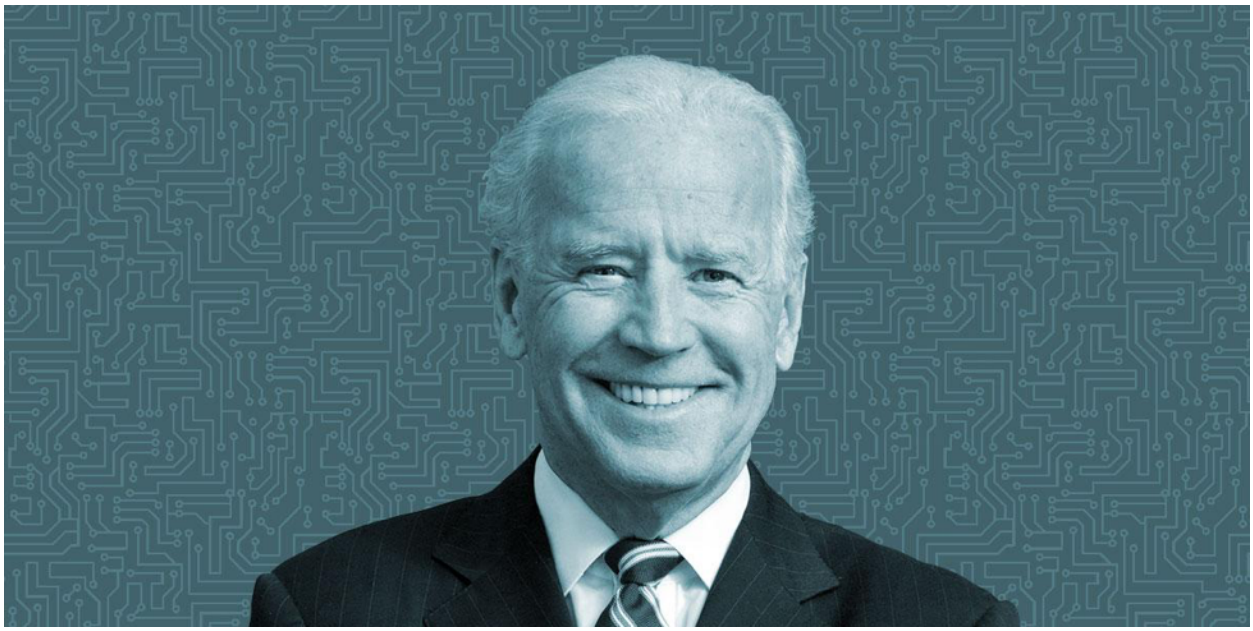
ELECTRONIC FRONTIER FOUNDATION

Transition Memo 2020



The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. We work to ensure that rights, freedoms, and innovation are enhanced and protected as our use of technology grows.

While we hope to work with you on a wide range of policies that affect digital rights in the coming years, we focus here on the ones that need your immediate attention and ask that you change course on the previous policies and practices discussed below.

If you have any questions or wish to discuss any of these topics further, please contact EFF's Legislative Counsel Ernesto Falcon at ernesto@eff.org or EFF's Director of Federal Affairs India McKinney at india@eff.org.

Thank you.

Table of Contents

1. Surveillance

As digital devices become cheaper and faster, all levels of government are moving to siphon up as much information as possible, insisting that such collection does not affect privacy and civil liberties until the government actually uses the data. Those same entities then proceed to fight any limitation on such use, on the theory that the data was "legally collected." This Catch-22 approach results in a system that no longer meets traditional 4th Amendment requirements. This trend needs to be reversed.

DOJ officials from both political parties have told Congress that the government needs to have "every tool in the toolbox" to keep the nation safe, and that Congress and the public should just trust them to do what is right. But a nation built on the rule of law does not depend on trust; it depends on transparency and accountability.

Stringent rules designed to protect privacy are not a referendum on the character of the people who work in law enforcement or in the intelligence community. Rather, they are an important tool in Congress and the Administration retaining the public's trust in government institutions.

Surveillance issues are also criminal justice issues and immigration issues. As biometric technology (like facial recognition) and artificial intelligence technology become cheaper and more accessible, it is imperative for Congress and the Administration to understand the inherent risks and to put strong protections in place to limit or restrict their use. Additionally, many forms of surveillance technology are often used first at the border before expanding to the interior of the country. Such technologies present risks to the privacy, security, and civil liberties of U.S. persons and non-U.S. persons alike.

Foreign Intelligence Surveillance Act

In 1978, after a revelation that the government was engaging in systematic domestic surveillance on domestic targets, Senator Frank Church convened a Senate investigative committee that produced a report[1] that led to the passage of the Foreign Intelligence Surveillance Act (FISA).[2] Most importantly, and in line with a Supreme Court ruling in 1973, FISA required an individualized, probable cause warrant for national security spying, just as the Fourth Amendment requires. While there is much to criticize in the original FISA, it did rein in the government, and together with the Church Committee report, ultimately put a stop to large scale domestic spying for decades.

Decades later, FISA is in dire need of reform. For too long, intelligence agencies have been allowed to secretly interpret and apply FISA authorities to pursue investigations and implement surveillance techniques that, when publicly disclosed, have shocked the public and eroded trust in our nation's intelligence services. [3]

---

[1] Assassination Archives and Research Center, *Church Committee Reports*, http://www.aarclibrary.org/publib/contents/church/contents_church_reports.htm (last accessed Nov. 19, 2020).

[2] 50 U.S.C. § 1801, et seq.

[3] R Street, Demand Progress, Freedom Works & Electronic Frontier Foundation, *Strengthening Congressional Oversight of the Intelligence Community* (Sept. 13, 2016),

When President George W. Bush authorized a broad warrantless wiretapping program and bypassed the Foreign Intelligence Surveillance Court (FISC) in 2001, almost immediately, there were concerns about how the Patriot Act would be used against Americans.[4] But unlike the relatively swift response in the 1970s, it took 15 years and a whistleblower's revelations to obtain even the modest statutory reforms in the USA Freedom Act.[5]

The past five years have shown those reforms were insufficient. At least three aspects of FISA will require the Administration and Congress's attention in the new term:

1) ensuring Section 215[6] is not reauthorized;
2) fundamentally reforming Section 702[7], which—even in its most narrow sense—is used to conduct surveillance on hundreds of thousands of individuals, resulting in the collection of billions of communications—without any type of individualized court review; and
3) strengthening other procedural and substantive aspects of FISA, including reforms to the procedures before the FISC and the notice and access requirements used in criminal prosecutions.

Section 215 must not be revived. First, it was regularly abused. From 2004 to 2013, the intelligence community—and, ultimately, the FISC—secretly interpreted Section 215 to authorize the surveillance and collection of millions of Americans call records. When this mass surveillance program was publicly exposed, it led to widespread public outcry; legislative reform; and, now, at least three federal courts have recognized the program was illegal.

Second, it was ineffective. The program never prevented a terrorist attack. Moreover, it was consistently plagued by operational problems; indeed, the NSA voluntarily terminated the program in 2019 following the latest in a series of compliance problems. In March 2020, with Section 215—and two other provisions of FISA—set to expire, Congress correctly allowed the law to sunset. It should not be reauthorized, and your Administration should ensure that mass call record surveillance does not occur under any other provision of FISA.

Section 702 should be fundamentally reformed. Section 702 is the primary legal authority the intelligence community uses to conduct warrantless electronic surveillance inside the United States against non-U.S. "targets" located outside the United States. Section 702 differs from other FISA authorities because the government can pick targets and conduct the surveillance without a warrant signed by a judge. Instead, the FISC merely reviews and signs off on the procedure. In 2019, the government conducted surveillance on over 200,000 targets—without a court ever reviewing the basis for any of those targeting decisions. Making matters worse, the intelligence community then uses those warrantlessly intercepted communications to search for

---

https://www.eff.org/files/2016/09/13/strengthening_congressional_oversight_of_the_ic_white_paper_sept_2016.pdf .

[4] Cindy Cohn & Trevor Timm, *In Response to the NSA, We Need a New Church Committee and We Need it Now*, EFF Deeplinks Blog (June 7, 2013), https://www.eff.org/deeplinks/2013/06/response-nsa-we-need-new-church-commission-and-we-need-it-now.

[5] Pub. L. 114-23 (2015).

[6] 50 U.S.C. § 1861.

[7] 50 U.S.C. § 1881, et seq.

the specific communications of U.S. persons (a so-called "backdoor search"). In 2019, intelligence agencies did this nearly 10,000 times. As currently operated, Section 702 is unconstitutional and in need of wholesale reform. It is scheduled to expire in 2023 and, absent comprehensive reform to the statute, it should not be reauthorized.

Other FISA reform is necessary. Other provisions of FISA remain outdated, incomplete, and ineffectual. For example, additional transparency is necessary in proceedings and decisions of the FISC, not least of which would be to respect the intention of Congress in releasing all significant opinions to the public. Also, the so-called amicus provision—an attempt to introduce an adversarial perspective in proceedings before the FISC—must be strengthened. Further, the provisions of FISA that require notice and disclosure to criminal defendants when FISA materials are used in the course of an investigation must be strengthened. Additionally, the Privacy and Civil Liberties Oversight Board (PCLOB), an independent agency in the executive branch created after a recommendation from the 9/11 Commission, must be fully staffed and given the resources to do the job it was created to do.

Recommendations

1) Do not seek to renew Section 215 authorities.
2) Do not renew Section 702 authorities; or at a minimum, do not do so without comprehensive reform without significant, comprehensive reform.
3) Ensure that all intelligence gathering programs are overseen by a robust legal review process with the authority to restrict or forbid unnecessary or illegal activities.

Facial Recognition Technology

Across the nation, federal, state, and local law enforcement agencies are using face recognition technology (FRT) to identify suspects, often with dire consequences. FRT uses computer algorithms to pick out specific, distinctive details about a person's face. These details, such as distance between the eyes or shape of the chin, are then converted into a mathematical representation and compared to data on other faces collected in an FRT database.

