2020 ANNUAL REPORT

ELECTRONIC FRONTIER FOUNDATION

TABLE OF CONTENTS

A WORD FROM OUR EXECUTIVE DIRECTOR

Dear friends,

2020 was a year that challenged us all, and EFF is no exception. The global pandemic forced EFF to instantly become a distributed organization even as we pivoted to ensure that your civil liberties, privacy, and right to innovate remained protected in this time of crisis.

EFF produced a tremendous amount of public and private work in response to the pandemic. We made sure that COVID-19 responses were closely tied to public health needs and didn't become an excuse to standardize massive data collection and surveillance. We pushed for more and better broadband access for all of us suddenly relying on the internet for social, family, work and school connections.

Then, just months later, the protests against police murders of Black people and the Black Lives Matter movement required us to renew and further develop our long-standing work protecting against overbearing public and private police surveillance. All the while, our core work continued without missing a beat. The truth is, 2020 required us to go above and beyond. And, thanks to the strong and unflagging support of members like you, we succeeded.

The truth is, 2020 required us to go above and beyond. And, thanks to the strong and unflagging support of members like you, we succeeded.

In this report you'll hear first-person accounts and reflections from a cross-section of our team. You'll hear from Ernesto Falcon how COVID reinforced our reliance on internet connectivity and underscored the need for universal fiber broadband to the home. You'll hear from Hayley Tsukayama, Adam Schwartz, and Alexis Hancock how,

as the pandemic hit, we put together a team of lawyers, technologists, and activists to ensure that our medical information remained secure and that we carefully evaluated and ensured privacy protections in much-hyped technologies like proximity tracking apps and "vaccine passports." At the same time, Jason Kelley tells how EFF led the fight against subjecting suddenly remote students to poorly designed and implemented disciplinary technologies.

But we didn't let up on longstanding EFF issues either. Katharine Trendacosta explains how we continued to stand up for your right to create free from copyright bot censorship. Daly Barnett shows how we supported the voices of our LGBTQ community, and continued to ensure an internet that serves everyone. Matthew Guariglia shares EFF's work exposing how Amazon's Ring built technologies to aid police mass surveillance of us on our public streets, and then used law enforcement to promote and sell those tools to homeowners. Saira Hussain explains how we demonstrated the dangers of these camera networks—and sued for accountability—after we caught the City of San Francisco illegally accessing a private camera network to spy on Black Lives Matter and Pride protesters.

None of this would have been possible without our community. EFF stands on the shoulders of our roughly 38,000 members and that support let us be flexible and fill the information void around COVID-related technology. I often say that EFF is "on patrol," meaning that our responsibility is not merely to plot out multi-year plans for change, but also to be ready to defend your rights when they are suddenly under attack and move toward a better internet whenever and wherever opportunity arises. 2020 put us to the test on all counts and I'm proud to say, we met it.

Sincerely,

Cindy Cohn, EFF Executive Director

LOCATION TRACKING AND EXPOSURE NOTIFICATION

Resisting Overbroad COVID Phone Tracking Apps

Adam Schwartz
SENIOR STAFF ATTORNEY

When COVID-19 struck in March 2020, I was really scared. We all knew people who got sick. Social distancing brought unprecedented isolation. In my home, this was especially hard for my teenage kids.

Proposals to "tech our way out of the crisis" arrived immediately. Many of us carry phones, which are constantly monitoring our movements and much more. Why not install a new health app to track where we've been and with whom? That way, if someone gets sick, we can quickly identify and test the people they've been near. This would parallel a traditional public health measure: contact tracing, which involves interviewing infected people to learn who they've been around. Why not automate this manual process? Proponents claimed this would help us avoid both illness and lockdown.

EFF quickly looked under the hood. We didn't like what we saw. And we blew the whistle.

We assembled a working group of our activists, lawyers, and technologists. We closely examined COVID phone tracking apps being implemented and proposed around the

world. The touchstone in our investigation was a hard lesson learned over many years: new surveillance technologies might sound good in the midst of a crisis, but they rarely accomplish their promised safety benefits, they often undermine our civil rights and civil liberties, and they are devilishly hard to dismantle when the crisis ends.

One proposal was to track our movements through our phones' GPS and cell-site location information (CSLI). This kind of location data is not sufficiently granular to show whether two people were close enough together to transmit the virus. The CDC recommended six feet of social distance, but CSLI is only accurate to a half mile, and GPS only to 16 feet. Yet CLSI and GPS are granular enough to invade our location privacy, and expose, for example, whether we've attended a union meeting or a BLM rally.

The touchstone in our investigation was a hard lesson learned over many years: new surveillance technologies might sound good in the midst of a crisis, but they rarely accomplish their promised safety benefits.

Another approach was to track our proximity to others by measuring a phone's Bluetooth signal strength. If two people install compatible proximity apps, and come close enough together to transmit the virus, then their phone apps can exchange digital tokens. Later, if one becomes ill, the other can be notified.

