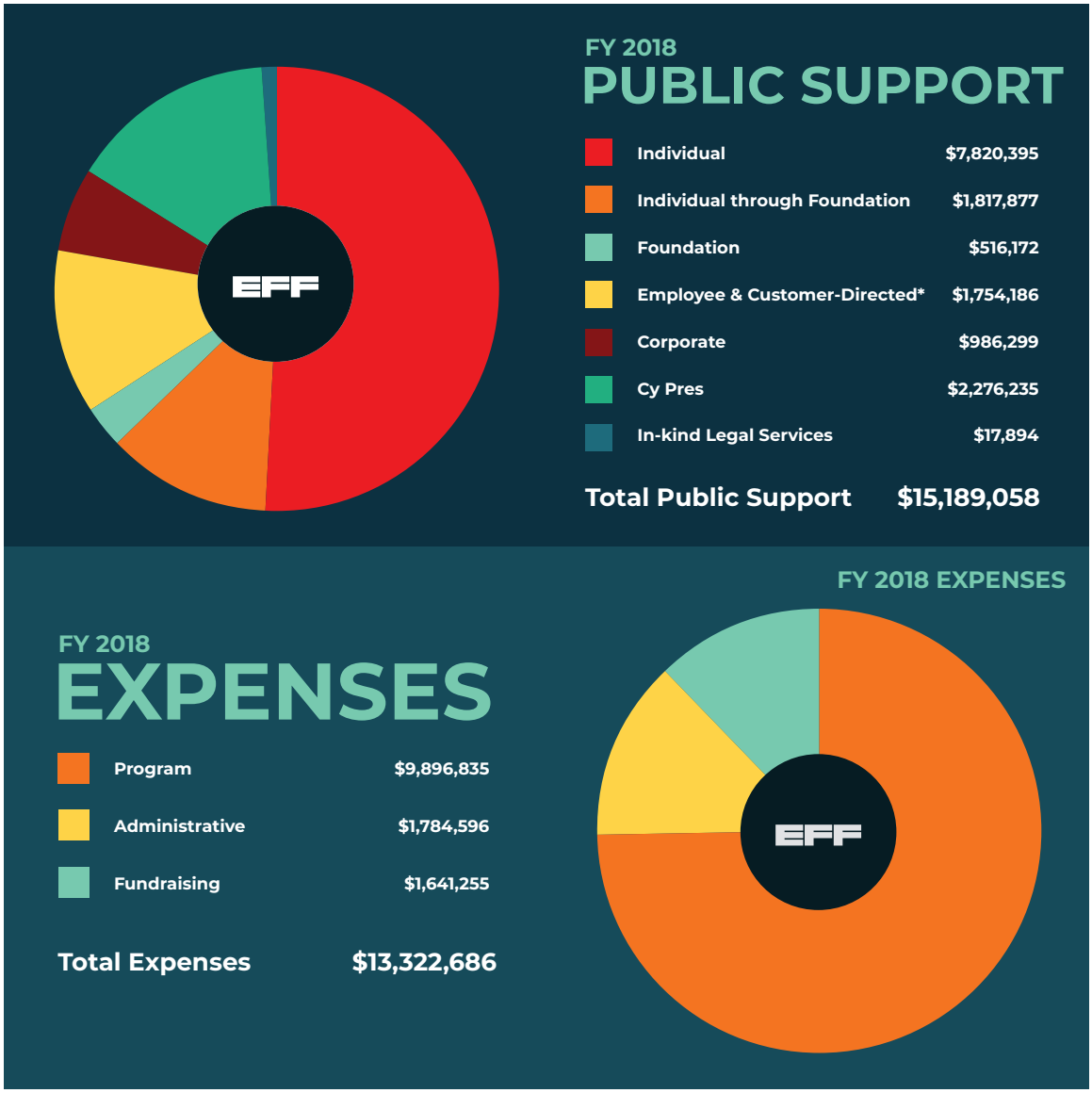
Over 30,000 EFF donors around the world power the movement for Internet freedom. Our activism, technology development, policy analysis, and impact litigation is only possible with broad support from the public. We are proud that the majority of EFF's funding comes from ordinary individuals, and over 80% of that funding consists of donations under $10,000. Direct contributions from businesses of any size comprised just 6% of our total public support.

