Transition Memo 2025

Memo from the Electronic Frontier Foundation to Congress and the Trump Administration to Ensure That Technology Supports Freedom, Justice, and Innovation for All Americans

ELECTRONIC FRONTIER FOUNDATION

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. We hope to work with you on a wide range of policies that affect digital rights in the coming years.

If you have any questions or wish to discuss any of these topics further, please contact EFF's Director of Federal Affairs India McKinney at india@eff.org or Assistant Director of Federal Affairs Maddie Daly at maddie@eff.org.

Thank you.

CONTENTS

Surveillance 5

Foreign Intelligence Surveillance Act. 6

Section 702 7

Facial Recognition Technology 8

Border Search and Immigration Surveillance 9

Surveillance Tech at the Border and the Virtual Wall 10

Reproductive Justice and Digital Surveillance 12

Encryption and Cybersecurity 15

End-to-End Encryption 15

Client-Side Scanning and Other Recent U.S. Attempts At Encryption Backdoors 16

Government Cybersecurity 17

Consumer Privacy. 20

Consumer Privacy Legislation 20

Private Companies and Facial Recognition/Biometrics 21

Age Verification and Internet "Safety" Proposals 22

Vehicle Data 23

Digital Identity 24

Artificial Intelligence 26

AI and Algorithmic Decision-Making 26

Transparency in AI Use and Development 26

Copyright Concerns in Generative AI Regulation 28

Broadband 30

21st-Century-Ready Access for All Americans 30

Net Neutrality 31

Network Usage Fees 32

Section 230 34

Deepfakes 35

Mandated Content Moderation 36

CSAM, Sex Trafficking and Other Unlawful Content 38

Competition 39

Continue to Reform Antitrust Law and Protect Innovation 39

Interoperability 39

A Forwarding Address 40

End to End for Everything 40

Copyright 42

Bolstering Right to Repair 42

Statutory Damages 42

Copyright Filter Mandates 43

No One Should Own the Law: Copyright in Standards Adopted Into Law 44

Digital Ownership 45

Site Blocking 46

Computer Fraud and Abuse Act 48

Recent Limitations on the CFAA's Scope 48

Further Opportunities for Reform 49

Patents 50

Patent Trolls 50

Defenses Against Bad Patents: *Alice v. CLS Bank* *51*

Defenses Against Bad Patents: Inter Partes Review 52

Increasing Transparency in Patent Ownership 53

Ensuring Fair Venue Distribution in Patent Litigation 54

Conclusion 55

Surveillance

As our technology becomes cheaper and faster, smaller and more wearable, our activities, our location, and even our otherwise private conversations have all become more available to scrutiny at all levels of government. Additionally, private companies collect more and more data—search history, location, purchase history, content of unencrypted conversations, and more—and frequently make that data available to the government, often without being legally required to do so. Law enforcement and the intelligence community continue to insist that such broad collection and access to data do not affect privacy and civil liberties.

Those same entities then fight any limitation on their use of this data, on the theory that the data was "legally collected." This Catch-22 approach results in a system that no longer meets traditional Fourth Amendment requirements. This trend needs to be reversed.[1]

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 individual liberty and privacy are not a referendum on the character of the people who work in law enforcement or the intelligence community. Rather, they are an important statement about the values we hold as Americans—freedom from tyranny also requires freedom from unfettered surveillance of our minds, bodies, and movements, as well as reasonable restrictions on how and when that surveillance can occur.

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 in place strong protections to limit or restrict their use. Many forms of surveillance technology are often used first at the border before expanding to the interior of the country. Unchecked use of such technologies presents risks to the privacy, security, and civil liberties of U.S. persons and non-U.S. persons alike. Additionally, when the government is freely given access to consumer data collected by companies, this sensitive data is now potentially criminal evidence, collected broadly, without cause or a warrant.

The Founding Fathers were clearly more concerned about a powerful government using its resources to surveil and punish whoever they chose to target, than letting actual criminals escape justice. It's past time for Congress and the Trump Administration to return to this healthy skepticism of broad surveillance powers and

institute reasonable limits on use of data and the tools used to collect that data.

Foreign Intelligence Surveillance Act

In 1975, 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 that led to the passage of the Foreign Intelligence Surveillance Act (FISA).[2] [3] Most importantly, and in line with a Supreme Court ruling from 1972, 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.

The original authors of FISA might not have been able to predict how the statute could be eventually used to rubber stamp mass surveillance, but for at least a few years, the legislative reforms in conjunction with the Church Committee report created a climate of accountability and oversight—before it was eventually chipped away.

As technology changed and in response to the 9/11 attacks, the government bypassed and weakened the original statute to enable renewed mass surveillance.

President George W. Bush authorized a broad warrantless wiretapping program and bypassed the Foreign Intelligence Surveillance Court (FISC) in 2001, as well as championing a weakening of FISA with the passage of the PATRIOT Act. Although there were immediate concerns about these changes, it took 15 years and a whistleblower's revelations to obtain even the modest statutory reforms in the USA Freedom Act.[4] [5]

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.[6]

The past five years, in particular, have shown those reforms were insufficient.

Other provisions of FISA remain outdated, incomplete, and ineffectual. For one, 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. The so-called amicus provision—an attempt to introduce an adversarial perspective in proceedings before the FISC—must also 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. Congress and the Trump Administration should strengthen 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.
2. Congress and the Trump Administration should increase transparency around FISC rulings and interpretations, as well as enable accountability through disclosures that would allow people surveilled to know when evidence in criminal cases had been acquired through national security surveillance programs. Such reforms must allow people who have been wrongly surveilled proper access in discovery that would let them seek restitution in court.
3. Congress should 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.

Section 702

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.[7] Section 702 differs from other FISA authorities because the government can pick targets and conduct surveillance without a warrant signed by a judge. Instead, the FISC merely reviews and signs off on the procedure. Even in its most narrow interpretation, Section 702 is used to conduct surveillance on hundreds of thousands of individuals, resulting in the collection of billions of communications—without individualized court review.