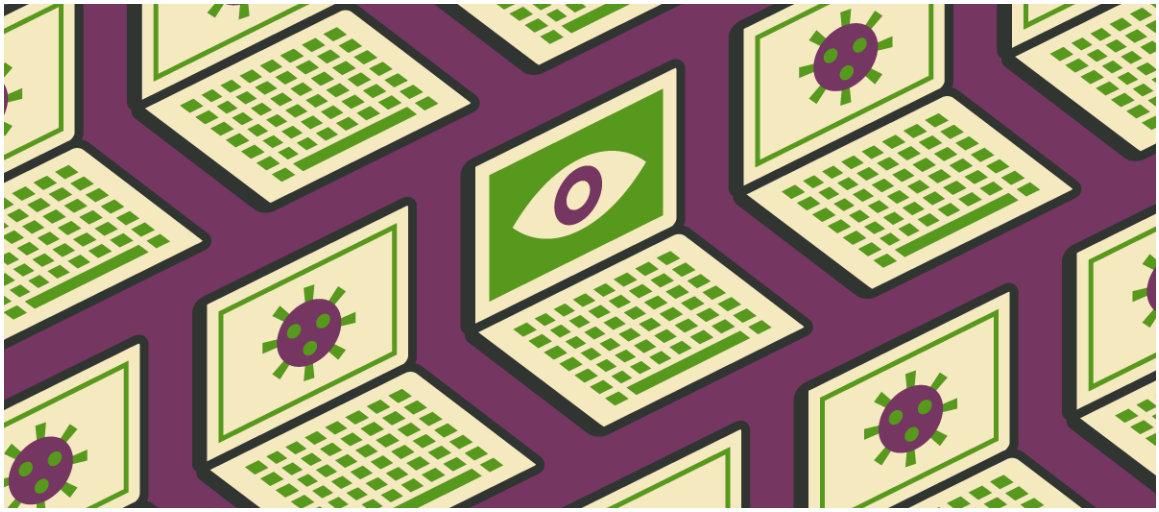
Proximity tracking might or might not help at the margins. It will be over-inclusive: two people standing a few feet apart might be separated by a wall. It also will be under-inclusive: many people don't have smartphones, especially among the groups most vulnerable to COVID, like low-income, unhoused, and elderly people. Moreover, many people simply won't use a proximity app. Perhaps most importantly, no app can fill the need for traditional public health measures, such as testing, manual contact tracing, support for patients in quarantine, social distancing, wearing a mask, and now vaccination.

Proximity apps must be engineered for privacy. Unfortunately, many are not. In a centralized model, the government has access to all the proximity data and can match it to particular people. This harms digital rights. Yet many nations have adopted it. A better approach is Google and Apple's Exposure Notification (GAEN). It col-

lects only ephemeral, random identifiers that are harder to correlate to particular individuals. Also, GAEN stores these identifiers in the users' phones. If a user tests positive, they can choose whether to upload the identifiers to a publicly accessible database. Public health authorities in many U.S. states and foreign nations sponsor GAEN-compliant apps. Of course, participation must be voluntary.

I'm proud that early in the pandemic, EFF helped steer the public conversations away from using our phones for location tracking and centralized proximity tracking. It is our job to quickly evaluate new technologies, and to educate policy makers, developers, and the public about unforeseen hazards.

My kids are excited to be coming out of lockdown. Thanks to EFF's work, they can do so without worrying about how to dismantle an invasive new surveillance system hardwired into the phones they carry everywhere they go.



DIGITAL IDENTITY AND "VACCINE BOUNCERS"

Scrutinizing the Risks of Digital Health Credentials

Alexis Hancock

DIRECTOR OF ENGINEERING, CERTBOT

As shelter-in-place took effect, pandemic response was something we all had to learn as we went. Some people stayed inside completely and others bought all of the toilet paper at Target. Among the initial panic came the development of technologies that promised to track the sick, log COVID-19 test results, and differentiate the sick from the healthy and the vaccinated from the unvaccinated.

As we all adjusted to working remotely at home, EFF's team delved into what exactly these proposals were about. Before governments even had a handle on vaccine distribution, various companies, groups, and organizations jumped to take on the task of creating digital COVID-19 credentials. The first proposals used the term "immunity passports." The problems were immediately apparent: "immunity" cannot be guaranteed by a digital token, and the "passport" designation conjured visions of a near future in which one's movement would be conditioned on unsubstantiated health standards.

This was not EFF's first time confronting national ID mechanisms and potential catalysts for them, and we were prepared to sound the alarm on the various risks that come with digital identities. Throughout the past year, our position has been strongly

against "vaccine bouncers" in particular. EFF and our community are all too familiar with the dangers of "temporary" surveillance measures with long-term consequences, especially in times of fear and panic. Taking society from the start of the pandemic to the end of it should not end up expanding our exposure to tracking and risk of data leaks. This is not the time to roll out experimental technology that could potentially further marginalize people; this is the time to create safeguards like data privacy legislation.

This is not the time to roll out experimental technology that could potentially further marginalize people; this is the time to create safeguards like data privacy legislation that can serve us in both healthy times and times of crisis.

We've had our work cut out for us. Companies like CLEAR, who already hold a presence in airports as a privatized TSA Pre-Check of sorts, developed the "Health Pass." The scope creep this "solution" introduced was less about public health measures, considering its timing, and more about clinching the spot as the premier platform for everyday exchange of digital identity to businesses. New York State rolled out the Excelsior Pass, built with IBM's digital health platform and a sparse privacy policy. Recently, California rolled out its Digital Health Record. Many "vaccine passports" are now evolving to present themselves as all-encompassing "health passes" and even digital driver's licenses. By sharing EFF's analysis of digital identity and its implications, I hope we've set guidelines for potential data privacy laws that can direct us in both healthy times and times of crisis.

Calls for digital pathways identity continue, in the U.S. and internationally. However, at the same time, digital inequity persists, companies operate with too little accountability, and too often digital "solutions looking for a problem" carry only a naive sense of consequences. Whether their intentions are good, malicious, or half-baked, what matters now isn't intent: it's impact. Since many of these products were rolled out during a time of crisis, their potential impact has bypassed the scrutiny it deserves. EFF has provided that needed scrutiny, and with your help we will stay vigilant as the conversation on digital health credentials continues.

SECURING COVID DATA

Building Data Privacy Rules on Shifting Ground

Hayley Tsukayama
LEGISLATIVE ACTIVIST

2020 brought a public health crisis unprecedented in our lifetimes. But, for EFF, the COVID-19 pandemic also presented a different challenge: a massive new push for data collection—and, with it, the spectre of serious privacy harms.

When facing the unknown, corporate appetite for data can be insatiable. Worse, a crisis encourages people to act first and deal with the consequences later. Still, it was easy to be swept up in the novelty of the problems posed by the pandemic. I myself sometimes questioned whether we should bend some rules. As the daughter of an infectious disease specialist father, advocating for privacy in a way that didn't confound public health aims was very important to me.

But, if you talk to public health experts about privacy, you may learn what I did. Public health and privacy initiatives are not at odds with each other. They in fact share an important common aim: to protect trust.