Research, including from the federal government, has shown over and over that FRT is flawed and misidentifies people, particularly people of color, women, young people, and transgender and nonbinary people. This issue is compounded by the fact that many police departments rely solely on FRT to identify subjects, rather than just serve as an investigatory lead. This can have disastrous consequences for people who are arrested as a result of a misidentification. For example, in Detroit, at least two Black men have been falsely arrested because of face recognition. One man is currently suing the city of Detroit.[8]

[8] Larry Hardesty, *Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems*, MIT (Feb. 11, 2018), https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212; Natalie O'Neill, *Faulty Facial Recognition Led to His Arrest – Now He's Suing*, Vice (Sept. 4, 2020), https://www.vice.com/en_us/article/bv8k8a/faulty-facial-recognition-led-to-his-arrestnow-hes-suing; Georgetown Law, *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Oct. 18, 2016), https://www.law.georgetown.edu/privacy-technology-center/publications/the-perpetual-line-up/ (last accessed Nov. 19, 2020).

FRT doesn't just impact people already caught up in the criminal justice system., During at least one of the Black-led protests happening in the summer in 2020, law enforcement used private cameras to unlawfully mass surveil protesters.[9] FRT would allow law enforcement to potentially identify leaders of those protests and track their movements. Thanks to information and image sharing between Departments of Motor Vehicles and other government agencies, the police are able to search the faces of millions of Americans with driver's licenses and compare them to suspects, regardless of whether those drivers have ever been accused of a crime. This subjects millions of people to constant suspicion and the threat of being falsely identified.[10]

As of Fall 2020, more than a dozen cities across the country have banned police use of face recognition. This includes large cities like San Francisco and Boston as well as other cities in California, Maine, Massachusetts, and Mississippi. California has also passed a state-wide moratorium on the use of FRT on police body-worn cameras. This movement is spreading rapidly, and a number of other cities are slated to consider similar bans in the coming months. The 116th Congress has also introduced several bills to ban or limit the use of FRT.

A number of companies that sell FRT, including Amazon, Microsoft, and IBM, have acknowledged the harms caused by police use of the technology and halted law enforcement acquisition of their products.

Recommendations: The federal government should ban government use of facial recognition technology and biometric technology. One way to start this process would be to support the passage of the Face Recognition and Biometric Technology Moratorium Act (S. 4084, in the 116th Congress), which would ban federal law enforcement use of FRT as well as curb some federal funding streams for local and state use of the technology.

Border Search and Immigration Surveillance

In recent years, the U.S. Department of Homeland Security has expanded its use of many forms of surveillance technology, first at the border, and in some cases, in the interior of the country.

Since 2017, EFF has challenged governmental policies permitting U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE) officers to conduct warrantless and usually suspicionless searches of electronic devices at the border. In FY 2019, CBP conducted more than 40,000 device searches, an eight-fold increase since FY 2012. EFF, ACLU, and ACLU of Massachusetts have a lawsuit pending in the U.S. Court of Appeals for the First Circuit, *Alasaad v. Wolf*, arguing that the government needs a warrant for border searches of electronic devices because of travelers' privacy interests in the vast amounts of sensitive

[9] Dave Maas & Matthew Guariglia, *San Francisco Police Accessed Business Ditrict Camera Network to Spy on Protestors*, EFF Deeplinks Blog (July 27, 2020), https://www.eff.org/deeplinks/2020/07/san-francisco-police-accessed-business-district-camera-network-spy-protestors.

[10] Thomas Germain, *Federal Agencies Use DMV Photos for Facial Recognition. Here's What You Need to Know*, Consumer Reports (July 08, 2019), https://www.consumerreports.org/privacy/federal-agencies-use-dmv-photos-for-facial-recognition/.

information contained within their devices.[11]

In addition to searches of digital devices, the past several years have seen a marked expansion of government proposals to collect biometrics, such as face prints, fingerprints, and DNA,[12] [13] both at the border and within the interior, from U.S. persons and non-U.S. persons.

In September 2020, the U.S. Department of Homeland Security (DHS) issued a notice of proposed rulemaking to expand the collection of biometrics from applicants for immigration benefits.[14] The proposed rule would allow for collection of biometrics beyond the current status quo of fingerprints, photos, and signatures to include palm prints, voice prints, iris scans, facial images, DNA, and even behavioral biometrics. The proposed rule would mandate biometrics collection from anyone applying for an immigration benefit, such as including immigrants and their U.S. citizen and lawful permanent resident family members. In this case, immigration benefits would include applications for permanent residency or naturalization, or petitioning for a family member to come to the U.S. EFF has called on DHS to rescind this proposed rule, pointing to grave threats to privacy, security, and civil liberties without justification or even the statutory authority to do so.[15]

Additionally, EFF has identified several other surveillance technologies at the border such as Automated License Plate Readers (ALPRs). ALPRs can collect massive amounts of sensitive location information, which can impact the privacy of people living in border communities. As EFF explained to a federal court n 2019, law enforcement must obtain a warrant to use databases of ALPR location information.[16]

In a different kind of digital surveillance, since May 2019, the U.S. Department of State has required nearly all U.S. visa applicants to disclose their social media accounts on their visa applications—a requirement that affects nearly 14.7 million people annually.[17] EFF opposes this

---

[11] Electronic Frontier Foundation, *Alasaad v. Wolf*, https://www.eff.org/cases/alasaad-v-duke (last visited Oct. 20, 2020).

[12] Jennifer Lynch, *Genetic Genealogy Company GEDmatch Acquired by Company With Ties to FBI & Law Enforcement – Why You Should Be Worried*, EFF Deeplinks Blog (Dec. 10, 2019), https://www.eff.org/deeplinks/2019/12/genetic-genealogy-company-gedmatch-acquired-company-ties-fbi-law-enforcement-why.

[13] Saira Hussain, *DOJ Moves Forward with Dangerous Plan to Collect DNA from Immigrant Detainees*, EFF Deeplinks Blog (March 19, 2020), https://www.eff.org/deeplinks/2020/03/doj-moves-forward-dangerous-plan-collect-dna-immigrant-detainees.

[14] *Collection and Use of Biometrics by U.S. Citizenship and Immigration Services*, 85 Fed. Reg. 56338 (proposed Sept. 11, 2020).

[15] Saira Hussain, Jennifer Lynch, and Nathaniel Sobel, *EFF Files Comment Opposing the Department of Homeland Security's Massive Expansion of Biometric Surveillance*, EFF Deeplinks Blog (Oct. 22, 2020), https://www.eff.org/deeplinks/2020/10/eff-files-comment-opposing-department-homeland-securitys-massive-expansion.

[16] Andrew Crocker, *To Search Through Millions of License Plates, Police Should Get a Warrant*, EFF Deeplinks Blog (Mar. 22, 2019), https://www.eff.org/deeplinks/2019/03/search-through-millions-license-plates-police-should-get-warrant.

[17] Brennan Center for Justice, *Doc Society v. Pompeo*, https://www.brennancenter.org/our-work/court-cases/doc-society-v-pompeo (last visited Nov. 19, 2020).

registration requirement because the policy invades privacy and chills the freedom of speech and association of both visa applicants and those in their social networks, including U.S. persons.[18]

Recommendations

1) Reverse the harmful expansion of surveillance technologies at the border.
2) Require a warrant to search a traveler's electronic device when they cross the border.
3) Block the proposed rule to expand the use of biometrics for all persons at the border.
4) Require a warrant to search a database of ALPR location information.
5) Reverse the policy that requires visa applicants to disclose their online activity.

[18] Sophia Cope & Saira Hussain, *EFF to Court: Social Media Users Have Privacy and Free Speech Interests in Their Public Information*, EFF Deeplinks Blog (June 30, 2020), https://www.eff.org/deeplinks/2020/06/eff-court-social-media-users-have-privacy-and-free-speech-interests-their-public.

2. Encryption

For thousands of years, people have used encryption to send messages to each other that (hopefully) couldn't be read by anyone besides the intended recipient. Today, digital encryption technology allows individuals to use encryption for everything from simple secure messaging to more elaborate purposes, such as verifying authorship or protecting the content of digital devices.

That ability is more essential than ever. As our digital devices grow more powerful, our privacy, ironically, grows more vulnerable – to bad actors, hostile governments, and/or service providers that wish to exploit our data for commercial purposes. Encryption is the best technology we have to protect our digital security.

Nevertheless, law enforcement, some Senators, and multiple high-ranking officials at the DOJ have argued that strong security measures have impeded legitimate law enforcement activities and that the protocols should be altered in various ways to allow "exceptional access." These proposals would undermine everyone's safety and should be uniformly rejected.

Background on Encryption Backdoors

In the 1990s, EFF led the fight to protect encryption and turn back government efforts to "backdoor"[19] secure communications, such as the "Clipper Chip." In collaboration with leading academics, industry associations, and politicians, we also helped establish that backdoors designed to provide the government with access to encrypted data leave an opening for malicious actors. EFF also successfully challenged export regulations that effectively prevented the development and distribution of strong encryption, establishing the legal principle that "code is speech" protected by the First Amendment.

After the failure of the Clipper Chip proposal, it seemed that the "Crypto Wars" had been resolved in favor of the right to create and use strong encryption, free of government-mandated backdoors. Even the 1994 Communications Assistance for Law Enforcement Act (CALEA)—which forced telephone companies to redesign their network architectures to make it easier for law enforcement to wiretap digital telephone calls—preserves the ability to use end-to-end encryption. In the last two decades, encryption has become widespread in technologies used by individuals, businesses, and the government itself. Apps such as WhatsApp and Signal are examples of secure messaging, which guarantees that no one but you and your intended recipients can read your messages or otherwise analyze their contents to infer what you are talking about. These applications implement end-to-end encryption, [20] which is the process by which a message is turned into a secret message by its original sender and is only able to be

[19] A "backdoor" is any mechanism someone designs into a system that allows for access via bypassing normal security measures. And although the word "backdoor" was historically used most often to refer to secret ways to access a system, a backdoor doesn't need to be secret.

[20] Electronic Frontier Foundation, *Surveillance Self-Defense: End-to-End Encryption*, https://ssd.eff.org/en/glossary/end-end-encryption (last accessed Nov. 19, 2020).

decoded by its final recipient.[21] Encryption also allows users of iPhones and Android devices to keep their data secure. In late 2016, a joint, bipartisan report produced by the House Commerce and Judiciary Committees concluded that "encryption is inexorably tied to our national interests" and "is a safeguard for our personal secrets and economic prosperity."[22]

However, in the last several years, FBI and DOJ representatives have renewed their efforts to obtain legal authority to force companies to build backdoors. They point to cases like the 2016 San Bernardino attack, in which the FBI misleadingly argued it could not access the contents of an encrypted iPhone. These agencies call for providers of encryption technology to either voluntarily include "lawful access" mechanisms in their products, or be forced to do so legislatively.