In 2023, the government conducted surveillance on over 250,000 targets without a court ever reviewing the basis for any of those targeting decisions.[8] The intelligence community then uses those warrantlessly intercepted communications to search for the specific communications of U.S. persons (a so-called "backdoor search"). In 2023, intelligence agencies did this nearly 4,000 times.[9] As currently operated, Section 702 is unconstitutional and in need of wholesale reform. The authority's two-year reauthorization in early 2024 only made it worse by expanding the circumstances under

which Section 702 data could be used and expanding which service providers are beholden to data requests from the NSA.

Recommendations

1. Congress should not renew Section 702 authorities or, at a minimum, not do so without significant, comprehensive reform.

Facial Recognition Technology

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

This widespread surveillance creates many problems. One major problem is that FRT chills and deters protest in public places. During at least one of the Black-led protests against police violence in the summer of 2020, law enforcement used private cameras to mass surveil protesters.[10] FRT allows law enforcement to identify participants and bystanders and track their movements warrantlessly. Federal agencies have done so, including the U.S. Park Police.[11] Thanks to information and image sharing between state 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 other government-issued identifications, and compare them to suspects, regardless of whether those people have ever been accused of a crime. This subjects millions of U.S. residents to the digital equivalent of a perpetual lineup and the threat of being falsely identified.[12]

Additionally, 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 have ineffective protections against erroneous matches serving as the primary form of subject identification. While on paper, most departments have guidance against FRT being used as a primary source, in practice officers and witnesses are subject to automation-bias. Officers give undue weight to matches the technology produces. Witnesses do the same when presented with a line-up produced by the technology.

This can have disastrous consequences for the people who are arrested due to FRT misidentification and their families. For example, in Detroit, several Black people

have been falsely arrested because of erroneous face recognition identification. A lawsuit against the city of Detroit ended with the city creating a robust regulatory framework and a large settlement—but these regulations do not go far enough to prevent the civil liberties harms inseparable from law enforcement's use of facial recognition technology.[13]

As of Fall 2024, 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. On the federal level, several bills have been introduced to ban or limit the use of FRT.

Recommendations

1. Congress and the Trump Administration should ban government use of facial recognition technology and biometric technology by:

   a. Passing the Face Recognition and Biometric Technology Moratorium Act, which would ban federal law enforcement use of FRT;[14]

   b. Restricting federal funding streams from being allocated toward local and state use of the technology;

   c. Withholding federal funding from law enforcement agencies using FRT for mass surveillance.

Border Search and Immigration Surveillance

In recent years, the U.S. Department of Homeland Security (DHS) 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 the federal government's 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 2023, CBP conducted more than 40,000 device searches, an eight-fold increase since FY 2012.[15] EFF has filed amicus briefs in several federal appellate courts, arguing that the government needs a warrant for border searches of electronic devices because of travelers' privacy interests in the vast amounts of sensitive information contained within their devices. EFF also supports federal legislation requiring the government to seek a warrant for border searches of electronic devices.[16] Rep. Ted Lieu currently has a bill in the House of Representatives seeking that requirement.[17] Previously, Sen. Ron Wyden and Sen.

Rand Paul introduced a bipartisan bill seeking that requirement, which unfortunately failed to advance out of the Senate.[18]

In addition to searches of digital devices, the past several years have seen a marked expansion of government efforts to collect biometrics, including DNA, both at the border and within the interior. In 2020, the Department of Justice implemented a rule requiring DHS to collect DNA samples from all individuals in immigration detention to add to the FBI's Combined DNA Index (CODIS) database.[19] This has resulted in over 1.5 million new DNA profiles being added to the database.[20] A recent report from the Center on Privacy & Technology at Georgetown Law identifies many of the privacy concerns inherent in the program, including its violation of the Fourth Amendment.[21]

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. This requirement affects nearly 14.7 million people annually. This "disclosure requirement" is the subject of ongoing litigation brought by the Knight First Amendment Institute at Columbia University and the Brennan Center for Justice at New York University School of Law.[22] EFF has filed amicus briefs in that case, arguing that the disclosure requirement invades privacy and chills the freedom of speech and association of both visa applicants and those in their social networks, including U.S. persons.[23] In addition to this direct harm, this policy may ultimately lead to other countries following the United States' lead and demanding social media data from U.S. citizens traveling abroad.

Recommendations

1. Congress should pass a bill that requires CBP to obtain a warrant to search travelers' electronic devices at the border, including at airports.
2. The Trump Administration should immediately halt all DNA collection programs based on executive immigration powers and expunge all profiles and samples collected thus far under the program.
3. The Trump Administration should require the U.S. Department of State to end the policy that requires visa applicants to disclose their online social media identifiers.

Surveillance Tech at the Border and the Virtual Wall

CBP has massively expanded its spending of taxpayer dollars on ineffective surveillance technology at the U.S.-Mexico border, despite decades of repeated failures and an absence of evidence that it has a positive effect on border security.[24] This

surveillance technology, which tracks and identifies everything in visual range, is a massive invasion of privacy for communities living in border regions. The Trump Administration and Congress must take bold action against these invasive technologies to prevent wasteful spending, including strengthening oversight, embracing transparency, and implementing new safeguards for civil liberties and human rights.

CBP's public messaging and media give the false impression that surveillance towers primarily monitor spacious, uninhabited areas along the border and only capture images of drug-runners and human-traffickers.

In actuality, EFF has documented scores of cameras placed in populated areas. In Texas, they are found in public parks through Laredo and abutting churches and RV parks in Mission. The towers above residential neighborhoods in Calexico, Calif., and Nogales, Ariz., are capable of spying on law-abiding residents on both sides of the border. Yet, CBP does not apply any different rules for towers placed in remote areas versus urban and suburban areas, nor does the agency take steps to mitigate the impact on the privacy of law-abiding citizens or engage communities in any meaningful way.