Many things were new about the COVID-19 crisis, but that challenge of building trust wasn't one of them. Public health officials often head into communities that are scared and worried about stigma. Strong public health programs are built around how

you build trust, how you maintain that trust, and how you honor it. Mess that up, and people won't want to tell you anything, which in turn slows our ability to predict, react to, and treat disease. Those conversations regrounded me and underscored how important it was to get COVID-related data collection right the first time. Asking for forgiveness later was not a good option.

If you talk to public health experts about privacy, you'll learn what I did: public health and privacy initiatives are not at odds with each other, and actually share the common aim of building trust.

There's no denying medical data in particular is ripe for abuse. Knowing someone was exposed to the virus that causes COVID can lead to discrimination against them. It could also lead to inferences, perhaps false ones, about what risks they take.

Furthermore, medical information is also not as well-protected as most people think. I started caring about privacy as an intern news reporter covering the health care debate in 2010. What I learned then was that HIPAA, the much-mentioned law that protects our health privacy, really only applies to information being held by certain kinds of entities such as insurance companies and hospitals. In other words, if you post the same information on a social networking site that you give to a hospital, only the latter information is protected by HIPAA. That's why it's vital to have explicit privacy rules for any entity that touches this information.

Throughout the pandemic we saw private companies, such as Google or smart thermometer firms, step in to collect or direct the stream of data. Without rules, they could use that information for advertising, preying on vulnerable people worried about their health. They could share it with others and put it on the opaque data marketplace, or turn it over to those who could weaponize it against vulnerable communities.

In some ways, advocating for strong privacy rules around COVID data brought me back to my roots. Covering HIPAA in 2010 led me to a career in technology journalism—and then a second career at EFF, once I felt the need to advocate for strong privacy rules rather than report on the harm that happens in a world without them.

Trying to build policy on shifting ground is hard. New questions pop up every day about how to handle COVID privacy in various areas of life. Answers are rarely black or white, and finding the right shade of gray remains very tricky. Finding solutions required recognizing our team's own limitations. We sought the expertise of other advocacy groups and experts on privacy, public health, and labor (to name a few) to lean on each other's expertise. And, yes, I had a lot of conversations with my dad.

The work is far from done. But I'm hopeful. For one, we know more now than we did a year ago about this specific disease. EFF has found allies to work with on this and other problems in the future. And we've also helped educate policymakers about the risks that come up from thoughtless data collection and sharing. All of these should ensure we're more prepared for the next challenge—whatever that may be.

COVID-19 AND THE DIGITAL DIVIDE

Connecting Everyone to Fiber

Ernesto Omar Falcon
SENIOR LEGISLATIVE COUNSEL

I'm old enough to remember the world before the internet. When I got dial-up for the first time, I did not think much of how it took minutes to download a single picture (or that my parents were paying per minute). I was just a kid blown away by technological magic. Upgrading from a 28k modem to 56k (that's 56 kilobits) felt like getting on the fast lane. That 3-minute download turned into a blazing 90 seconds! I fondly remember my highs chool economics teacher remarking that someday soon that 56K modem was going to be replaced by a 1000K modem—that's 1 *million* bits. I couldn't believe it, but he was completely right.

As I continued to experience the pace of innovation in internet connectivity and speed, absent from my knowledge was the titanic struggle within Congress to lay the foundation of the commercial internet, or how the preceding Department of Justice efforts to break up the largest corporation in the world (AT&T) made it possible. Little did I know that the technological innovations I experienced had a long history that was rooted in decisions made by industry and government.

That history—and the digital divide it has created in the U.S.—was laid bare this year when workplaces, schools, and other community sites adopted social distancing in

response to COVID-19. As people depend on the internet in new ways for remote schooling, working from home, community connections, and public safety information, the pandemic has revealed two starkly different Americas: households who reap the benefits of competition among ISPs, and households who are forced to rely on obsolete infrastructure—or worse yet, who have no broadband options at all. The fact that we are still contending with such a stark "digital divide" in 2021 is a clear sign of failure in our current approach to broadband.

After a grueling pandemic year in which remote access became the norm, policymakers are finally catching on to how our progress on internet access is stuck in reverse.

Our current internet ecosystem is failing many Americans. And any infrastructure recovery effort that comes out of this crisis should address the digital divide at its source: policy decisions that have left us at the mercy of a few giant companies whose business concerns don't include all Americans.

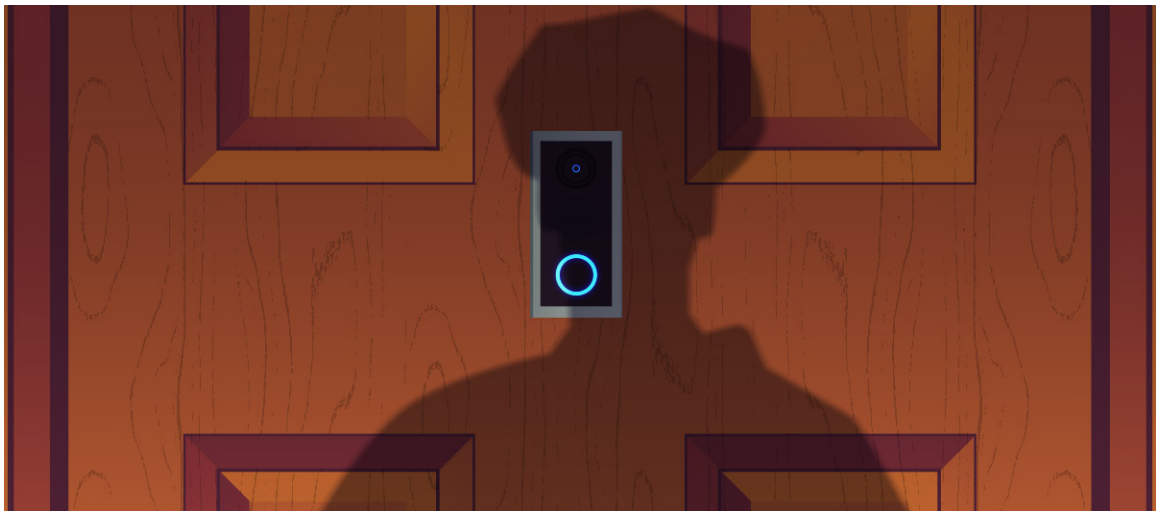
None of this is new. More than 15 years ago, before coming to EFF, I was in Washington, D.C. working for Congress in 2004 working on internet policy. Still a newbie, I did not appreciate the gravity of the following year's events, when Verizon began deploying 21st-century fiber optics and the FCC decided to not regulate fiber networks the same way it had early competitive DSL broadband. As a congressional staffer I began digging into how to get everyone fiber, naively assuming it would be an easy win. But unlike so many previous leaps in access technology, still less than half of America has fiber.