Despite a longstanding expert consensus that it is impossible to require a mechanism for government to "lawfully access" the contents of encrypted data without undermining the security of the system[23], there have been several legislative proposals to require such government backdoors. The most recent is the sweeping Lawful Access to Encrypted Data Act (LAEDA), S. 4051 (116th Cong.), which would give the Justice Department the ability to require that manufacturers of encrypted devices and operating systems, communications providers, and many other companies must have the ability to decrypt data upon request.

Furthermore, recent reporting has shown that law enforcement officials are able to bypass encryption on phones far more often than previously understood.[24] Upturn, a non-profit, recently released a comprehensive report that demonstrates that state and local law enforcement agencies have performed hundreds of thousands of cellphone extractions since 2015, often without a warrant, all while many leaders of the law enforcement community were asking Congress to force companies to break encryption protocols.[25] This reporting demonstrates that rather than requiring companies to allow "lawful access," Congress and the Administration should instead be conducting oversight into how often and under what circumstances law enforcement agencies access the contents of encrypted devices.

Recommendations

1) Reject LAEDA and other attempts to mandate government backdoors to encrypted, secure software and devices.
2) Produce a formal administration policy in favor of encryption.

---

[21] Andrew Crocker & Gennie Gebhart, *Don't Let Encrypted Messaging Become a Hollow Promise*, EFF Deeplinks Blog (July 19, 2019), https://www.eff.org/deeplinks/2019/07/dont-let-encrypted-messaging-become-hollow-promise.

[22] House Judicial Committee & House Energy and Commerce Committee, *Encryption Working Group Year-End Report* (Dec. 20, 2016), https://web.archive.org/web/20170101203556/http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/documents/114/analysis/20161219EWGFINALReport_0.pdf (Last Accessed Nov. 19, 2020).

[23] MIT Press, *'Keys Under the Doormats" Security Report* (July. 10, 2015), https://mitpress.mit.edu/blog/keys-under-doormats-security-report.

[24] Logan Koepke, Emma Weil & Urmila Janardan, *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones*, Upturn (Oct. 2020), https://www.upturn.org/reports/2020/mass-extraction/.

[25] Shira Ovide, *Police Can Open Your Phone. It's Okay*, New York Times (Oct. 21, 2020), https://www.nytimes.com/2020/10/21/technology/police-can-open-your-phone-its-ok.html.

End-to-End Encryption and Client-Side Scanning

Encryption backdoors are a straightforward attempt to undermine encryption. But sometimes, people claim they can have their cake and eat it too: keep messages encrypted, but also allow some parties to gain access to those messages. This is fundamentally impossible, but the proposals keep coming.

The most prominent idea is called client-side scanning. This privacy-invasive proposal works like this: every time you send a message, software that comes with your messaging app first checks it against a proprietary database of "hashes," or unique digital fingerprints, usually of images or videos. If it finds a match, it may refuse to send your message, notify the recipient, or even forward it to a third party, possibly without your knowledge.

Proposals to do client-side scanning purport to give us the best of all worlds: they claim to preserve encryption, while also combating the spread of illegal or morally objectionable content. In reality, while it may technically maintain *some* properties of end-to-end encryption, client-side scanning would render the user privacy and security guarantees of encryption hollow by allowing third parties to decrypt any content they put in the database.

Most important, it is impossible to build a client-side scanning system that can only be used to scan for a single type of content. For instance, the same system that scans for child abuse images can and eventually will be used by governments around the world to read protesters' communications. As a consequence, even a well-intentioned effort to build such a system will break key promises of the messenger's encryption itself and open the door to broader abuses.

Client-side scanning is at the heart of the debate over the EARN IT Act (S. 3398), introduced in early March. EARN IT's sponsors claim it would not break encryption, noting that the proposed bill doesn't refer to encryption directly. But in practice, the proposed legislation creates the opportunity for an all-out assault on encryption by forcing companies to adopt weaker encryption protocols through various measures. In its original form, the commission created by EARN IT would have banned encryption outright. The Manager's Amendment added in July by Sen. Patrick Leahy (D-VT) doesn't eliminate this problem; instead it empowers over 50 jurisdictions to follow Attorney General Barr's lead in targeting encryption.

Sen. Leahy's amendment prohibits holding companies liable because they use "end-to-end encryption, device encryption, or other encryption services." But the bill still encourages state lawmakers to look for loopholes to undermine end-to-end encryption, such as demanding that messages be scanned on a local device, before they get encrypted and sent along to their recipient. We think that would violate the spirit of Senator Leahy's amendment, but the bill opens the door for that question to be litigated over and over, in courts across the country.

***Recommendation*:** Reject EARN IT and other attempts to covertly mandate government backdoors to encrypted, secure software and devices.

3. Broadband

21st-Century-Ready Access for All Americans

Universal fiber-to-the-home (FTTH) networks are the proper foundation of 21st century-ready-broadband access.[26] Fiber networks are future proof and the only type of infrastructure that have a cost-effective basis to scale up ahead of consumption for decades. The incumbent local exchange carriers (ILEC) and cable industry, however, have mostly stopped transitioning their networks over to fiber. By contrast, small private and local public networks are actively deploying FTTH in even the most rural areas at a density as low as 2.5 people per square mile.[27] Lastly, 5G high-speed broadband access competition is contingent on the availability of dense fiber networks on the ground that come from FTTH deployments.[28] These market failures are why the United States has the slowest and most expensive Internet access market among modern economies[29] while the EU and advanced economies in Asia march forward with universal fiber plans.

It is now long past time for the Federal Communications Commission (FCC) to reverse the course set in 2005 when the agency concluded that regulating fiber networks was unnecessary to promote competition, affordability, and universal access. Since then, fiber networks have disproportionately favored the upper half of the median income while ignoring both rural and low-income neighborhoods throughout the United States. Such a deployment of FTTH has resulted in not just a digital divide, but a speed and price chasm among broadband choices.

The new FCC must establish a universal fiber policy and begin adopting new models to promote its deployment. Some examples of new models include Alabama's joint ventures between power utility and fiber providers; Utah's multi-city funded construction of an open-access fiber network; and South Korea's mandated fiber sharing to promote national 5G coverage. Each of these approaches has promoted more high-speed access to broadband rather than deterred it.

Recommendations:

1) Swift passage of Majority Whip Clyburn's Accessible, Affordable Internet for All Act.
2) Reinstatement of the FCC's authority to regulate broadband providers in order to institute open access policies and mandatory build-out for low-income communities in cities to close the digital divide.
3) Updating the FCC's broadband standard to 100/100 mbps low latency to assess where fiber infrastructure is and is not being deployed.

---

[26] Bennett Cyphers, *The Case for Fiber to the Home, Today: Why Fiber is a Superior Medium for 21st Century Broadband*, EFF Deeplinks Blog (Oct 11, 2019), https://www.eff.org/files/2019/10/15/why_fiber_is_a_superior_medium_for_21st_century_broadband.pdf.

[27] Christopher Mitchell, *United Fiber Tackles Missouri's Most Rural-Community*, Broadband Bit Podcast (Feb. 14, 2017), https://muninetworks.org/content/united-fiber-tackles-missouris-most-rural-community-broadband-bits-podcast-240.

[28] Wireless Infrastructure Association, *Fiber: Inextricably Linked with 5G Connectivity*, WIA Blog (Aug. 19, 2020), https://wia.org/blog/fiber-inextricably-linked-with-5g-connectivity.

[29] Becky Chao & Claire Park, The Cost of Connectivity 2020, Open Technology Institute (Jul. 15, 2020), https://www.newamerica.org/oti/reports/cost-connectivity-2020.

Net Neutrality and Public Safety

Net neutrality is the idea that Internet Service Providers (ISPs) should treat all data that travels over their networks fairly, without improper discrimination in favor of particular apps, sites, or services. At its core, net neutrality is a principle of equity and a protector of innovation, ensuring that large monopolistic ISPs don't get to use their gatekeeping roles to determine winners and losers in the marketplace for services products – or ideas. All services, sites, and apps get the same treatment, succeeding or failing based on their merits.

In 2015, the FCC adopted the Open Internet Order, which prohibited ISPs from engaging in blocking, throttling, or paid prioritization, protecting a free and open Internet. 86% of Americans supported these rules.[30] Nonetheless, in 2017 the Trump Administration's FCC repealed these protections in the so-called "Restoring Internet Freedom Order."

Today, Internet access remains an incredibly concentrated market with growing monopolization in high-speed access. As a result, most Americans—particularly rural Americans—are at the mercy of their Internet providers. Without net neutrality, those Internet providers can intervene to shape our online experience by blocking and slowing down access to sites and services while favoring others.

ISPs have proven themselves more than willing to do so.[31] For example, in the years that have followed the repeal, AT&T announced that it would not count HBO Max, a service it owns, against mobile plan data caps.[32] Not counting the data used by an app against a data cap is a practice known as a "zero-rating." This practice, and any practice that preferences some data over others, distorts the information market. Low-income and rural users can end up spending most of their Internet time on zero-rated services, which limits their access to information to what is on those services. To take another example, in places where Facebook was zero-rated, users concentrated most of their Internet time on Facebook,[33] which means their consumption of online information was largely controlled by Facebook's choices.

These problems are magnified in rural, low-income, and BIPOC communities, which are more likely to rely on mobile devices for Internet access. About 20 percent of Americans are "smartphone-only," that is, they do not have a home broadband subscription, only a

---

[30] Overwhelming Bipartisan Public Opposition to Repealing Net Neutrality Persists, University of Maryland (April 18, 2018), https://www.publicconsultation.org/united-states/overwhelming-bipartisan-public-opposition-to-repealing-net-neutrality-persists

[31] Timothy Karr, *Net Neutrality Violations: A Brief History*, Free Press (January 24, 2018), https://www.freepress.net/our-response/expert-analysis/explainers/net-neutrality-violations-brief-history.

[32] Nilay Patel, *HBO Max Won't Hit AT&T Data Caps, But Netflix and Disney Plus Will*, The Verge (June 2, 2020), https://www.theverge.com/2020/6/2/21277402/hbo-max-att-data-caps-netflix-disney-plus-streaming-services-net-neutrality.