Although CBP has been quick to promote its new AI strategy to vendors through various industry events, the agency has devoted few resources to evaluating its impact on the public. CBP's Border Surveillance Systems Privacy Impact Assessment (PIA) was last updated in 2018, prior to the implementation of the Autonomous Surveillance Tower program, which boasts AI technology.[25] CBP's PIA does not mention these new capabilities at all.

In addition, CBP has significantly weakened the singular transparency element that was once in place: the National Environmental Policy Act's requirements for conducting Environmental Impact Assessments. Hundreds of autonomous surveillance towers were installed between 2019 and 2024, causing untold impact; however, CBP did not conduct Environmental Impact Assessments for these towers. In at least one recently discovered case, an Autonomous Surveillance Tower installed near Presidio, Tex. destroyed important cultural remains at a historic site.[26]

Furthermore, from 2021-2023 DHS provided $270 million to state and local governments as part of the FEMA-administered Operation Stonegarden program, which encourages local law enforcement agencies to contribute to border security. However, significant amounts of money have gone to states that have pursued policy counter to, or in direct defiance of, national strategy. These taxpayer dollars are often spent on surveillance technology, primarily driven by tech vendors that see Operation Stonegarden as ripe for exploitation. Companies routinely approach small departments and offer to assist with grant writing in exchange for the agency purchasing their technology, whether they need it or not. As a result, their mobile

surveillance towers can often be seen in mall parking lots along highways.[27] In FY 2023 alone, Texas claimed $37 million in Operation Stonegarden funds with little evidence that technology has impacted border security.[28]

Recommendations

1. Congress and the Trump Administration should conduct a complete audit and reevaluation of the Border Surveillance Systems, including aerostats, surveillance towers, unattended ground sensors, and trail cams.
2. The Trump Administration should implement updates to all Privacy Impact Assessments prior to the implementation of new surveillance programs.
3. Congress and the Trump Administration should end the Operation Stonegarden program, a wasteful and ineffective use of taxpayer funds.

Reproductive Justice and Digital Surveillance

Now that *Roe v. Wade* has been overturned, expansive digital surveillance puts pregnant people, their support networks, and their reproductive healthcare providers at risk. As states pass dangerous new laws applying criminal and civil penalties to abortions, mass data collection threatens every person offering or seeking safe reproductive healthcare. What was often benign data before is now potentially criminal evidence. Since the 2022 *Dobbs* decision, attorneys general in multiple states have advised consumers to use encrypted apps if they are communicating about their right to abortion access.[29]

Location data is of particular concern. Our largely unregulated system of location data collection poses a serious threat to reproductive freedom. Companies and data brokers harvest location information from cell phones and apps and sell access to the highest bidder, including government agencies.[30] Under the current system, law enforcement can acquire this information without ever seeking a warrant.[31]

Congress and the Administration should also ban law enforcement from sending reverse location warrants (also known as “geofence warrants”) to corporate holders of location data. These warrants allow police to seize information about all people present at a particular time and place, such as an abortion clinic.

The exploitation of location data is not the only problem; online chat logs can show if you talked about abortion with someone. Web browsing history can tell police if you searched for the address of a clinic or for information about abortion medication.

EFF has been working with legislators on common-sense privacy legislation to

protect the full range of consumer data that could be weaponized against abortion seekers, facilitators, and providers.

Finally, since abortion restrictions are now determined state-by-state, the sharing of electronic health records (EHRs) across state lines presents a serious matrix of concerns. EHRs are digital transcripts of medical information meant to be easily stored and shared between medical facilities and providers. However, as some academics and privacy advocates have outlined, EHRs can jeopardize the safety of patients when reproductive healthcare data is shared across state lines.[32]

We urge the administration to support confidentiality in the healthcare system and help protect patients and providers by passing the Department of Health and Human Services' proposed updates to the information blocking exceptions, specifically the Protecting Care Access exception (to be codified in 45 CFR 171.206).[33] [34] Under the Protecting Care Access exception, healthcare providers would be able to withhold electronic health information based on a "good faith belief" that exchanging that information could put persons "seeking, obtaining, providing, or facilitating reproductive healthcare" at "risk of being potentially exposed to legal action."[35] This is a crucial supplement to existing protections, significantly as some states increase legal attacks on healthcare workers for providing or facilitating reproductive healthcare.

EFF also supported HHS's final rule amending the HIPAA Privacy Rule, which went into effect on June 25, 2024.[36] The rule prohibits covered entities from using or disclosing reproductive health information to conduct "criminal, civil, or administrative" investigations or to "impose criminal, civil, or administrative liability" on any person for "seeking, obtaining, providing, or facilitating" reproductive healthcare.[37] We call on the administration to protect and defend this HIPAA Privacy Rule amendment from legal challenges.[38]

Recommendations

1. Congress and the Administration should pass privacy legislation requiring corporations to minimize the collection and processing of location data to only what is strictly necessary. The law should include *all* location data, not just sensitive reproductive healthcare data.
2. Congress should pass the Fourth Amendment is Not for Sale Act, prohibiting law enforcement from purchasing location data that would otherwise require a warrant.[39]
3. Congress should pass federal legislation banning the use of geofence warrants.

4. Congress should pass the My Body My Data Act, which would restrict businesses and non-governmental organizations from collecting, using, retaining, or disclosing reproductive health information that isn't essential to providing the service a patient is seeking.[40]
5. The Trump Administration should support passage of HHS's proposed "Protecting Care Access" information-blocking exception.[41]
6. The Trump Administration should protect HHS's HIPAA Privacy Rule To Support Reproductive Health Care Privacy from legal challenges.
7. Congress should pass legislation that gives patients and providers greater control over how sensitive healthcare data is shared across electronic medical record systems.