What is tragic about this digital divide is that there are no good reasons for it to exist, let alone continue. If the major ISPs universally converted their older networks over to fiber to the home, they would be net profitable in the long run in many places. Contrary to assertions that smartphones and wireless plans alone are sufficient, nothing can truly substitute for a high-capacity connection in the home. As we all experienced this past year, the more and more we do online, the less and less our phones and outside-the-home options will be compelling replacements.

The market has failed to deliver fiber because the government has allowed telecom monopolies to return. With no competition, large ISPs have opted to leave countless millions connected to yesterday's internet to raise profits while lobbying state legislatures to ban local community alternatives. But this year, things might change. After a

grueling pandemic year in which remote access became the norm, policymakers are finally catching on to how our internet access is stuck in reverse. States like Washington and Arkansas are repealing the laws cable monopolies pushed, while California recently approved the largest investment in public fiber infrastructure in history—following years of state activism led by EFF.

Without hesitation, I believe fiber is the future for the internet. But it will take strong commitments by local, state, and federal government actors to local options and fiber infrastructure funding to end the digital divide in the U.S. Each day we are getting closer and closer to that goal.



AMAZON RING

Working Together to Confront Public-Private Surveillance and Digital Over-Policing

Matthew Guariglia
POLICY ANALYST

In June of 2019, during my first week working at EFF, I was asked an important question: what is the biggest technological threat to privacy that not enough people seem to be talking about yet? At the time, the answer seemed obvious. That summer I had looked around and noticed that my walk to the grocery store had been captured on no less than a dozen cameras, mounted next to people's doors, pointed out to film the sidewalk. This was how I became concerned about Amazon Ring and other internet-connected security devices.

There is nothing wrong, per se, about a person wanting to keep an eye on their front door. People have been using security cameras for as long as we've been able to record footage. But, whereas a previous generation of security cameras backed up to a VCR in the garage, these cameras swept all of your footage onto a server somewhere far away—where it would be accessible to employees and police with a warrant without your knowledge. (And sure enough, four Ring employees have been fired for inappropriate access to users' footage.) But, what made me particularly concerned about Ring wasn't just its ubiquity, or its security concerns, but Ring's willingness to build and provide special tools designed to make their whole system legible and useful to police.

Consumer goods are just that—goods for consumers. But Ring represents a larger

trend in the private surveillance marketplace. Companies build free products to make sure their growing network benefits law enforcement by making it easy to request footage, speak to users, etc. What do Ring and companies like it get in exchange? A new marketing team that carries around the added legitimacy of a badge and a gun.

These types of cameras, which send an alert to a user every time there is motion in front of their house, are also more likely to forge a climate of fear, rather than security. There are a million reasons why a person might be pausing momentarily outside a house—ranging from delivering a package to tying a shoe to admiring the architecture—but every person seen through a security camera is going to be seen through the lens of suspicion. This creates a recipe for racial gatekeeping: people now have a digital tool designed to help them decide who does and does not belong in a neighborhood or near a house, based on how they look.

In addition to raising the alarm with consumers, EFF has been providing support to investigative reporters writing about Ring. We mapped Ring-police partnerships on our Atlas of Surveillance, and conducted our own public records investigations. In the last year EFF has helped to uncover that the LAPD had requested footage from Ring users of Black Lives Matter protests, and that throughout 2016 LAPD officers received dozens of free cameras in exchange for support spreading the adoption of Ring cameras. EFF's technologists even uncovered that Ring's app was filled with undisclosed third-party trackers that sent information off to other companies, including Facebook.

What made me particularly concerned about Ring wasn't just its ubiquity, or its security concerns, but Ring's willingness to build and provide special tools designed to make their whole system legible and useful to police.

Our activism—which we did alongside a coalition of racial justice, immigration rights, and civil liberties groups—didn't go unnoticed. Senators have written letters to Ring voicing their concern and asking questions about how their surveillance impacts people's lives. The LAPD has launched an investigation into the financial relationship between Ring and officers. Even Ring itself has made several reforms. In the last year Ring has implemented two-factor authentication, created an end-to-end encryption program to keep footage shielded even as it sits on Amazon's servers, and recently

changed how police are able to request footage from users.

And yet, the fight continues. Ring cameras continue to blanket entire neighborhoods around the country—and as long as Ring continues to build tools for police to capitalize on home safety devices, these connected doorbells will continue to cause real-world problems for vulnerable people who already suffer the lion's share of surveillance, criminalization, and over-policing.

WILLIAMS V. SAN FRANCISCO

Fighting Against the Surveillance of Protestors

Saira Hussain
STAFF ATTORNEY

I joined EFF over two years ago with the goal of bringing my expertise in racial and immigrant justice to the fight against government surveillance. And these issues came to the forefront during the summer of 2020, when the largest protest movement in U.S. history was sparked by the murder of George Floyd.

EFF quickly ramped up our efforts to stand for Black lives, online and in the streets. We provided technical resources, including Surveillance Self-Defense guides on attending protests, and in particular cell phone surveillance at protests. We worked with the National Lawyers Guild to develop a guide to observing visible and invisible surveillance at protests for their Legal Observer program. We published advice about the right to safely and legally record the police, based on amicus briefs we have filed over the years in support of this important First Amendment right. And we used open records laws to uncover how law enforcement was employing surveillance technologies to monitor protests.