[33] Danelle Dixon, *Mozilla Releases Research Results: Zero Rating Is Not Serving as an On-Ramp to the Internet*, Mozilla (July 31, 2017), https://blog.mozilla.org/blog/2017/07/31/mozilla-releases-research-results-zero-rating-not-serving-ramp-internet/ (last visited Oct. 20, 2020)

smartphone.[34] Black, Hispanic, lower-income, young, and rural Americans are all more likely to rely on their smartphones for Internet access than their peers.[35]

During the pandemic, the need for high-speed, reliable Internet access is even more clear. Americans need to be able to communicate and access reputable information, regardless of whether the communications service or information website is a preferred partner of their provider. In emergencies, for example, the blocking of Skype or Google Voice would go from anti-competitive to disastrous.

Net neutrality is even more important for our first responders. In July of 2018, the Mendocino Complex Fire ravaged California. At the time, it was the largest fire in California history. In fighting that fire, Santa Clara County in California deployed a vehicle to "track, organize, and prioritize routing of resources from around the state and country to the sites where they are most needed."[36] Verizon throttled the data flowing to the fire department's vehicle. When the county asked Verizon to restore full speed, the company attempted to upsell them. Such conduct would have run afoul of the general ban against unjust and unreasonable conduct under the 2015 Open Internet Order.

Recommendations

1) Reclassify broadband providers into Title II common carriers and institute updated net neutrality rules to prohibit discriminatory zero-rating practices.
2) Work with states to promote public safety practices to avoid a repeat of the Verizon-Santa Clara fire incident.
3) Terminate Department of Justice litigation against states attempting to enact consumer protection statues such as SB 822, California's net neutrality law. The federal government should work in partnership with states to protect consumer Internet access rights.

[34] Pew Research Center, *Internet/Broadband Fact Sheet* (June 12, 2019), https://www.pewresearch.org/internet/fact-sheet/internet-broadband (Last Accessed Nov. 19, 2020).
[35] *Id*.
[36] Declaration of Fire Chief Anthony Bowden in Mozilla Corporation v. FCC, (August 20, 2018), https://www.sccgov.org/sites/opa/newsroom/Documents/Bowden%20Decl%20and%20Ex%20A.pdf.

4. Section 230

All Internet users rely on multiple online services to connect, engage, and express themselves online. That means we also rely on 47 U.S.C. § 230 ("Section 230"), which provides broad—but not absolute—legal protections to platforms when they offer their services to the public and when they moderate the content that relies on those services, from the proverbial cat video to an incendiary blog post.

Internet intermediaries—including ISPs, web hosting companies, websites, and social media platforms—enable users to share and access content online. Without these companies, the Internet would not function. And without Section 230—or even with a weakened Section 230—online platforms would be encouraged to limit their own liability by removing far more user content, which would be bad for everyone's opportunity to be heard on the Internet.

Section 230 is an essential legal pillar for online speech. As EFF told Congress in 2019,[37] the creation of Section 230 ushered in a new era of community and connection on the Internet. People can find friends old and new over the Internet, learn, share ideas, organize, and speak out. Those connections can happen organically, often with no involvement on the part of the platforms where they take place. Some of the most vital modern activist movements—#MeToo, #WomensMarch, #BlackLivesMatter—are universally identified by hashtags.

However, when powerful people don't like that speech, disagree with the content moderation decisions from a platform, or just don't like the platforms that host it, they often blame Section 230's protections.

These attacks are often based on a fundamental misunderstanding of the law. In passing Section 230, Congress made the deliberate choice to protect online free speech and innovation, while also providing discrete tools to go after culpable companies. The world has changed in many ways, but online innovation and the speech it enables is more important, not less, than it was two decades ago. As it was originally written, Section 230 allows good-faith moderation by platforms without fear of taking on undue liability for their users' posts. Altering the law to force the removal of so-called "disinformation," to demand the political neutrality of their decisions, or to broaden platform liability for already-unlawful content would have consequences that reach far beyond the intended targets.

A better approach would be to adopt policies to foster competition in social media, so that users who object to a given platform, based on its content moderation choices or for any other reason, can go elsewhere. For example, some users who objected to Twitter's moderation choices during the 2020 election migrated to an alternative service, Parler.[38]

---

[37] Corynne McSherry, *Testimony to House Committee on Energy and Commerce on Section 230*, EFF Documents Page (Oct. 16, 2019), https://www.eff.org/document/testimony-house-energy-and-commerce-committee-section-230.

[38] Jason Murdock, *Parler Tops App Store Charts as Conservatives Flock to Site After Biden Victory over Trump*, Newsweek (Nov. 9, 2020), https://www.newsweek.com/parler-tops-app-store-ios-android-charts-conservatives-twitter-biden-trump-election-1545921.

Deepfakes

Deepfake is a portmanteau of "deep learning" and "fake," and refers to images or video generated using machine-learning techniques that combine existing images and videos onto source images or videos. The purpose of this is to make videos or images that appear authentic but are not. Deepfakes can be used to create pornographic videos that convincingly splice the face of one real person (such as a celebrity) onto the body of another. They have also been used to depict public figures, including elected officials and celebrities, saying things that they did not in fact say. Additionally, some researchers and members in the intelligence community collected evidence that foreign intelligence operatives have used deep fake photos to create fake social media accounts from which they have attempted to recruit Western sources or influence events.[39] [40]

Unfortunately, the term deepfake is often used by the public and elected officials to describe *any* edited or altered video or image, despite the fact that individuals have been doctoring photos, splicing new video into historical footage, and altering news stories since long before machine learning existed.

This has practical consequences for any proposed legislation or regulations; a vague definition of deepfakes would render either ineffective. After all, if any altered media is considered a deepfake, then all kinds of innocuous media—including Forrest Gump being spliced into black-and-white footage—could be subject to regulation.

Sweeping every piece of altered media into deepfakes regulation would also raise significant First Amendment concerns. People frequently alter media for parody, satire, and criticism. Each Presidential candidate has published spliced footage of their opponent. Such expression, even when designed to be caustic or extremely critical of the targets, is protected by the First Amendment.

Some have proposed amending Section 230 to force platforms to police deepfakes more aggressively by increasing their liability risk. This idea should be rejected. First, it is unnecessary. As currently written, that law does not prohibit a victim of a deepfake from seeking civil remedies against the creator, nor would it protect an online service that created or materially contributed to the creation of a harmful deepfake.

Second, amending Section 230 to make online services civilly liable for hosting user-generated deepfakes would result in broad censorship of legitimate and lawful online expression. If a platform faces liability for hosting a user-generated deepfake, it would likely to react by prohibiting anyone from posting altered images or video, even those that are not deepfakes and those that are valuable parody and satire.

---

[39] Ben Collins & Brandy Zadrozny, *How a Fake Persona Laid the Groundwork for a Hunter Biden Conspiracy Deluge*, NBC News (Oct. 30, 2020), https://www.nbcnews.com/tech/security/how-fake-persona-laid-groundwork-hunter-biden-conspiracy-deluge-n1245387.

[40] Kelley M. Sayler & Laurie A. Harris, *Deep Fakes and National Security*, Congressional Research Service (Aug. 26, 2020), https://crsreports.congress.gov/product/pdf/IF/IF11333.

Recommendation: Any proposal regarding deepfakes must (1) properly define deepfakes and (2) limit its reach to harmful conduct such as endangering a person's physical safety or engaging in harassment.

Mandated Political Neutrality

In two early cases over Internet speech, courts allowed civil defamation claims against Prodigy but not against its competitor Compuserve; a judge reasoned that since Prodigy deleted some messages for "offensiveness" and "bad taste," it was responsible for the posts it *didn't* screen. Rep. Chris Cox has called this decision "surpassingly stupid" and cites it as a motivation for introducing the Internet Freedom and Family Empowerment Act, which would later become Section 230.

Creating additional hoops for platforms to jump through in order to maintain their Section 230 protections would lead them to provide even fewer opportunities to share opinions and experiences online, not more. Around the world, the groups actually silenced on Facebook and other platforms are often those marginalized in other areas of public life.[41]

However, exactly this kind of content moderation, which Section 230 is meant to protect, has come under attack. Several Republican Senators and Members of Congress, as well as the Trump Administration, have wrongly claimed that Section 230 requires platforms to be "politically neutral." They also have written legislation demanding that platforms freely allow objectionable user-generated content to flourish on their services, or lose legal protections under Section 230 when they exercise their First Amendment rights to moderate users' speech.

This is an unconstitutional condition that violates the First Amendment.[42] It is also impractical. While there are reasons to be concerned about politically motivated takedowns of legitimate online speech, this approach would be counter-productive.

We also oppose legislation that would require platforms to remove "disinformation," or deprive platforms of Section 230 protection if they declined to do so. False speech is generally protected under the First Amendment.[43] Facebook and Twitter should not be tasked with being the arbiters of truth—that is not a role they want, and they are not competent to perform this role. Nor are the government officials that would be called upon to determine whether platforms complied with such a law. Conditioning Section 230 protections on the veracity of the content a platform allows is neither useful nor constitutional.

Recommendation: Avoid passing legislation that is both unconstitutional and impractical.

---

[41] Jillian C. York & Karen Gullo, *Offline/Online Project Highlights How the Oppression Marginalized Communities Face in the Real World Follows Them Online*, EFF Deeplinks Blog (March 6, 2018), https://www.eff.org/deeplinks/2018/03/offlineonline-project-highlights-how-oppression-marginalized-communities-face-real.

[42] Sophia Cope & Aaron Mackey, EFF EARN IT Act First Amendment Letter to SJC, EFF Documents Page (March 9, 2020), https://www.eff.org/document/eff-earn-it-act-first-amendment-letter-sjc.

[43] *U.S. v. Alvarez*, 567 U.S. 702 (2012) ("some false statements are inevitable if there is to be open and vigorous expression of views in public and private conversation, expression the First Amendment seeks to guarantee")

CSAM, Sex Trafficking and other Unlawful Content

Section 230 generally bars claims against Internet intermediaries based on federal civil law, and state criminal and civil law. However, the statute does not bar claims based on federal criminal law, intellectual property law, certain communications privacy laws, and (as recently amended) certain anti-sex trafficking laws.[44]

Opponents to Section 230 argue that the law should be further amended to strip companies' immunity for a variety of concerning third-party content, including child sexual abuse material ("CSAM"). Yet current law already provides robust protection for victims of such content: if an online service provider has knowledge of an apparent or imminent violation of anti-CSAM laws, it must notify the National Center for Missing and Exploited Children's (NCMEC) CyberTipline, which in turn notifies the appropriate law enforcement agencies.[45] This system results in millions of reports being sent to law enforcement each year.[46] If companies willfully fail to report, they may be fined hundreds of thousands of dollars. [47]

Weakening Section 230 protection would give states a green light to hold Internet intermediaries criminally and civilly responsible for CSAM on their services that they might not even know about. Such a massive expansion of legal exposure will incentivize online platforms to over-censor legitimate user content, to mitigate the risk that they will be held liable for the illegal actions of their users. There is no evidence that this would actually help children in the real world. But it would cause platforms to restrain vast quantities of user content, creating fewer and less diverse avenues for online speech.