Encryption and Cybersecurity

The right to have a private conversation is fundamental to all free, democratic societies. In the 21st century, it is vital to protect that right—in the physical world, and in the digital world. But as our digital devices have grown more powerful, our privacy has become vulnerable in new ways—to bad actors, hostile governments, or service providers that want to exploit our data for profit. Encryption is the best technology we have to protect our digital security against these threats.

End-to-End Encryption

It is impossible to have a private conversation online without strong end-to-end encryption.[42] Without it, we can't securely send messages to family members, friends, or co-workers. Encryption is also critical to more complex tasks like verifying authorship and protecting the content of our digital devices if they fall out of our hands.

Congress and state officials have long recognized the importance of strong encryption. In 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."[43] Even the 1994 Communications Assistance for Law Enforcement Act (CALEA), which forced telephone companies to redesign their network architectures to make it easier to wiretap digital calls, preserved the ability to use end-to-end encryption.

Technology providers continue to respond to users' strong demand for privacy-protective products that use strong encryption. Messaging apps, including iMessage, WhatsApp and Signal, have implemented end-to-end encryption for years. In recent years, companies as varied as Meta, Apple, Google, Zoom, and Discord have all dramatically increased user access to end-to-end encryption.[44] [45] [46] [47] [48]

Unfortunately, law enforcement agencies and some lawmakers also continue to put forth proposals that would weaken and undermine encryption. They insist that encryption systems impede law enforcement and endanger the public, arguing that government agencies should have some form of special "backdoor" access to peoples' digital content.

Proponents maintain that these methods of special access do not violate encryption and do not constitute what EFF calls "backdoors" to encryption. But reporting has shown law enforcement officials are able to bypass encryption on phones far more often than previously understood. Upturn, a nonprofit, released a comprehensive

report that demonstrates 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[49] [50]

Recommendations

1. Congress and the Trump Administration should support companies providing robust privacy-protective security to their users, including end-to-end encryption.
2. Congress and the Trump Administration should conduct oversight into how often and under what circumstances law enforcement agencies access the contents of encrypted devices.
3. Congress should not pass legislation or regulation requiring companies to allow "extraordinary access" to law enforcement agencies in any circumstance.

Client-Side Scanning and Other Recent U.S. Attempts At Encryption Backdoors

In recent years, proponents of special access have said their proposals do not break encryption because they do not technically affect the workings of the encryption algorithms. Instead, they propose systems requiring users' own devices to betray them by analyzing messages and reporting their findings to government agencies before the encryption process begins. This process is often known as "client-side scanning," although it has been called by other terms such as "endpoint filtering" or simply "local processing."[51]

When an app or website tells users that messages are "end-to-end encrypted," it makes a specific promise: only the sender and the intended recipient of the message will have the means to read it. Client-side scanning, in all its forms, breaks that promise. It checks peoples' messages against a database of "hashes," or digital fingerprints, of images or videos. Some governments, including the former EU head, have even proposed that client-side scanning could use AI to analyze text messages that suggest criminality.

These systems will not scan only for criminal content. Nor, once built, will they be used only by open and democratic governments. The same system that scans for child abuse images can be and quickly will be, used by governments around the world to read protesters' and dissenters' communications. Even well-intentioned efforts to create scanning systems to catch predators open the door to broader abuses by criminal groups, or state-sponsored hacking by foreign governments.

That's why leading technologists have called client-side scanning proposals a form of "bugs in our pockets."[52]

The most recent U.S. effort is the EARN IT Act (S. 1207), which has been proposed in varying forms since 2020.[53] The original form of EARN IT proposed a government commission dominated by law enforcement that could have banned encryption outright. Later forms of EARN IT—including the bill currently being debated in Congress—allow providers of secure communications services to be sued or prosecuted. EARN IT would allow state attorneys general to regulate the internet as long as the stated purpose for their regulation is to protect kids from online exploitation.

While fighting online child abuse is the excuse for EARN IT's choice to create new punishments for communications providers, the bill's clear purpose is to scan user messages, photos, and files. Bill sponsors have even suggested specific software that could be used to monitor users. The EARN IT bill also explicitly allows the fact that a tech provider has offered encryption to users to constitute evidence against them in court.

Recommendations

1. Congress and the Trump Administration should oppose EARN IT, and any legislation that would weaken and/or undermine encryption, including proposals like client-side scanning or "special access."

Government Cybersecurity

Spyware is the term for a software tool that allows governments to covertly gain full access to the data on computers or mobile devices. It has been used around the world to gather intelligence on foreign adversaries, as well as domestically to spy on activists, political dissidents, and journalists. A recent example is from a Chinese state-sponsored hacking group called "Salt Typhoon," which is behind a recent major breach of at least nine U.S. telecom service providers.

According to reports, the hack took advantage of systems built to give law enforcement and intelligence agencies' access to customer data of internet service providers (ISPs) like Verizon, AT&T, T-Mobile, and Lumen Technologies (formerly CenturyLink).[54] By using spyware to hack into these systems, China secretly received unprecedented access to data related to U.S. government requests to these major telecommunications companies, reportedly allowing it to map the U.S. government targets for data collection and surveillance. It's still unclear how much communication and internet traffic, and related to whom, Salt Typhoon accessed.