In July 2020, we sent public records requests to several San Francisco Business Improvement Districts (BIDs)—quasi-government entities, some of which were outfitted with private networks of surveillance cameras that capture hundreds of blocks of city life. The Union Square BID, located in the heart of the city, revealed in their

response that they had given the San Francisco Police Department (SFPD) live access to their network of over 400 cameras for one week to surveil protests.

This live monitoring violated the city's Surveillance Technology Ordinance, which was enacted in 2019 by a nearly-unanimous vote of the San Francisco Board of Supervisors. The ordinance bars city agencies like the SFPD from acquiring or using surveillance technology without first seeking permission from the Board of Supervisors following a public process that allows opportunity for community voices to be heard.

In our client's words, "We have the right to organize, speak out, and march without fear of police surveillance."

EFF is part of the legal team representing three activists of color—Hope Williams, Nathan Sheard, and Nestor Reyes—against San Francisco for the police department's violation of the Surveillance Technology Ordinance. The lawsuit seeks a court order requiring San Francisco to enforce the ordinance and bring the SFPD back under law.

I fight for protestors like Hope, Nathan, and Nestor because movements for justice have long been the target of relentless government monitoring, made only more invasive by the advancement of surveillance technologies. We must protect the rights of protestors to speak freely. In Hope's words, "We have the right to organize, speak out, and march without fear of police surveillance."

A THEORY OF DISCIPLINARY TECH

Pushing Back Against Normalized Surveillance

Gennie Gebhart
ACTIVISM DIRECTOR

Over the past year, EFF has sharpened our focus on an expanding category of consumer and enterprise software, apps, and devices that are normalizing surveillance in everyday life. We call them "disciplinary technologies," and they typically show up where surveillance is most accepted and where power imbalances are the norm. We have "bossware" in our workplaces; remote proctoring, social media monitoring, and device surveillance in our schools; and stalkerware, "kidware," and home monitoring systems in our homes and neighborhoods.

I've been chewing on the relationships between these various types of tech since I first came to EFF five years ago, fresh out of a Master's in Library and Information Science. The thing that has stuck with me the most over the years is a course on feminist privacy theories. It formally introduced me to the evolving idea that the most "private" domains of life—like the home and the family—are also the places where violence against women is most shielded from outside scrutiny or intervention. Our task as students was to understand where vulnerable and marginalized people had the "wrong kinds of privacy at the wrong times," and envision privacy values that did not go out of their way to provide cover for the powerful. As I slogged through demanding data science homework and problem sets, ethics classes like this reminded me why I was in school in the first

place: to learn how technology exacerbates power imbalances, and to be part of the movement to tip the scales back.

And that's exactly what EFF is doing with our new public education campaign around disciplinary technology. It's the great trick of the surveillance economy to convince us to not only accept pervasive surveillance, but also proactively fill our own workplaces, schools, and homes with it. The challenge is that our typical advocacy rallying cries around user choice, transparency, and strict privacy and security standards are not complete remedies when the surveillance is the point. Fixing the spread of disciplinary technology requires stronger medicine. We need to combat the growing belief, funded by disciplinary technology's makers, that spying on your colleagues, students, friends, family, and neighbors through subterfuge, coercion, and force is acceptable behavior for any person or organization.

Our typical rallying cries around user choice, transparency, and strict privacy and security standards are not complete remedies when the surveillance is the point. Fixing the spread of disciplinary technology requires stronger medicine.

Disciplinary technology as a group flourishes because it's so hard to define and, for some, so easy to justify. But there's no reason to believe that disciplinary technology is actually capable of achieving its advertised aims. Bossware does not conclusively improve business outcomes, and there is no independent evidence that school surveillance is an effective safety or anti-cheating measure. And it's clear that digitally stalking one's partner or children is the opposite of a healthy relationship. If the goal is to use surveillance to give authority figures even more power, then disciplinary technology could be said to "work"—but at great expense to its targets, and to society as a whole.

My greatest fear is that the next generation will grow up under constant monitoring at home and at school, and then won't even blink when they are subject to the same monitoring as adults in workplaces and relationships. My colleague Eva calls this hideous technological lifecycle "cradle-to-grave surveillance." But what keeps me hopeful are the calls and emails we get every day at EFF from parents, from kids, from workers, from homeowners. They feel that something is not right about the technology they find creeping into various areas of their lives, and they're ready to fight.

Targeting just one disciplinary technology at a time will not work. Each use case is another head of the same Hydra that reflects the same impulses and surveillance trends. If we narrowly fight stalkerware apps but leave kidware and bossware in place, for example, the fundamental technology will still be available to those who wish to abuse it with impunity.

That's why we're working to address this group of technology as a whole: demanding anti-virus companies and app stores recognize spyware more explicitly, pushing companies to design for abuse cases, and educating people and institutions who might otherwise be tempted by empty promises from surveillance vendors. We have our work cut out for us, but we also have a growing community of supporters with us every step of the way. And that's why I show up to work every day: to get a little bit closer to tipping those scales.

STUDENT PRIVACY

Protecting Students From Turbo-Charged Surveillance At School and At Home

Jason Kelley
ASSOCIATE DIRECTOR OF DIGITAL STRATEGY

In June, Supreme Court Justice Breyer wrote that "America's public schools are the nurseries of democracy." We agree, which is one reason why EFF filed an amicus brief in that case. The Court correctly ruled in favor of a student who was suspended for her off-campus Snapchat posts criticizing the school. But for many, school feels more and more like a closet than a nursery: a place where self-censorship is required, mistrust is the norm, and speaking your mind is dangerous. And much of this student privacy crisis—which often affects students who stand out due to their race, sexuality, disability, or simply their curiosity—has been exacerbated by technology.

It wasn't always this way. Many of my own teen years were spent logged on at my high school through the first high-speed connection I'd ever accessed. Nearly anything I wanted to know I could search for, or ask in a chat room, and someone could explain it to me or point me in the right direction. The school's high-speed connection became my new library, and the books were nearly unlimited. I even got my first summer job, setting up systems for the school district, thanks to my interest in all things digital.