Recommendation: Section 230 should not be altered.

[44] 47 U.S.C. § 230(e).

[45] 18 U.S.C. § 2258A.

[46] *NCMEC Data*, National Center for Missing and Exploited Children, https://www.missingkids.org/ourwork/ncmecdata (16.9 million reports to the CyberTipline in 2019).

[47] 18 U.S.C. § 2258A(e)

5. Consumer Privacy

Big businesses are harvesting and monetizing our personal data on an unprecedented scale. Because our nation's privacy laws have not kept up, these companies are free to put their profits before our privacy. They build increasingly comprehensive dossiers about our lives, choices, and preferences, by using shadowy and sophisticated technologies to scrutinize our movements, online "clicks," and personal relationships.

This is a grave menace to our privacy and other liberties. Hackers can steal our data, leading to identity theft and stalking. Employees can misuse it, leading to harassment. Corporate executives can deploy it in ways consumers could never imagine. Police can seize it, to spy on protesters. Immigration officers can buy it, to locate and deport immigrants.

Consumer Privacy Legislation

More than 90% of Americans feel that they have no control over their data or their online privacy.[48] Congress and the Administration should be working to give control back to individual people, instead of letting the companies dictate users' legal rights.

Data collection, harvesting and subsequent monetization have become an extremely lucrative industry. An industry whose entire business model depends on collecting as much information from individuals as possible cannot be trusted to regulate their own activities. Government must create a strong federal privacy law that gives consumers real power to stop invasive practices.

EFF urges inclusion of the following provisions in any federal comprehensive privacy law:

- *No preemption*. The states are laboratories of democracy. Many have enacted important data privacy laws, including California's Consumer Data Privacy Act, Illinois' Biometric Information Privacy Act, and Vermont's Data Broker Registration Act. A federal data privacy law must expressly not preempt stronger state privacy laws.
- *Private right of action*. A law without strong enforcement is just a piece of paper. No agency will have sufficient resources to address every violation of a law. Also, regulated businesses too often have undue influence over agency enforcement decisions. So, people need a private right of action,[49] so they can sue businesses that violate their statutory privacy rights.
- *No "pay for privacy" schemes*. Businesses frequently require consumers to pay for privacy,[50] by withholding discounts or providing inferior service when a consumer refuses to share their personal data. These schemes must be prohibited, because they

[48] Lee Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, Pew Research Center (March 27, 2018), https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/.

[49] Adam Schwartz, *You Should Have the Right to Sue Companies That Violate Your Privacy*, EFF Deeplinks Blog (Jan. 7, 2019), https://www.eff.org/deeplinks/2019/01/you-should-have-right-sue-companies-violate-your-privacy.

[50] Adam Schwartz, *The Payoff From California's "Data Dividend" Must Be Stronger Privacy Laws*, EFF Deeplinks Blog (Feb. 15, 2019), https://www.eff.org/deeplinks/2019/02/payoff-californias-data-dividend-must-be-stronger-privacy-laws.

discourage everyone from exercising their privacy rights, and lead to income-based privacy "haves" and "have-nots."

- *Opt-in consent.* Businesses should be required to obtain informed, opt-in consent before processing a consumer's personal information.
- *Data minimization*. Businesses should be prohibited from processing a consumer's personal information beyond what is necessary to provide the good or service that they requested.
- *Rights to access, port, correct, and delete*. Businesses must be required, on request from a consumer, to provide access to their data (including in a portable electronic form), to correct errors, and to delete it.
- *Worker protections*. Employers increasingly deploy surveillance technologies to scrutinize their workers. Federal legislation must protect workers as well as consumers.
- *Information fiduciaries*. When a consumer gives their personal data to an online company, it should be required to exercise loyalty and care in its use of that data.

Recommendation: Pass robust, comprehensive federal consumer data privacy legislation with strong enforcement mechanisms.

Private Companies and Facial Recognition/Biometrics

Clearview AI, a private company, extracted faceprints from billions of photos without anyone's consent, and sells police departments the service of identifying the unknown people in probe photos. This is a grave menace to biometric privacy. It exemplifies the way that companies place their profits over our privacy, and unduly amplifies the surveillance powers of police agencies.

To ensure that companies like Clearview do not collect consumers' biometric data without their knowledge or consent, Congress and the Administration should include protections against this kind of collection in a comprehensive federal consumer data privacy legislation. For example, private companies that collect, use, retain, or share information about us—including our face prints or other biometric information—should be required to get informed opt-in consent before doing so.

Recommendation: Comprehensive federal privacy legislation that gives consumers real power over their data and real power to fight back.

Student Data

The federal government provides privacy protections for children, both online and while in school, through the Family Educational Rights and Privacy Act (FERPA), which applies to schools that receive federal funding.[51] FERPA forbids schools from disclosing student information without parental consent.

[51] U.S. Department of Education, *Family Education Rights and Privacy Act (FERPA)*, https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html#:~consumer-privacy (Last Accessed Nov. 19, 2020).

But FERPA has limitations: (1) it only applies to certain types of student information; and (2) there are exceptions which can be exploited. Even before distance learning became the norm, schools were increasingly adopting surveillance technology to spy on students at school, at home, and on their social media. School districts can use a loophole in the law to get around the parental consent requirement by characterizing educational software companies as "school officials," and some schools condition a student's access to education on their participation and cooperation in these systems. These "ed tech" and student surveillance companies gather, retain, and share vast amounts of sensitive data on students, their lives, and even their families.[52]

This surveillance includes: social media monitoring; AI scanning of documents, emails, and messages; spyware on school- and student-owned devices; cameras with tracking capabilities and facial recognition; microphones with aggression-detection capabilities; monitoring and filtering of web browsing; and location tracking.

This data is often shared with additional third parties, which increases the risk of a data breach. Millions of students have already had their data stolen, yet they have no way to ensure it will not happen again because they cannot opt out of this data ecosystem.

In the COVID-19 crises, many schools are also utilizing remote learning and testing platforms that further invade the privacy of students and their families. This is particularly egregious when students' academic success is tied to this monitoring, as with remote test proctoring technologies. These tools involved compelled mass biometric surveillance of potentially millions of students, whose success will be determined not by correct answers, but by algorithms that decide whether their "suspicion" score is too high.

Recommendations

1. Reform the Family Educational Rights and Privacy Act (FERPA) to exclude third-party education technology vendors from being considered "school officials," thus requiring prior consent for educational records to be released to tech companies. This could be accomplished by amending the statute or 34 CFR § 99.31(1)(i)(B).
2. Amend FERPA to establish a private right of action for students and families to take action against schools and Ed Tech companies.
3. Ban the use of surveillance technologies in educational settings, including but not limited to facial recognition, social media surveillance, and personal device surveillance.

[52] Caroline Haskins, *Gaggle Knows Everything About Teens and Kids in School*, Buzzfeed News (Nov. 1, 2019), https://www.buzzfeednews.com/article/carolinehaskins1/gaggle-school-surveillance-technology-education.

COVID and Health Data Privacy

COVID-19 has exposed many weaknesses in our U.S. public health system, including potential damage to our privacy. First, even in 2001 experts recognized that public health law was badly in need of reform.[53] Second, the massive amounts of personal health data generated during prevention, contact tracing, treatment, and epidemiological research are appetizing to data-hungry tech giants.

Third, government is stressed during emergencies like a pandemic, which can make it susceptible to sweetheart deals with private companies (perhaps paying them with *our* data). This point deserves emphasis because many people assume that public health data is protected by the federal Health Insurance Portability and Accountability Act (HIPAA). It is not. Public health authorities are not "covered entities"[54] —so HIPAA doesn't regulate them.[55] Even worse, they don't have to be "public": under HIPAA, "a person or entity acting under a grant of authority from, or under a contract with, a public health agency," is a public health authority.[56]

California, for instance, partnered with Verily, a healthcare data subsidiary of Google's parent company Alphabet, to offer screening for COVID testing locations.[57] But it was unclear whether people's privacy would be protected if they used Verily's websites, and it was worrying that people had to have Google accounts before they could fill out the screening survey.[58] San Francisco and Oakland eventually stopped participating in these programs, partly out of concern for privacy.[59]

The federal government seems to be contemplating similar mistakes. This summer, the Department of Health and Human Services (HHS) issued two database notices that allowed for significant sharing of patient data without consent, including to unnamed private companies.[60]

---

[53] "Public health law reform is necessary because existing statutes are outdated, contain multiple layers of regulation, and are inconsistent." Lawrence O. Gostin, *Public Health Law Reform*, American Public Health Law Association (Sept. 2001), https://ajph.aphapublications.org/doi/full/10.2105/AJPH.91.9.1365

[54] HIPAA generally only applies to "covered entities," like doctors and health insurance companies (payors). The status of "public health authority" is important in that HIPAA expressly permits covered entities to disclose protected health information, without authorization, to public health authorities. 45 CFR 164.512(b)).

[55] A public health authority could be a "covered entity" if very specific conditions are met. https://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm ("a public health agency that operates a health clinic, providing essential health-care services and performing covered transactions electronically, is a covered entity").

[56] See 45 CFR 164.501.

[57] Brian Barrett & Louise Matsakis, *Trump Caught Google Off Guard With a Bogus Coronavirus Site Announcement*, Wired (March 13, 2020), https://www.wired.com/story/coronavirus-donald-trump-google-website/.

[58] Gennie Gerbhart, *Verily's COVID-19 Screening Website Leaves Privacy Questions Unanswered*, EFF Deeplinks Blog (Marc 25, 2020), https://www.eff.org/deeplinks/2020/03/verilys-covid-19-screening-website-leaves-privacy-questions-unanswered.

[59] Jenny Gold & Rachana Pradhan, *Two Bay Area Counties Halt COVID-19 Test Program Run by Google Offshoot*, Los Angeles Times (Oct. 26, 2020), https://www.latimes.com/california/story/2020-10-26/verilys-covid-testing-program-halted-in-san-francisco-and-oakland.