The Chinese-backed Salt Typhoon appeared to have used proprietary software for its attacks, but the commercial spyware industry plays a role in many cybersecurity attacks as well. In March 2023, the prior Administration issued Executive Order 14093, "Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security."[55] In part, this order states:

> ***The United States has a fundamental national security and foreign policy interest in countering and preventing the proliferation of commercial spyware that has been or risks being misused for such purposes, in light of the core interests of the United States in protecting United States Government personnel and United States citizens around the world; upholding and advancing democracy; promoting respect for human rights; and defending activists, dissidents, and journalists against threats to their freedom and dignity. To advance these interests and promote responsible use of commercial spyware, the United States must establish robust protections and procedures to ensure that any United States Government use of commercial spyware helps protect its information systems and intelligence and law enforcement activities against significant counterintelligence or security risks; aligns with its core interests in promoting democracy and democratic values around the world; and ensures that the United States Government does not contribute, directly or indirectly, to the proliferation of commercial spyware that has been misused by foreign governments or facilitate such misuse.***

The Trump Administration should uphold and expand on this executive order. It should by no means reverse it; in addition to the significant impact on the freedom and privacy of Americans around the world, reversing this order would further empower companies that sell software to Iran or other adversaries. We should not assume that only those countries with the sophistication to build their own spyware will seek to hack into U.S. systems.

U.S. government agencies should not encourage telecommunications and other companies to build in back doors or other vulnerabilities in order to facilitate their own "lawful access" spying and surveillance. As with Salt Typhoon, those vulnerabilities will create unacceptable access avenues for our adversaries and other nefarious actors.

Additionally, the Cybersecurity and Infrastructure Security Agency (CISA) should be empowered to investigate and take actions to defend critical infrastructure—such as industrial control systems, the telephone system, the power grid, transit systems, flight control systems, and more—against foreign attackers. Regarding the telecommunications system specifically, CISA should be empowered to test and verify the claims of network security that the mobile phone industry has made.

The Trump Administration should empower CISA, or another appropriate agency, to take on the task of improving the cybersecurity defensive posture of all branches of our government and those selling technologies or services to the government. The ongoing ransomware crisis, along with attacks like the Salt Typhoon hack, demonstrate that a simple cyberattack has the potential to grind the wheels of commerce to a halt.

Recommendations

1. The Trump Administration should continue to abide by Executive Order 14093, "Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security."
2. The Trump Administration should expand the protections against spyware by discouraging companies from building "lawful access" back doors into their customers' communications and data.
3. The Trump Administration should strengthen CISA and increase their capacity to defend against critical cyber threats to national security.

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 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 and use it to spy on law-abiding citizens.

Consumer Privacy Legislation

More than 90% of Americans feel that they have no control over their data or their online privacy.[56] Congress and the Trump Administration should give control back to each of us as individual users of technology, instead of letting the companies dictate the rules. Many of the internet's ills have one thing in common: They're based on the business model of widespread corporate surveillance online. We encourage lawmakers to advance privacy first as a solution to these issues, rather than often ill-conceived bills intended to tackle a broad set of digital topics ranging from child safety to artificial intelligence.[57] [58] [59] Dismantling this system of corporate data surveillance would not only be a huge step forward for our digital privacy. It would raise the floor for serious discussions about the internet's future.

What would this comprehensive privacy law look like? We believe it must include these components:[60]

- No online behavioral ads
- Data minimization
- Opt-in consent
- User rights to access, port, correct, and delete information.
- No preemption of state laws
- Strong enforcement with a private right to action
- No pay-for-privacy schemes
- No deceptive design

Strong and comprehensive data privacy laws promote security, privacy and free expression. These laws move us forward in the fight to protect children, support journalism, advance access to health care, foster digital justice, limit foreign government surveillance, and strengthen competition. These are all issues on which lawmakers are actively pushing legislation—both good and bad.[61] [62]

Comprehensive privacy legislation won't fix everything. New businesses will still have to struggle against the deep pockets of their established tech giant competitors. Governments will still have tools to surveil people directly. But with this one big step in favor of privacy, we can take a bite out of many of those problems and foster a more humane, user-friendly technological future for everyone.

Recommendations

1. Congress should pass robust, comprehensive federal consumer data privacy legislation with strong enforcement mechanisms, including a private right of action, and no preemption of state law.

Private Companies and Facial Recognition/Biometrics

Clearview AI, a private company, extracts faceprints from billions of photos without anyone's consent, and sells police departments the service of matching known people with subjects in probe photos. This is a grave menace to biometric privacy and serves as a particularly troubling example of companies placing their profits over our privacy while unduly amplifying the surveillance powers of police agencies.

To ensure that companies like Clearview do not collect consumers' biometric data without their knowledge or permission, Congress and the Administration should include protections against biometric data collection without explicit consent in comprehensive federal consumer data privacy legislation. Companies should be required to get our informed opt-in consent before they collect, use, retain, or share our biometric information, including our face prints. In drafting federal legislation on this point, a great starting point is the Illinois Biometric Information Privacy Act (BIPA). Any law should also apply to companies that attempt to sell personal data to the government.[63]

Recommendations

1. Congress should pass federal privacy legislation addressing biometric collection by private entities, such as the National Biometric Information Privacy Act.[64]

Age Verification and Internet "Safety" Proposals

Everyone has a right to speak and access information online. Lawmakers should remember that protecting kids' online safety doesn't require online surveillance and censorship.

Online age-verification mandates are unconstitutional because they block internet users from content they have a First Amendment right to access, burden their First Amendment right to browse the internet anonymously, and chill data security. Further, privacy-minded individuals are justifiably leery of disclosing intensely personal information to online services. Proposals that seek to limit young people's ability to access social media websites or other online services violate both adults' and minors' First Amendment rights. Despite what some lawmakers believe, the Supreme Court has repeatedly ruled that minors have nearly the same First Amendment rights as adults and has struck down laws that limit minors' access to lawful speech on claims that the speech is harmful to children.[65]

These mandates also carry with them broad, inherent burdens on all internet users' rights to access lawful speech online and expose users' most sensitive personal data to increased security risks. These burdens will not and cannot be remedied by new developments in age-verification technology.[66]

Kids Online Safety Act

The Kids Online Safety Act ("KOSA") is a prominent example of age-verification legislation that raises serious free speech and privacy concerns. In addition to being a dangerous and unconstitutional censorship bill, KOSA is also likely to exacerbate the risks of children being harmed online because it will place barriers on their ability to access lawful speech and key resources about addiction, eating disorders, reproductive health, and other important topics.