I never once thought that what I was doing when I sat down behind the keyboard would be recorded or surveilled by others. Had that been the case, my life would be immeasurably different—much smaller, much less curious, and much less interesting. I'd have asked fewer questions, worried more about what I was looking up, and been much more cautious with what I said, to my detriment.

In 2021—twenty-five years later—the internet offers so many more incredible ways to learn, communicate, and express yourself. But as the opportunities to go online have expanded, so have the abilities of schools to use technology to monitor and discipline, students.

There is still much work to be done to push back against these disciplinary technologies and protect student privacy, but it became clear this year that it's a battle we can win.

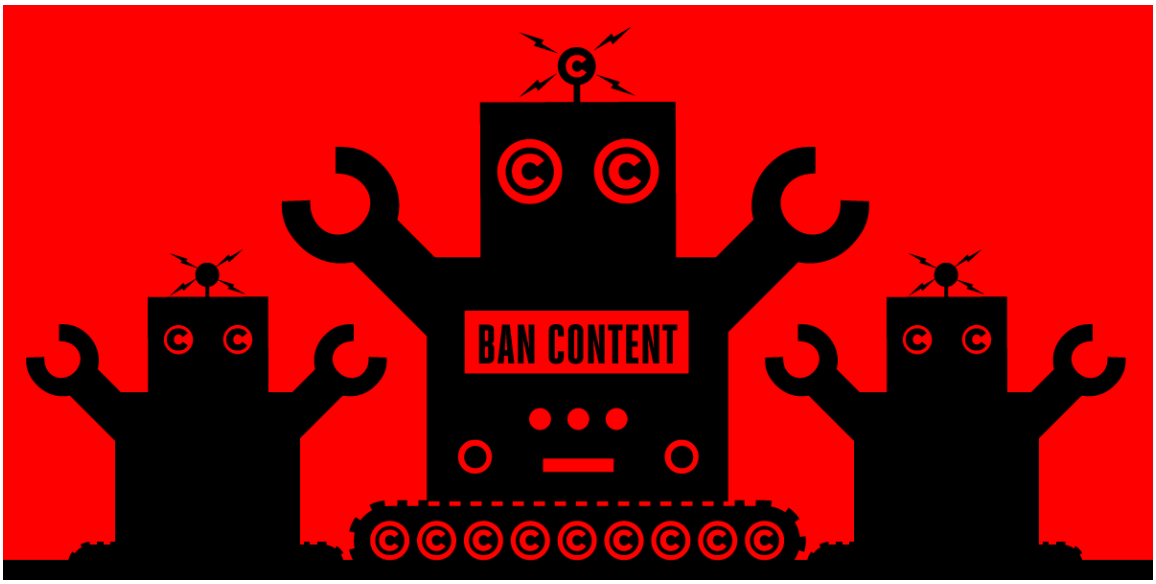
Schools now track students' online activity, and even social media posts when they are off school grounds. Schools block plenty of websites, too, often incorrectly: for example, clunkily filtering content based on LGBTQ-related keywords. This is all bad enough—but during the pandemic, it got much, much worse. Unable to directly monitor students while they took classes remotely, school surveillance began entering the homes of children of all ages through online proctoring tools. These tools aren't just privacy-invasive—they're also biased and dangerously flawed. They purport to detect cheating, but in reality, they merely flag "non-standard" behavior during tests, like looking offscreen, through faulty artificial intelligence. Thousands of students have been inaccurately flagged as cheaters just for acting outside the norm, and some students are flagged more than others—those who are neuroatypical or have disabilities, for example.

In one particularly egregious case, seventeen students at Dartmouth Geisel School of Medicine were charged inaccurately with cheating after the administration misread software logs during remote exams. These false charges put the students' entire medical careers at risk. When the school instituted a social media policy that chilled students from talking about the allegations online, EFF fired on all cylinders to start a media firestorm. With the help of EFF's legal team, technologists, and activists, the students were able to convince the administration to drop all of the charges, and the Dean eventually apologized to those that he had put through the painful investigation.

School should be a place where inquiry is encouraged, not encroached on; where self-expression is a basic right, not a blasphemy; and where experimentation is rewarded instead of constrained. Student surveillance curtails all of these. But I believe wholeheartedly that we can turn back the tide, as we did at Dartmouth. Across the country, schools are at last reckoning with the dangers that biased surveillance technology presents to students. Thanks in part to student pushback, the University of California is just one of many schools that now recommend alternative approaches to online proctoring tools. And one of the major proctoring companies—ProctorU—has even decided to stop offering its dangerous, artificial intelligence-powered service unless flagged cases are also reviewed internally.

There is still much work to be done to push back against these disciplinary technologies and protect student privacy, but it became clear this year that it's a battle we can win.

Schools should be foundational in helping a young person understand what it means to be human. And privacy is a necessary human right—even for a teenager. I know that my teenage self would be thankful for the work I now do at EFF to protect, and expand, student privacy. And I'm beyond proud that because of this work, there are many more students able to use technology in ways that satisfy their curiosity, allow them to express themselves, and expand their rights, rather than diminishing them.



YOUTUBE CONTENT ID

Championing Independent Creators' Expression Online

Katharine Trendacosta

ASSOCIATE DIRECTOR OF POLICY AND ACTIVISM

I have often described my entire career as "creative-adjacent." When I was an entertainment journalist and media critic, I was writing about creative works. When I went to law school, it was because I was interested in helping creative people make and share their work. I was particularly interested in the new creative class I was seeing online: people who made new things while incorporating the copyrighted material of others. But it seemed to me that things I loved kept disappearing because of copyright, and I wanted to learn why and how to help them.

As an activist at EFF working on copyright, I still see that as my job. But while I had foreseen that much of the fight around copyright online would revolve around the Digital Millennium Copyright Act (or DMCA), I hadn't predicted how much of my time would be spent helping people deal with copyright filters.