[60] Jennifer Lynch, Lee Tien & Adam Schwartz, *Comments of the Electronic Frontier Foundation Regarding System of Records Notices 09-90-2001, 09-90-2002*, Electronic Frontier Foundation (Aug. 17, 2020), https://www.eff.org/document/2020-08-17-eff-comments-re-hhs-regs-re-covid-data.

Unfortunately, HHS has not been transparent about its new systems, including how the privacy of patient data will be protected by any of these companies.[61]

Recommendations:

1. We need a thorough review of what the previous administration actually did, data-privacy-wise, with data collected as part of addressing COVID.
2. We need a thorough review and then reform of both the law and the institutional safeguards that protect the privacy of all individuals during public health emergencies.

[61] Liz Essley Whyte, *New, Secretive Data System Shaping Federal Pandemic Response*, Center for Public Integrity (Sept. 22, 2020), https://publicintegrity.org/health/coronavirus-and-inequality/secretive-data-system-shaping-pandemic-response-hhs-protect/.

6. Competition

As Internet-related markets—including social networks, communications platforms, Internet access providers, and infrastructure operators—grow more concentrated, the information we receive and our ability to communicate about it are in the hands of a dwindling cohort. For example, high speed Internet access is largely controlled by a small group of companies, who seek in turn to leverage their gatekeeper role to charge for access to users—extracting rents from both customers and the companies that wish to communicate with them.

Market concentration has also accelerated the erosion of online privacy. Internet giants like Google, Facebook, and Amazon exploit their scale to deepen the troves of data they amass on Americans' private lives, finding ever more intrusive ways to extract this information. Much of this data is turned to anticompetitive purposes or used to create barriers to entry.

In the past, the churn of innovation put real limits on the lifespan of most tech monopolies. But that cycle has broken down, as Internet-related monopolists have been able to use their dominant positions to acquire or otherwise eliminate competitors (as with companies like Google, Facebook, and Amazon), to constrain independent software developers and extract monopoly rents (as with Apple), and to insulate themselves from competition through regulatory capture (as with the largest broadband providers).

Reform Antitrust Law

U.S. antitrust laws and their enforcement have not kept pace with Internet industries. Courts have struggled to use a pricing-based consumer welfare standard in applying the Sherman and Clayton Acts to services that are free to the consumer. Rulings in antitrust cases are increasingly determined by esoteric economic theories rather than direct evidence of harm to the competitive process. Enforcement agencies, including the Department of Justice and the Federal Trade Commission, have been reticent about intervening in mergers and acquisitions, even when the resulting conglomerates pose serious threats to consumer choice and privacy, and of locking out independent innovation.

The House of Representatives' recent report on antitrust[62] lays out a good foundation of many changes that need to be sought (with the exception of the proposed exemption for news media).

Competitive Compatibility

While necessary, antitrust reform alone is not sufficient to restart the cycle of competition in Internet markets. This Administration should also enact policies that promote interoperability and data portability among high-technology products and services from competing vendors. Interoperability and data portability allow consumers to leave a dominant firm without losing their data or ability to communicate, and they allow innovation from diverse sources to flourish.

[62] MAJORITY STAFF REPORT AND RECOMMENDATIONS OF H. COMM. ON THE JUDICIARY, INVESTIGATION OF COMPETITION IN DIGITAL MARKETS

There are two approaches this Administration should pursue. One is reducing legal barriers to new products and services that seek to interoperate with incumbent platforms. Today's Internet giants misuse laws like the Computer Fraud and Abuse Act, section 1201 of the Digital Millennium Copyright Act, and the licensing of standards-essential patents to stop independent innovation. This Administration should help protect independent, good-faith innovators and entrepreneurs from the abuse of these laws, through revision of these laws, executive orders, merger conditions, consent decrees, procurement guidelines, and other forms of leverage over market conditions.

The other avenue is requiring incumbent platforms with market power to interoperate with good-faith competitors. This can be imposed as a remedy or negotiated settlement in antitrust litigation, or in some cases, as targeted regulation of specific industry sectors. Such policies should be carefully tailored to apply only to large firms with market power, so that they don't act as barriers to entry for new competitors.

Recommendations

1) More exacting reviews of mergers and acquisitions, including vertical and conglomerate mergers where both firms possess large compilations of user data.
2) A new policy that otherwise unlawful mergers will not be approved subject to conditions regarding consumer privacy if the merging firms have a history of breaking public commitments about privacy.
3) A renewed emphasis on investigating and challenging single-firm conduct such as monopolization, attempted monopolization, product tying, and raising rivals' costs.
4) Amend the antitrust laws to better target anticompetitive mergers, acquisitions, and single-firm conduct.
5) Promote interoperability to counteract the network effects of incumbent platforms proven to have market power.
6) Reform Section 1201 of the Copyright Act and the Computer Fraud and Abuse Act to end the anti-competitive litigation Big Tech companies engage in to snuff out competitors.

7. Copyright

For years EFF has fought efforts to amend the copyright laws to promote entrenched industry interests at the expense of innovation and new creativity.

We welcome a fresh perspective that supports balanced copyright law and ensures space for new creators and innovation. We strongly recommend that the incoming administration avoid putting establishment industry players in positions with authority over copyright issues, which would cement established industry preferences. Such approaches have faced substantial grassroots opposition such as the 2012 protests against the Stop Online Piracy Act, with good reason.

Intermediary Liability (DMCA Section 512)

The Internet has democratized information distribution, to the benefit of creators and users alike. That democratization depends, in turn, on the safe harbors Congress created for Internet companies early on, particularly Section 512 of the Digital Millennium Copyright Act (DMCA). In a nutshell, Section 512 shields intermediaries from copyright liability for content their users upload, as long as they promptly take down infringing material that is brought to their attention. In exchange, content holders got a powerful tool to police infringement, known as "notice and takedown": by sending an email or filling out a form, they can excise infringing content. Thousands of companies and organizations, big and small, rely on Section 512 every day, including interactive platforms like video hosting services and social networking sites. This framework is vital to democratic participation online, and the ability of ordinary users to forge communities, access information, and discuss issues of public and private concern.

Section 512 strikes a balance between the interests of service providers, copyright owners, and Internet users—but the system is not perfect. It is too easy for copyright owners (or people pretending to be copyright owners) to have speech taken down, which comes at a high price for free expression and the public interest. The problem of false and abusive takedown notices is widespread and well documented.[63] This February, for example, baseless copyright claims were used to disable streams of a Democratic presidential primary debate.[64]

Section 512 should be amended to better protect ordinary Internet users. But some proposals to change the notice and takedown system would actually exacerbate the problem of abuse. Major media and entertainment companies have argued for a new system that requires Internet companies to assume the responsibility for copyright enforcement and proactively filter user content (also referred to as "notice and stay-down" and/or a "filter mandate"). Any such system would do serious harm to online speech, creativity, and competition. Existing copyright filters, such as Google's Content ID, are notorious for suppressing lawful speech and harming independent artists. This is not a fixable problem but a fundamental conflict between the rigidity

---

[63] Corynne McSherry, *Statement of Corynne McSherry, Ph.D. re. Notice and Takedown Mechanisms: Risks for Freedom of Expression Online*, EFF Documents Page (Sept. 7, 2020), https://www.eff.org/document/notice-and-takedown-mechanisms-risks-freedom-expression-online.

[64] Charlie Hall, *Report: Phony DMCA Claims Nuked Twitch Streams of the Democratic Debate*, Polygon (Feb. 28, 2020), https://www.polygon.com/2020/2/28/21155955/twitch-streamers-banned-democratic-debate-phony-dmca.

of automated filters and the flexible, context-sensitive nature of fair use. Filtering systems also are ruinously expensive; making them mandatory will simply solidify the strength of incumbent tech giants and insulate them from future competition and disruption.[65]

Also troubling are calls for stricter "repeat infringer" policies. Section 512(i) already requires covered entities to adopt a policy for terminating accounts of repeat infringers. Congress left this open-ended, allowing the wide range of covered companies the flexibility to craft policies appropriate to their services. Rightsholders seek changes that would require companies to enforce those policies far too aggressively, e.g., to ban more users based on mere accusations of infringement.[66] In the case of ISPs, that would mean cutting off Internet access entirely for the alleged infringer and anyone who shares their account.[67] This has always been a dangerous idea, and is even worse now, when people are more reliant on the Internet for their work, education, and.

Recommendations

1) Do not mandate copyright filters. Such a mandate would only strengthen Google's dominance in the user generated platform space through YouTube's Content ID.
2) Do not strengthen repeat infringer policy with bans on accessing the Internet. Under no circumstances should an individual be banned from an essential service such as Internet access.
3) In order to deter abuse of the notice and takedown system, revise Section 512(f) to clarify that the 'good faith belief' requirement in § 512(c)(3)(A)(v) encompasses an objective, rather than a subjective standard, *i.e.,* that the sender of a takedown notice must have a reasonable belief that the content targeted is unlawful.

Freedom to Tinker and Right to Repair (DMCA Section 1201)

In 1998, in the name of combating copyright infringement, Congress enacted the disastrous law known as Section 1201[68] of the DMCA. Since then, courts have interpreted the language to not only restrict copyright infringement, but a wide range of important and legitimate activities. The impact of the law has also ballooned as software has been embedded in more and more devices over the past two decades, such as cars, medical devices, appliances, and even children's toys.

---

[65] Paul Sawers, *YouTube: We've Invested $100 million in Content ID and Paid Over $3 billion to rightsholders*, VentureBeat (Nov. 7, 2018), https://venturebeat.com/2018/11/07/youtube-weve-invested-100-million-in-content-id-and-paid-over-3-billion-to-rightsholders.

[66] Mitch Stoltz, *Another Lawsuit Tries to Force an ISP into Being a Copyright Cop*, EFF Deeplinks Blog (Apr. 26, 2017), https://www.eff.org/deeplinks/2017/04/another-lawsuit-tries-force-isp-being-copyright-cop; U.S. Copyright Office, *Section 512 Report* 96–97 (May 2020), https://www.copyright.gov/policy/section512/section-512-full-report.pdf.

[67] Corynne McSherry & Katharine Trendacosta, *Internet Users of All Kinds Should Be Concerned by a New Copyright Office Report*, EFF Deeplinks Blog (June 1, 2020), https://www.eff.org/deeplinks/2020/06/internet-users-all-kinds-should-be-concerned-new-copyright-offices-report.