KOSA imposes a "duty of care" on online services to ensure that their "design features" do not cause harm to minors. This vague and overbroad provision will cause platforms to over-censor a wide range of valuable and constitutionally protected speech. If they don't, they could be held legally liable for content that public officials believe causes anxiety, depression, "compulsive use," or other alleged harms to minors. Depending on the views of those in power, KOSA opens the door to sweeping censorship all along the political spectrum—from guns and vaccines to LGBTQ+ issues and abortion.

KOSA will also result in online services imposing age-verification systems to prevent minors from having the same access to content as adults. Though the bill does not contain an explicit age-verification mandate, regulated platforms must be able to

identify minor users in order to either filter or restrict their access to content considered harmful under the law. The only way to do that is by requiring all users—both adults and minors—to submit to age verification, thereby risking everyone's privacy and undermining their rights to speak, seek information, and browse the internet anonymously.

Recommendations

1. Congress should avoid passing laws that will not pass constitutional scrutiny. Instead, Congress should pass consumer-focused, comprehensive federal privacy laws that would protect young people without infringing on the First Amendment rights of everyone who uses the internet.
2. The Trump Administration should encourage Congress to pass stronger competition laws that would open the field and force platforms to innovate, offering more user choice for parents and teens.

Vehicle Data

Car companies collect troves of data about our driving behavior, ranging from how often we brake to how rapidly we accelerate.[67] This information is then sold to data brokers and directly to insurance companies, where it's used to guess a driver's risk and then unfairly jack up insurance rates. Some promoters of this surveillance claim it's a way to get discounts on insurance, when in fact, your insurance rates may go up.

In a letter to the Federal Trade Commission (FTC), Senators Ron Wyden and Edward Markey urged the FTC to investigate several car companies caught selling and sharing customer information without drivers' clear consent.[68] Alongside details previously gathered from reporting by *The New York Times*, the letter also showcases exactly how much this data is worth to the car companies selling this information.[69]

Car makers should not sell our driving and location history to data brokers or insurance companies, and they shouldn't make it as hard as they do to figure out what data gets shared and with whom.[70] [71] This tracking is especially dangerous to vulnerable populations such as survivors of domestic abuse.[72]

Recommendations

1. The FTC should investigate this industry further, just as it has recently investigated many other industries that threaten data privacy.[73] [74] [75]
2. Congress should pass comprehensive consumer data privacy legislation with strong data minimization rules and requirements for clear, opt-in consent.[76]

Digital Identity

There's a substantial push for implementing identification (ID) programs such as mobile driver's licenses. However, these systems raise fundamental privacy and equity concerns. While specifications for digital ID often recommend data minimization and privacy protections, these recommendations are not mandatory. But they must be; we cannot base our freedoms on promises.

Governments first should lay out legal protections for any new digital ID system. Identity data is highly sensitive. A key concern is the misuse or indiscriminate sharing of personal data by issuers (who provide you a digital ID) and verifiers (who request your digital ID to identify you) during digital ID transactions.

Any digital ID system must require:

- Data minimization.
- Transparency about creation, use, and retention of data.
- User control over data sharing and scope of digital credentials.
- A right to paper or physical documents over digital ones.
- Adequate and accessible backup for when digital ID fails.

Requiring digital identification also poses significant equity issues. Millions of people in our country do not have government-issued identification. We should not apply identity verification regimes against people who often face barriers to compliance, such as license suspension for unpaid traffic fines, or deny people benefits for not having digital identification.

Additionally, many people lack a smartphone (or an up-to-date smartphone) or may share a smartphone with their family. Many proponents of "digital first" solutions assume a fixed ratio of one smartphone for each person. While this assumption may work for some, others will need humans to talk to on the phone or face-to-face to access vital services.

Recommendations

1. Congress should pass a comprehensive data privacy law that gives individuals control and consent over how their identity information is shared and processed.
2. Congress should pass a law explicitly prohibiting law enforcement from using consent for mDL scans to conduct warrantless device searches.

3. Congress and the Trump Administration should direct all federal agencies to implement common-sense data privacy and data security standards in all digital identification program requirements, including offering a right to paper or physical credentials rather than digital ones.

Artificial Intelligence

Artificial intelligence (AI) is riding a wave of hype into adoption in a wide variety of industries and government operations. While current machine learning technologies have some positive applications, they are also being adopted in consequential decision-making contexts in which these emerging technologies are likely to cause harm and unlikely to deliver the promised benefits.

AI and Algorithmic Decision-Making

The use of algorithmic decision-making tools (ADMs) by government agencies in adjudicating people's rights and privileges is of particular concern. Governments increasingly rely on algorithmic systems to make consequential assessments and determinations about people's lives, from judging eligibility for social assistance to automated and so-called "AI-enhanced" surveillance at the U.S.- Mexico border.

AI tools have been shown to be deficient when used in these sorts of complex contexts. At best, this technology can reproduce the patterns present in a training data set. At worst, it can—and often does—fail in troubling and unpredictable ways. When used to inform decisions that implicate the rights of Americans, AI reproduces historic bias by design and presents a high risk of causing new harm. Human rights violations cannot be justified by promises of mere cost savings—promises which are failing to manifest in the private sector, as workers find themselves putting in *more* labor to correct inaccuracies created by machine learning systems.

There are huge risks to using machine learning technology for criminal investigation or punishment or in determining eligibility for housing, medical care, employment, or other essential human needs. Government and private use of these systems must be regulated carefully to avoid infringements upon the civil rights of persons subject to their decisions.

Transparency in AI Use and Development

Across the federal government, AI procurement has moved with remarkable speed. This has led to an alarming lack of transparency in government use of AI that has entrenched the largest AI companies. Without a transparent process, there is a much greater risk of wasteful spending as federal resources are poured into systems with no proven track record.[77]

Two practices can help mitigate this risk.