Copyright filters, also called copyright bots, are automated systems that check uploaded content against a database of material submitted by rightsholders. After ascertaining that there is a match between some portion of the uploaded content and some portion of something in the database, the system can do any number of things. But

the worst is when it disables access to the upload, resulting in, for example, a YouTube video takedown. Despite the problems surrounding using filters to regulate online expression, major studios and record labels consistently call on tech companies and Congress to implement more of them.

I wanted to put together a resource that laid out the problems—micro and macro—of filters: how the technology worked, what was blocked and altered, and the stories of creators who keep getting burned by the demands of the big businesses who claim to represent them. I wanted to rebut what Congress had been hearing from the movie and recording industry associations—that they alone knew what was best for creators, and that what was best was more filtering.

Large corporate rightsholders may see copyright filters as protecting their property, but small independent creators experience them as restrictions on what they can see and say online.

In 2020, the Senate Subcommittee on Intellectual Property held a hearing almost every month on copyright, the internet, and new technology. More often than not, the only sides represented were those of the big tech companies or the major entertainment industry, leaving users and small, independent creators out of the discussion. EFF wanted to shift the conversation. The large corporate rightsholders may see filters as protecting their property, but users and other creators experience them as restrictions on what they can see and say online.

EFF shines when we champion users. We grow when internet communities—like that of YouTubers—see us as a trusted ally. It's easy to get in the weeds of something like copyright, but it's equally important that EFF, as an advocacy organization, tell compelling stories to counter those told by those with lots of money to throw at policymakers.

The goal was to publish a white paper on this problem before the Senate Subcommittee on Intellectual Property held its hearing on the extrajudicial measures platforms use, like filters. As with many things in 2020, that hearing was delayed multiple times. But sure enough, we rolled with all the schedule changes to publish "Unfiltered: How YouTube's Content ID Discourages Fair Use and Dictates What We See Online" the

week before the hearing. Whenever someone mentions a problem with Content ID, I see people I don't even know pointing them to this paper. I've personally drawn from it a fair bit in drafting our responses to various proposals. We delved deep, but still made sure it was a compelling read.

In December of 2020, Senator Tillis unveiled his Digital Copyright Act draft, which, if passed as it currently looks, mandates filtering in at least three separate provisions. We will fight that fight and we will win it, because we spent last year preparing as only EFF can do: building up a repository of evidence, reaching out to online communities, and working together to make users' stories heard.

PRIDE AND ONLINE EXPRESSION

Uplifting LGBTQ Voices Online

Daley Barnett
STAFF TECHNOLOGIST

There's a line in that corny movie "Hackers" from 1995 that basically states that technology creates a world where your work and ideas alone can stand for themselves. Unseen biases, discrimination, bigotry, and fill-in-the-blank-phobia won't be present; people, not machines, are the causes and carriers of that. As a technologist with an unconventional background, I'll admit that this idea of a working environment that's free from that garbage actually duped me at first. Computers can't be biased, right?

Of course, it's an obvious gotcha. But it bears repeating, again, and again, and again, and again: human biases, unseen or not, bigoted or not, are inextricable from the technologies we create. While there is a deeply complex conversation to be had about how computers themselves are actually neutral machines and it's the ongoing dialogue between biased people and the abstractions we create using computers that perpetuate bigotry in digital spaces, I trust you get the oversimplified point I'm making here.

In 2020, a small group of us EFFers got together and planned ways we could align

momentum from international LGBTQIA+ Pride Month and the work we're already doing. A few different areas of our work presented clear opportunities: coded bias in platform censorship, free speech, digital privacy and security specific to marginalized communities, and evaluating EFF's own internal procedures when it comes to a committed practice of diversity, equity, and inclusion. It was important to us to do all of this in a way that carefully avoided reeking of pinkwashing for PR clout. We kept the focus on LGBTQ voices, and using EFF's expertise and resources to clear the way for their vital speech and expression, both online and off.

It bears repeating, again, and again, and again, and again: human biases, unseen or not, bigoted or not, are inextricable from the technologies we create.

We've continued to uplift the work of sex worker rights and technology advocates fighting against sexist puritanical content moderation. We've brought in organization leaders representing Black trans women in America, LGBT communities in the Middle East, and community organizers working on the front lines fighting against LGBTQ+ targeted violence. We've written security and privacy guides for protesting and for online dating as a queer person. We hosted online events and conversations with prominent voices like Chelsea Manning. We created a dedicated issue tag for it all on the EFF site.

Not surprisingly, there have been some unfriendly responses. I think that's usually a sign we're doing something right. One example was near the end of our Pride Month livestream. During the Q&A portion, a question came up from the Twitch chat audience: "Why is it only focused on LGBTQ+++? Doesn't everyone's freedom matter?" Ian Coldwater, one of our guest panelists, mentioned a tenet from organizing meetings at George Floyd square in Minneapolis: don't assume everyone has the same idea of liberation. I've been thinking about that since, and it's a perfect way of affirming why EFF's work for LGBTQ+ issues matters, as well as referencing the nuance and change that is possible when we consider digital rights fights from an intersectional lens. It matters because we choose to value the perspectives of those that aren't in the majority.

I've been an activist longer than I've been a paid technologist, and if there's one thing that's deeply ingrained in me, it's that this kind of work demands stamina for repeating the same things over and over. Taking that to heart—and using it to in-

form the small part I can play in shaping the internet I want to see—is what drove me to working at EFF. And it's what keeps me here: taking a humanist approach to technology, calling out privileged ignorant biases that paint the internet as a neutral marketplace of ideas, balancing our realistic paranoia with a fiercely optimistic vision of what technology can do and what the internet can be. We are uplifting the voices of those that don't typically get to be heard, and doing it with Pride.

FINANCIALS

Contributions from over 38,000 members around the world form the backbone of the Electronic Frontier Foundation.