[68] Section 1201 means that you can be sued or even jailed if you bypass digital locks on copyrighted works—from DVDs to software in your car—even if you are doing so for an otherwise lawful reason, like security testing.

A regime that bars device owners from understanding how devices work enables unprecedented mischief. Without independent review, software more often contains malicious features, either by design or by neglect. It also enables manufacturers to monopolize the aftermarket for repairs and improvements, as evidenced by lawsuits over repair of cars, boats, and medical devices. Section 1201 also impedes free expression by blocking the ability to comment on, critique, and remix existing culture in order to create a vibrant public sphere. Creators must either use lower-quality material, or download an unlicensed copy to make their fair use, instead of buying a copy and circumventing the access controls.

Recognizing the danger of limiting activities that do not infringe on copyright, Congress created a safety valve in the form of a rulemaking process that allows users to seek exemptions. Yet the process, over seen by the Librarian of Congress and the Register of Copyrights, is far from adequate, First, it takes place only every three years, a bad mismatch to the pace of innovation. Second, the process often stifles activities it should be supporting. For example:

1) Confronted with exemptions covering vehicles and devices, the Copyright Office has waded into issues of environmental and medical safety it is ill-equipped to consider, and then delayed implementation of exemptions.
2) The Copyright Office has diverged from the statutory language and insists that the Librarian has total discretion to deny or delay exemptions, even if the law is met.
3) The process does not allow for exemptions to the law's ban on sharing technology that can be used for circumvention. The expectation is that every blind person will crack Adobe's restrictions on their own to enjoy ebooks, because it's unlawful to give them the tool to do it. This is why farmers resort to downloading software from Ukraine to repair their own tractors.

Section 1201 should be repealed. It interferes with legitimate and critical activities and has no demonstrated effect on copyright infringement (which is already against the law). The primary impact of Section 1201 is to interfere with people who are trying to stay on the right side of the law as they exercise their rights to engage with copyrighted works.

Short of full repeal, Congresswoman Lofgren's Unlocking Technology Act would go a long way towards restoring the traditional balance provided by copyright law. It's unfortunate that some courts interpreted Section 1201 so aggressively, but the that interpretation is chilling speech, innovation, and competition across the country.

Statutory Damages

Copyright law currently allows copyright holders who sue for infringement to seek "statutory damages" of at least $200 and as much as $150,000 per work. Statutory damages are determined by a jury, but do not require any evidence of the actual harm (if any) suffered by the copyright holder. Because of this law, potential penalties in civil copyright cases can be shockingly high. A 2006 suit against XM Satellite Radio over the design of a portable receiver with recording functions created a potential liability of $37 *billion*, nearly three times the annual revenue of the entire recording industry at that time.

Statutory damages also vary widely from case to case, even when facts are similar, making it difficult for businesses to predict potential liability. For example, a record label challenging three companies that used its recordings under similar circumstances received $10,000 per work in one case, $30,000 per work in another, and $50,000 per work in a third. The size and unpredictability of statutory damages fuels an industry of abusive infringement lawsuits against individual Internet users and small businesses based on scant or even falsified evidence. The risk of massive statutory penalties coerces innocent people to pay $2,000 to $10,000 in "settlement" of these abusive claims. Indeed the former U.S. Register of Copyrights, Maria Pallante, emphasized the need to fix statutory damages in a 2014 address.

Recommendation: Amend the Copyright Act to limit the availability of statutory damages. Encourage legislation to require parties in copyright litigation to prove actual harm where possible, in order to avoid excessive damage awards that overcompensate plaintiffs.

8. Computer Fraud and Abuse Act

EFF has long advocated in the courts and Congress to end overbroad applications of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030. Passed in 1986 to target serious computer break-ins, the CFAA makes it a crime to "access" a computer connected to the Internet "without authorization," but it does not define this key term or other key terms.

Due to the CFAA's core vagueness, some courts have mistakenly converted the law into a general-purpose tool for criminalizing ordinary behavior on the Internet, including the enforcement of computer use policies such as websites' boilerplate terms of service. The statute has also enabled overzealous prosecutors to go after behavior that doesn't have anything to do with computer break-ins, as in the tragic case of the researcher and activist Aaron Swartz.[69] The CFAA also chills the essential work of independent security researchers who frequently access computers in contravention of use policies to uncover and correct serious vulnerabilities that endanger everyone.

Finally, companies have used the CFAA as an anti-competitive tool to block their competitors from using automated web browsing tools to access publicly available information.[70] This poses a serious threat to fundamental norms of open access that allowed the technology sector to grow in the first place.

Upcoming Supreme Court Ruling and Further Opportunities for Reform

In 2021, the Supreme Court may rule on whether violation of an employer's computer use policy violates the CFAA.[71] Lower courts have found that violating a corporations terms of service could result in a violation of this criminal statute. In briefs to the Court, EFF argues that the statute should be construed to apply only to serious computer break-ins, in keeping with its intended purpose. Even if the Court agrees, however, it is unlikely to resolve all of the problems with the law.

In Congress, there have been both efforts to amend the CFAA. EFF has supported Rep. Zoe Lofgren's "Aaron's Law," H.R. 1918 (114th Cong.), which would begin with common-sense reforms to narrow the CFAA and limit overcriminalization. Meanwhile, we have opposed poorly-taken efforts that would expand CFAA liability in the name of combating various cyberthreats. In general, these bills would duplicate existing criminal laws and pose serious threats to valuable computer security research.

Recommendations

1) Pending the *Van Buren* decision, direct the Department of Justice to make an explicit statement that violating a computer use policy cannot create liability under the CFAA.
2) Pledge to only enforce the CFAA against computer break-ins that result in serious harm.
3) Support legislative efforts to roll back overcriminalization of the CFAA such as Aaron's Law.

---

[69] Peter Eckersley, *Farewell to Aaron Swartz, an Extraordinary Hacker and Activist*, EFF Deeplinks Blog (Jan. 12, 2013), https://www.eff.org/deeplinks/2013/01/farewell-aaron-swartz.

[70] *hiQ Labs, Inc. v. LinkedIn Corp.,* 938 985 (9th Cir. 2019), *cert. filed* (Mar. 12, 2020).

[71] *Van Buren v. United States*, No. 19-783.

9. Patents

EFF seeks to ensure that the patent system serves its constitutionally-mandated purpose of promoting, rather than impeding, innovation and economic growth. As with much of our work, this involves a combination of impact litigation and legislative proposals.

In 2012, EFF launched its Defend Innovation project[72] to address the crisis America faces in its patent system as litigation and intimidation have impeded the very innovation patent law was meant to promote. EFF's recommended changes to patent law come, in part, from an extensive analysis of more than 16,500 public responses to our proposals, as well as the "Saved by Alice" project, where EFF collects stories from small businesses and start-ups that were able to fend off baseless patent lawsuits because of the Supreme Court's *Alice Corp. v. CLS Bank* decision on patent-eligibility.

Low Quality Patents

The purpose of the patent system is to promote innovation and economic growth. In exchange for publicly disclosing a new advance, an inventor gets the right to use it exclusively for a limited period of time to recover investment costs before competing against free-riders. Because these exclusive rights are such a powerful exception to the rule of market competition, they are only to be granted to those who actually develop new and useful inventions.

Unfortunately, the U.S. Patent Office has for decades failed to apply legal patentability requirements correctly and consistently. As a result, there is a staggering number of overbroad, invalid, and ineligible patents. Many of the patents exploited by trolls are low quality patents that should never have been granted in the first place. Addressing patent quality at the Patent Office would go a long way to repairing systemic patent deficiencies.

The Patent Office is overburdened and under-resourced. On average it spends 19 hours on an application and only a fraction of that time investigating prior art to determine if the patent should be rejected on obviousness grounds.[73] As a result, many old and trivial ideas receive a government-issued monopoly to the detriment of actual innovation. This in turn invites litigation from patent trolls. Armed with vague patents that should never have come into existence in the first place, they have cost American businesses of all sizes billions of dollars on an annual basis.

The Patent Office should make patent quality a key metric of the agency's success and prioritize efforts to improve patent quality systematically. Research shows that efforts to improve patent quality will ultimately be cost-saving: one study indicates that the Patent Office would save $123 million.[74] More rigorous and time-intensive patent examination procedures would not only

---

[72] Electronic Frontier Foundation, *Defend Innovation*, https://defendinnovation.org.

[73] Michael D. Frakes & Mellissa F. Wasserman, *Is the Time Allocated to Review Patent Applications Inducing Examiners to Grant Invalid Patents*?: *Evidence from Micro-Level Application Data*, National Bureau of Economic Research Working Paper No. 20337 (July 2014), http://www.nber.org/papers/w20337.

[74] Michael D. Frakes and Melissa F. Wasserman, *Irrational Ignorance at the Patent Office*, 73 Vanderbilt L. Rev. 975, 1007 (May 7, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3284109.

prevent bad patents from issuing, but produce improvements over time in the clarity and quality of granted patents as well.

Patent Trolling

The majority of patent lawsuits, especially in software, are filed by patent trolls, also called non-practicing entities (NPEs) or patent assertion entities (PAEs). These are companies that provide no products or services. Many of these entities have as their "place of business" empty offices with no employees.[75] But patent trolls demand money from other, productive, companies, as well as small business owners.

In 2019, patent trolls were responsible for between 55 and 58 percent of all patent litigation.[76] Those numbers are down only slightly from 2013, when patent assertion companies filed 62 percent of all patent litigation and may have threatened more than 100,000 operating companies in a single year.[77] A full 30 percent of that litigation is directed at e-commerce and software.

Fueled by patent trolling, the volume of patent lawsuits annually has more than doubled over the last ten years.[78] Venture capitalists frequently complain that the risk of patent litigation makes them unwilling to invest in a startup and that patent troll demands have a significant impact on a company. Indeed, patent trolling scared away almost $22 billion in venture capital funding in the five years before the passage of the America Invents Act.[79]

Preliminary data from 2020 shows that patent troll litigation actually increased during the COVID-19 pandemic, compared to a similar period from 2019.[80] One patent troll firm acquired patents from the fraudulent company Theranos and used them to sue operating companies that

---

[75] This American Life, *When Patents Attack!*, https://www.thisamericanlife.org/radio-archives/episode/441/when-patents-attack (Last Access Nov. 19, 2020)

[76] Unified Patents 2019 Patent Dispute Report, https://www.unifiedpatents.com/insights/2019/12/30/q4-2019-patent-dispute-report, finding that NPE litigation constituted 58% of the total patent litigation in 2019. RPX, a competitor to Unified, found that NPE litigation constituted 55% of the total: https://www.rpxcorp.com/wp-content/uploads/sites/6/2020/08/RPX-2019-Patent-Litigation-and-Marketplace-Report-Public-Excerpt.pdf.; Robin Feldman, *Patent Demands and Startup Companies: The View from the Venture Capital Community,* UC Hastings Research Paper NO. 75 (Oct. 28, 2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2346338.