The first is implementing a robust public notice-and-comment practice consistent with the Administrative Procedure Act, which requires public notice and comment for many types of agency action. Just as an agency would have to give notice and invite comment in order to change rules for deciding eligibility or action, it should be required to do so when adopting an AI or ADM tool that informs such a decision. A public and transparent notice-and-comment process will help reduce harm to the public and government waste by working to weed out bogus products and identify applications where certain types of tools, such as AI, are inappropriate.

The second is favoring technologies developed in accordance with the widely-held transparency principles of free and open-source software. By using technology that is developed transparently and subject to adversarial review, we can ensure that the supposedly scientific basis of many ADM tools holds up to scrutiny. Abiding by core transparency principles will also enable agencies and the public to have more informed conversations about the merits and drawbacks of particular AI systems. Transparency is key because state legislatures around the country, as well as Congress, have begun to grapple with questions of fairness and legal compliance when secret AI and ADM systems are used.

It's important to note that although there is a clear need to regulate AI, lawmakers should not rush to adopt a regulatory framework that would consolidate the industry by locking out small innovators. Regulating general-purpose tools too aggressively would both punish innocent actors and favor the large, incumbent companies that can afford legal battles, while pushing out academic and startup innovators. Focusing on speculative, long-term, catastrophic outcomes from AI (like machines going rogue and taking over the world) pulls attention away from the AI-enabled harms that are directly before us.[78] Accordingly, while those who misuse AI tools should be subject to appropriate legal constraints, any transparency framework should not unduly burden the ability of technologists, particularly small innovators, to develop general purpose AI tools just as they develop other general purpose tools that may be used for both malicious and beneficial purposes. Regulators should focus on *the use* in question, not the tool itself.

Recommendations

1. Congress and the Trump Administration should aid transparency efforts in AI development and use whenever possible.

Copyright Concerns in Generative AI Regulation

Anxiety about generative AI is growing almost as fast as the use of the technology itself. Artists are increasingly concerned about the harms of AI tools used to mimic their respective styles. In addition to the now-infamous AI-generated song that seemed to feature Drake and The Weeknd, digital artists, musicians, actors, writers, and others are seeing their names regularly invoked, without their permission, to generate new works.[79]

Despite the flurry of lawsuits, most new works that are created using generative AI, and the training of the tool itself probably do not infringe the copyright in any work used to train that AI tool.[80] [81]

That said, there are legitimate concerns that may require some rules of the road. As they consider drafting such rules, policymakers should answer some crucial questions:

- **Is the proposed legislation properly focused?** Generative AI is a category of general-purpose tools with many valuable uses; legislators should avoid technology mandates that might inhibit the development of those tools, particularly by smaller innovators that seek to compete with entrenched oligopolies.
- **Are the harms the proposal aims to alleviate documented or still speculative?** Thoughtful researchers and civil society groups have been sounding the alarm about the risks of AI-based decision-making for years. We should not let hyperbole and headlines about the *future* of generative AI distract us from addressing the damage being done by other forms of AI *today*.
- **Is the proposed regulation flexible enough to adapt to a rapidly evolving technology?** Technology often changes much faster than the law, and those changes can be difficult to predict, let alone accurately legislate around.
- **Will the law alleviate the harm it targets?** This question gets overlooked far too often. For example, there have been several proposals to require generative AI users and developers to "watermark" the works they produce. Watermarking of AI generated content is an easy-sounding fix, but research into adversarial watermarking for AI is just beginning, and there's no strong evidence to show that it will fix the thorny problem of disinformation.
- **Finally, how does it affect other public interests?** For example, proposals designed to ensure remuneration for creators, such as a new copyright licensing regime, could make socially valuable research based on machine learning and data mining prohibitively complicated and expensive. EFF has great sympathy for creators who struggle to be appropriately compensated for their work. But we must look for ways to ensure fair pay that don't limit the

potential for all of humanity to benefit from valuable secondary uses.

Recommendations

1. Congress should oppose overly broad bills, such as the NO FAKES and NO AI Fraud, that do not offer satisfactory answers to these questions.

Broadband

21st-Century-Ready Access for All Americans

To remain globally competitive, the United States must close the digital divide. Congress recognized this when it passed the Infrastructure Investment and Jobs Act (IIJA) in 2021, providing more than $42 billion to construct broadband networks that would provide 21st-century-ready-broadband access to all Americans. The Trump Administration should support the National Telecommunications and Information Administration's (NTIA) Broadband Equity Access and Deployment (BEAD) program in disbursing these monies, with an eye toward building fiber networks throughout the United States.

Nearly 80% of Americans consider internet access as essential as water and electricity. As work, business, health services, education, entertainment, and our social lives increasingly have an online component, we cannot accept a future where the quality of our internet access—and so the quality of our connection to these crucial facets of life—is determined by geographic, socioeconomic, or otherwise divided lines.[82]

The only way to solve this problem and build a proper foundation for 21st-century-ready broadband access for all is through universal fiber-to-the-home (FTTH) networks.[83] Fiber networks are future-proof and the only applicable network infrastructure with the scalability to remain cost-effective for decades to come. Put another way, internet usage has steadily increased for decades and will continue to do so for decades to come.[84] Fiber networks are uniquely suited to handle that increase so building now creates the foundation for future success. While wireless broadband access has a role to play, 5G competition and innovation is dependent on the availability of dense fiber networks capable of handling 5G speeds.[85]

Incumbent local exchange carriers (ILEC) and the cable industry have largely stopped transitioning their networks over to fiber. Where they are building fiber networks, they disproportionately favor the upper half of the median income, at the expense of rural and low-income neighborhoods. Such a deployment of FTTH exacerbates the digital divide and broadens the chasm of speed and cost in the consumer broadband market. Given these practices it comes as no surprise that the United States has some of the slowest and most expensive internet access options among modern economies, while our competitors in the global market continue to advance and march forward with universal fiber plans.[86] [87]

Through its BEAD program, the NTIA has set a course correction in motion. In Louisiana, 95% of their BEAD funds have gone toward building fiber networks.[88] As

states continue to disburse their BEAD funds, small private and local public networks—which have historically been active in deploying FTTH even in the most rural areas with population densities as low as 2.5 people per square mile—will be given capital to expand their pre-existing fiber networks.[89] Fiber networks are the literal foundation of the future. Failing at this juncture will mean falling behind the rest of the world.