EFF MEMBERS MAKE A BETTER DIGITAL FUTURE POSSIBLE

ALBERTO VILLALUNA

HEAD OF RESOURCE DEVELOPMENT

Fiscal Year 2020 was a year like no other for EFF. It was a year of innovation and resilience as the pandemic brought the world to a halt and forced us to find a new way of thinking, learning, working, and living. But the challenges of 2020 didn't stop us. In fact, as our Executive Director Cindy Cohn notes in her letter introducing this annual report, EFF didn't skip a beat. EFF's activists, lawyers, policy experts, and technologists worked tirelessly to champion your civil liberties, to defend the internet and digital innovation, and to continue to stand up for the users.

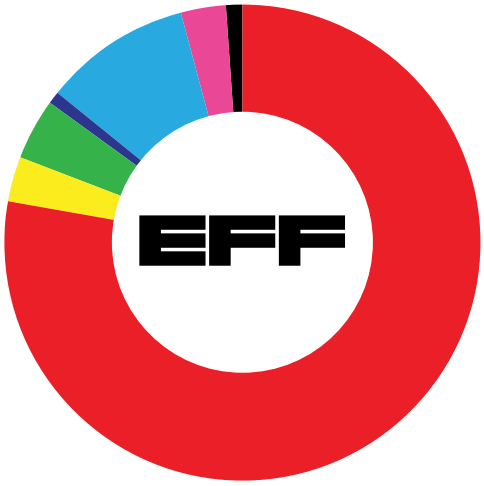
2020 didn't slow us down thanks to supporters and members like you – over 38,000 strong. And as you'll read in the financial report below, over 90% of our funding in the 2020 fiscal year from July 2019 to June 2020 came from individuals. Over half of those were donations below $1,000. You joined with us as members, as major donors, and through employee giving and customer-directed programs. The rest of our funding comes from philanthropic institutions and organizations that believe in EFF's values and mission to make the internet and the digital world better for everyone.

We take the responsibility of your financial support very seriously. We keep our administrative and fundraising costs as low as possible, allocating almost 72% of our funds towards our programmatic work. But don't take our word for it: Charity Navigator, the watchdog non-profit organization dedicated to providing unbiased, objective, data-based assessments of over 9,000 global organizations, gave EFF the highest possible rating of four stars in accountability and transparency. This was the eighth year in the row that we've received this top rating.

Thank you for your support, and for your belief in EFF's mission. We cannot do this without you. Together, we stand up for digital civil liberties even in the most difficult times. 2020 proved it.

Sincerely,

Alberto Villaluna, EFF Head of Resource Development



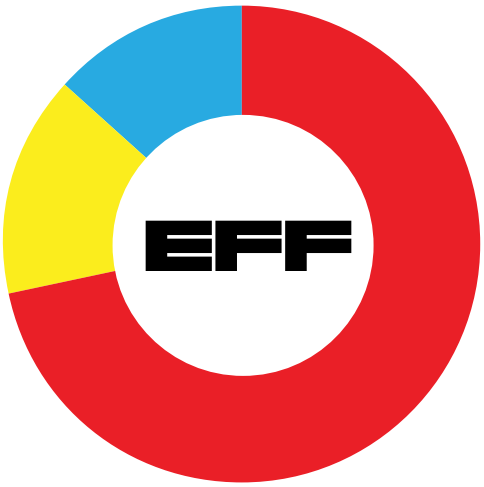
FY 2019-2020
PUBLIC SUPPORT

Individual	$ 8,575,908
Individual through Foundation	321,072
Foundation	434,366
Cy Pres	112,948
Employee & Customer-Directed Gifts	1,067,832
Corporate	369,251
In-kind Legal Services	101,150
Total Public Support	**$10,982,527**

FY 2019-2020
EXPENSES

Program	$ 10,699,683
Administrative	2,303,451
Fundraising	2,013,202
Total Expenses*	**$15,016,336**

*Includes Payroll Protection Program Loan.
See Page 38 for Net Expenses.



INCOME

PUBLIC SUPPORT

Individual Contributions	
Individual Contributions over $50,000	$1,541,865
Individual Contributions $10,000-$50,000	$1,130,968
Individual Contributions under $10,000	$5,903,075
Total Individual Contributions	$8,575,908
Individual Contributions through Foundations	
Individual Contributions through Foundations Over $50,000	$248,000
Individual Contributions through Foundations Up to $50,000	$73,072
Total Individual Contributions through Foundations	$321,072
Foundation Grants	$434,366
Cy Pres Awards	
Ossola, et al. v. American Express Company, et al.	$12,675
Cottage health Settlement	$100,273
Total Cy Pres Awards	$112,948
Corporate Contributions	
Employee and Customer-Directed Gifts*	$1,067,832
Other Corporate Contributions	$369,251
Total Corporate Contributions	$1,437,083
In-kind Legal Services	$101,150
TOTAL PUBLIC SUPPORT	**$10,982,527**

REVENUE

Net Investment Income	$1,398,645
Attorneys' Fees Awarded	$567,592
EFF Event Income, net of expenses	-$3,930
Miscellaneous	$76,701
TOTAL REVENUE	**$2,039,008**

TOTAL SUPPORT AND REVENUE $13,021,535

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

EXPENSES

Salaries & Benefits	$12,407,966
Legal & Professional Fees	$873,866
Membership Expenses	$473,775
Amortization & Depreciation	$283,218
Building Expenses	$260,238
Office Expenses	$150,890
Travel Expenses	$126,646
Litigation Expenses	$125,129
Corporate Insurance	$117,128
Planning & Development	$94,110
Furniture & Equipment Expense	$54,789
Other Administrative Expenses	$26,491
Awareness Events	$12,447
Intern Expenses	$6,936
Fundraising Expenses	$2,707
TOTAL EXPENSES	**$15,016,336**
Payroll Protection Program Loan (Loan Forgiven, February, 2021)	-$1,692,000
NET EXPENSES	**$13,324,336**

NET INCOME -$302,801

THANK YOU

EFF members around the world drive the movement for digital privacy, the free exchange of ideas, and an online world in which the public's interests come before corporations and politicians. Because of you, our values live in the law, in code, and in the way we defeat threats and champion progress. We're proud of and humbled by our members' passion for ensuring that technology supports freedom, justice, and innovation for all the people of the world. Together, we make a better digital future possible.

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