[77] President's Council of Economic Advisers, the National Economic Council, & Office of Science and Technology Policy, *Patent Assertion and U.S. Innovation*, Obama White House Archive (June 2013), https://obamawhitehouse.archives.gov/sites/default/files/docs/patent_report.pdf.

[78] Catherine Tucker, *The Effect of Patent Litigation and Patent Assertion Entities on Entrepreneurial Activity*, MIT (June 22, 2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2457611; Robin Feldman, *Patent Demands and Startup Companies: The View from the Venture Capital Community*, UC Hastings Research Paper NO. 75 (Oct. 28, 2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2346338.

[79] Joe Mullin, *New Study Suggests Patent Trolls Really are Killing Startups*, Ars Technica (June 11, 2014), http://arstechnica.com/tech-policy/2014/06/new-study-suggests-patent-trolls-really-are-killing-startups.

[80] Unified Patents, *The Great Recession Resulted in an Explosion of NPE Assertions*, https://www.unifiedpatents.com/insights/2020/great-recession-explosion-of-npe-assertions (Last Accessed Nov. 19, 2020).

make COVID-19 tests.[81] Another patent troll firm sued a healthcare company that made ventilators.[82] In a health emergency, EFF supports the government taking direct action against patent monopolies that threaten public health.[83]

Inter Partes Review

When Congress passed the America Invents Act in 2011, it created new procedures for challenging patents before the Patent Trial and Appeal Board (PTAB) at the Patent Office. These procedures, particularly inter partes review (IPR) have become valuable tools for weeding out low quality patents.

The real threat to most innovators isn't that they won't be able to get a patent monopoly—it's that they will be overwhelmed by the costs of defending against a low-quality patent. IPR allows inventors to fight back against false patent claims. The cost of filing an IPR, while still significant, is far less than litigating a case in district court. That allows smaller entities to defend themselves against an invalid patent, rather than simply capitulating because of the legal costs of defense.

For example, EFF filed an IPR to challenge a patent asserted against podcasters. To do so, we raised more than $80,000 from more than 1,300 individual donors—people who create podcasts and passionate users. Regular people care about fighting back against bad patents, and IPR proceedings can give them a chance to do so.

Unfortunately, the Patent Office in recent years has taken a number of steps to undermine IPR, threatening its ability to do what Congress intended: provide a cheaper, faster alternative to district court litigation. First, the Office changed its claim construction standard so that patent owners can more easily avoid prior art—and thus, invalidity—in IPR. Then, the Office imposed claim amendment rules that made it easier for patent owners to re-write their claims during IPR. Finally, it authorized so-called "discretionary denials" of IPR petitions based largely on the time, logistics, and gamesmanship of parallel district court litigation.

The PTAB should grant review whenever a petition satisfies the statutory requirements for IPR. If the petition satisfies those requirements, it means there is a reasonable likelihood the patent is invalid. If a patent is invalid, having a trial is a waste of time, money, and effort for the parties as well as the taxpayer-funded court system. From the public's perspective, the status of pending litigation is irrelevant to the public benefits that come from cancellation of an invalid patent through IPR.

---

[81] Nicole Wetsman, *A SoftBank-Owned Company Used Theranos Patents To Sue Over Covid-19 Tests*, The Verge (March 18, 2020), https://www.theverge.com/2020/3/18/21185006/softbank-theranos-coronavirus-covid-lawsuit-patent-testing.

[82] Joe Mullin, *New Low for a Bad Patent: Patent Troll Sues Ventilator Company*, EFF Deeplinks Blog (May 20, 2020), https://www.eff.org/deeplinks/2020/05/new-low-bad-patent-patent-troll-sues-ventilator-company.

[83] Alex Moss and Elliot Harmon, *The Feds Can Stop Patent Trolls from Endangering COVID-19 Testing and Treatment*, EFF Deeplinks Blog (March 25, 2020), https://www.eff.org/deeplinks/2020/03/feds-can-stop-patent-trolls-endangering-covid-19-testing-and-treatment.

PTAB invalidates patent claims at a rate similar to U.S. District Courts, and the European Patent Office.[84] So misleading terms like "patent death squad" can't stand up to a challenge. Rather, PTAB proceedings have been very successful at weeding out the worst patents.

Recommendation: Before imposing any new restrictions on access to IPR, the incoming Administration should study the impact the PTAB's changes already have had, including on the viability of IPR proceedings as an alternative to litigation.

Alice v. CLS Bank

In June 2014, the Supreme Court confirmed that applying generic computer technology to an otherwise abstract idea does not make that abstract idea eligible for a patent. This prevents patent owners from claiming a monopoly on basic methods of organizing human activity simply by requiring the use of a computer connected to the Internet. When this decision was issued, some proponents of a broken patent system predicted that it would "decimate" the software industry. In fact, the industry continues to grow and thrive. In the two years after *Alice*, the software industry's impact on GDP increased by 18.7%, and on jobs increased by 6.5%.[85] Furthermore, hundreds of bad patent cases have been thrown out, including cases EFF has been involved in defending.[86]

If it wasn't for *Alice*, these patents would have been used to extract unjustified settlements from businesses—many of them small ones. Our "Saved by *Alice*" project highlights small businesses that have managed to defeat wrongly granted patents.

While *Alice* was a step forward, the Patent Office under the Trump Administration has taken steps backward with drastic revisions to the patent-eligibility guidance it gives to examiners for use when reviewing patent applications.[87] This makes it more difficult—if not impossible—for examiners to apply *Alice* correctly.[88] This will lead to more invalid patents.

Recommendation: The Administration should resist any and all efforts to overturn *Alice*, so that the software industry, and startups, can thrive.

---

[84] Josh Landau, *A Little More Than Forty Percent: Outcomes at the PTAB, District Court, and EPO*, Patent Progress Blog (May 1, 2018), https://www.patentprogress.org/2018/05/01/a-little-more-than-forty-percent/.

[85] Conner Forrest, *Software Industry Boosts US GDP by $1.14 Trillion, Grows Economy in All 50 States*, Tech Republic (Sept. 27, 2017), https://www.techrepublic.com/article/software-industry-boosts-us-gdp-by-1-14-trillion-grows-economy-in-all-50-states/

[86] Daniel Nazer, *Happy Birthday Alice: Two Years Busting Bad Software Patents*, EFF Deeplinks Blog (June 20, 2016), https://www.eff.org/deeplinks/2016/06/happy-birthday-alice-two-years-busting-bad-software-patents.

[87] Daniel Nazer, *EFF Comments Regarding 2019 Revised Patent Subject Matter Eligibility Guidance, Docket NO. PTO-P-2018-0053*, EFF Documents Page (March 8, 2019), https://www.eff.org/document/eff-comments-patent-offices-2019-subject-matter-eligibility-guidance.

[88] Alex Moss, *The Patent Office Is "Adjusting" to a Supreme Court Ruling by Ignoring It,* EFF Deeplinks Blog (May 7, 2020) https://www.eff.org/deeplinks/2020/05/patent-office-adjusting-supreme-court-ruling-ignoring-it.

More Patents Do Not Result in More Software Innovation

Software is a uniquely bad fit for patent protection: it is often faster and cheaper to write software code, and thus create a product, than get a patent. Because the cost of development can be so low and the ability to reach users is so great (largely because of the Internet and other networking advances), there is no reason to assume that exclusive rights lasting twenty years are necessary to ensure innovation in this field.

We must not make policy on the assumption that more software patents will lead to more software innovation. Rather, Congress must study the impact that patents have on software innovation, development, and industry growth, and are likely to have in the coming years as the costs of computer technology continue to fall and the potential applications expand.

For example, Congress should study whether government-conferred monopolies, rather than other incentive systems, such as prizes, grants, and tax subsidies, are the most effective means of promoting continued growth and innovation in the software industry and ICT sector as a whole. Such research is particularly important given that non-US entities receive more than half of the utility patents the Office grants each year.[89] Yet the record of continued growth and advancement in the software industry since Alice demonstrates that these patent-eligibility standards are working.

The government can and should gather and release more data about how patent assertions affect the economy. For instance, the Federal Trade Commission (FTC) conducted a 2016 study on patent assertion entities.[90] The study looked at 22 patent assertion entities, which filed 2,452 lawsuits over a six-year period, but did not reveal the names of the PAEs in question. The FTC could conduct additional studies of PAE activity, but also release data on specific PAEs and the specific patent assertions they make.

Recommendations

1. The Patent Office should take steps to improve the quality of granted patents and reduce the number of invalid patents, including giving examiners more time and resources to review pending applications.
2. The Patent Office should adopt practices and procedures that ensure IPR remains an efficient and effective alternative to district court litigation for disputes of patent validity.
3. The Patent Office should provide guidance on patent-eligibility that is consistent with the Supreme Court's *Alice v. CLS Bank* decision and ensure examiners are not granting software patents that would be ineligible under *Alice*.
4. Before changing patent-eligibility standards, the Administration should study the impact of patent protection to determine whether lowering standards for those seeking twenty-year monopolies would promote or impede innovation and growth in the U.S. software industry.

---

[89] U.S. PATENT & TRADEMARK OFFICE, https://www.uspto.gov/web/offices/ac/ido/oeip/taf/us_stat.htm (last visited Sept. 25, 2020).

[90] Federal Trade Commission, *Patent Assertion Entity Activity: An FTC Study*, https://www.ftc.gov/system/files/documents/reports/patent-assertion-entity-activity-ftc-study/p131203_patent_assertion_entity_activity_an_ftc_study_0.pdf (Last Accessed Nov. 19, 2020).

5. To enhance transparency, require patent owners to submit patent assignment agreements along with recordation at the Patent Office.
6. Allow technology users and consumers to stay suits during parallel litigation against upstream suppliers.
7. Make fee-shifting against plaintiffs automatic for objectively baseless patent lawsuits.
8. Make methods of organizing human activity ineligible for patent protection.