EFF received a four-star rating (the highest possible) and a perfect score of 100 in accountability and transparency from watchdog Charity Navigator, a non-profit organization dedicated to providing an unbiased, objective, and numbers-based assessment of over 9,000 charities. EFF is also careful to keep administration and fundraising expenses low, with 74% of funds supporting programs.

I invite you to take a look at the following financial report for EFF's fiscal year from July 2017 to June 2018. Thank you for supporting digital civil liberties and for ensuring EFF's work will always remain fiercely independent.

Aaron Jue

EFF Development Director


FY 2018
PUBLIC SUPPORT
Individual $7,820,395
Individual through Foundation $1,817,877
Foundation $516,172
Employee & Customer-Directed* $1,754,186
Corporate $986,299
Cy Pres $2,276,235
In-kind Legal Services $17,894
Total Public Support $15,189,058
FY 2018
EXPENSES
Program $9,896,835
Administrative $1,784,596
Fundraising $1,641,255
Total Expenses $13,322,686
FY 2018 EXPENSES

INCOME

PUBLIC SUPPORT

Individual Contributions	
Individual Contributions over $50,000	$534,263
Individual Contributions $10,000 - $50,000	$786,060
Individual Contributions under $10,000	$6,500,075
Total Individual Contributions	$7,820,395
Individual Contributions through Foundations	
Individual Contributions through Foundations Over $50,000	$1,045,000
Individual Contributions through Foundations Under $50,000	$772,877
Total Individual Contributions through Foundations	$1,817,877
Foundation Grants	$516,172
Cy Pres Awards	
Couser v. Comenity Bank	$59,833
The Home Depot, Inc., Customer Data Security Breach Litigation	$971,169
Ossola v. American Express Co.	$7,321
Ashley Madison Customer Data Breach Litigation	$415,014
Khoday v. Symantec Corporation	$92,086
Gehrich c. Chase Bank	$402,727
Zepeda v. Paypal	$328,084
Total Cy Press Awards	$2,276,235
Corporate Contributions	
Employee and Customer-Directed Gifts*	$1,754,186
Other Corporate Contributions	$986,299
Total Corporate Contributions	$2,740,486
In-kind Legal Services	$17,894
TOTAL PUBLIC SUPPORT	**$15,189,058**

REVENUE

Net Investment Income	$1,844,408
Attorneys' Fees Awarded	$87,305
EFF Event Income, Net of expenses	-$24,164
Miscellaneous	$172,222
TOTAL REVENUE	**$2,079,772**

TOTAL SUPPORT AND REVENUE $17,268,830

EXPENSES

Salaries & Benefits	$10,671,197
Legal & Professional Fees	$691,319
Membership Expenses	$579,256
Amortization & Depreciation	$256,336
Travel Expenses	$220,993
Building Expenses	$211,995
Planning & Development	$182,434
Office Expenses	$123,9453
Corporate Insurance	$117,674
Litigation Expenses	$98,963
Furniture & Equipment Expense	$94,416
Awareness Events	$29,564
Other Administrative Expenses	$24,984
Intern Expenses	$17,561
Fundraising Expenses	$2,049
TOTAL EXPENSES	**$13,322,686**

NET INCOME $3,946,144

THANK YOU

For 29 years, members have joined EFF to defend freedom of expression, protect encryption, battle with patent trolls, stand up for the freedom to tinker, and so much more. Because of you, our values live in the law, in code, and in the way we defeat threats and champion progress. Whether in the courts, in the streets, or appearing before Congress, we're proud and humbled by our members' passion for freedom and for the future that ought to be. Thank you.

EFF Membership Form

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

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

MEMBERSHIP INFORMATION

Name: _____

Email: _____

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

Phone Number: _____

Street Address: _____

City/State/Province: _____

Postal Code/Country: _____

We respect your privacy!

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

MEMBERSHIP LEVEL

Silicon: ($25-64)
$ _____
- ☐ Stickers

Copper: ($65-99)
$ _____
- ☐ Stickers
- ☐ Shirt

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

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

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

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

SHIRT/HOODIE SIZE:

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

PAYMENT INFORMATION

Credit Card #: _____

Expiration Date: _____

Signature: _____

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

Please return membership form to:

ELECTRONIC FRONTIER FOUNDATION

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