Recommendations

1. The Trump Administration and Congress should encourage the NTIA to continue its work disbursing BEAD funds with a goal toward building fiber networks.
2. The Trump Administration should prioritize fiber buildout within state implementation; 5G and wireless technology are dependent on the availability of dense fiber networks.

Net Neutrality

Net neutrality is the idea that 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 protector of innovation, depriving large monopolistic ISPs of the ability to determine winners and losers.

Net neutrality is crucial for consumer protection, especially as internet access becomes more concentrated. A 2016 FCC report found that only 38% of Americans have more than one choice for high-speed broadband.[90] Without choices, most Americans—particularly rural Americans—are at the mercy of their internet providers. Without net neutrality, internet providers can determine what we can see online, and block or slow down access to sites and services. Without checks on this power, ISPs have proven themselves more than willing to do so.[91]

ISPs are already testing their ability to create "network slices," violating net neutrality.[92] [93] Network slicing allows ISPs to segment their capacity into buckets with different characteristics, like speed or quality. These apps or services, chosen by ISPs, are given exclusive reserved fast lanes or cost reductions while the rest of the internet must operate on throttled capacity. While network slicing can be a useful tool for things like remote surgery or vehicle-to-vehicle communication, broadband network slicing should not be used as a loophole to circumvent principles of net neutrality.[94]

Fundamentally, net neutrality ensures that users determine their online experience, not ISPs. It is fundamental to user choice, access to information, and free expression online. ISPs should not get to pick winners and losers and entrenched companies

should not be able to beat competition merely by being able to pay for their services to be faster.

When the Federal Communications Commission (FCC) adopted the Open Internet Order in 2015 to prohibit ISPs from engaging in blocking, throttling, or paid prioritization and thereby protecting a free and open internet, 86% of Americans supported these rules.[95] The FCC repealed these protections in 2017, then rightly reinstated these immensely popular protections in 2024.

Unfortunately the 2024 order was then challenged in court, and the 6th U.S. Circuit Court of Appeals ruled against the FCC. The court's holding misunderstands both the Telecommunications Act and the nature of broadband internet access. However, it does suggest a need to pass clear legislation protecting net neutrality, including requirements that ISPs be transparent about how traffic is managed over their networks in order for anyone to know when there's a problem.

We want the internet to live up to its promise, fostering innovation, creativity, and freedom. We don't want ISPs acting as gatekeepers, making special deals with a few companies and inhibiting new competition, innovation, and expression.

If the FCC and the courts aren't able to protect net neutrality, it's past time for legislators to do it.

Recommendations

1. Congress should pass a law that codifies net neutrality protections.

Network Usage Fees

Network usage fees hurt America's economic competitiveness and capacity for innovation in the tech industry. The idea behind network usage fees is that ISPs suffer because companies that create and/or deliver information and content online, called content and applications providers (CAPs)—think Amazon, Netflix, and Google—are "free-riding" off the ISPs' physical infrastructure networks. This is a complete mischaracterization of the relationship.[96] CAPs have invested almost $900 billion into physical internet infrastructure, which not only saves ISPs billions of dollars annually but also does not substantively increase operating costs for ISPs.[97]

The argument for network usage fees also completely mischaracterizes the growth of the modern internet. The internet as it is today exists because of the following virtuous cycle: 1) consumers and end users request services (data) from CAPs, 2) CAPs, to fulfill increasing consumer demand, make investments to create more content

and higher quality content, which uses more data, and 3) consumers and end users demand increased internet service speeds from ISPs, motivating ISPs to make their own investments into network infrastructure.[98] With greater speeds, consumers can demand more, and so the cycle repeats, driving growth to this day.

Network usage fees break the virtuous cycle that has led to American dominance in the tech industry. The Trump Administration must not entertain this dangerous idea that will destroy this crucial aspect of the American economy.

Recommendations

1. The Federal Communication Commission should not pursue the creation of a network usage fees regime in the United States.

Section 230

Internet users rely on intermediaries—ISPs, web hosting companies, websites, and social media platforms—to connect, engage, and express themselves online. That means we also rely on 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.

Section 230 says that any site that hosts the content of other "speakers"—writing, videos, pictures, code that others write or upload—is not liable for that content, except for some important exceptions for violations of federal criminal law and intellectual property claims.

That means that Section 230 is an essential legal pillar for online expression. It makes only the speaker themself liable for their speech, rather than the intermediaries through which that speech reaches its audiences. This makes it possible for sites and services that host user-generated content to exist, and allows users to share their ideas without first having to create their own individual sites or services. This gives many more people access to the content that others create, and it's why we have flourishing online communities for many niche groups, including sports teams, hobbyists, or support groups, where users can interact with one another without waiting hours or days for a moderator or an algorithm to review every post.

Without Section 230, or even with a weakened Section 230, online platforms would be encouraged to limit their liability by removing or restricting far more user content. Around the world, groups silenced on Facebook and other platforms are often those marginalized in other areas of public life.[99] A weak or non-existent Section 230 would be bad for everyone's opportunity to be heard online.

Section 230 doesn't only allow sites that host speech to exist. It also allows them to exist without putting their thumbs on the scale by censoring legal but controversial or potentially problematic content. And because what is considered "controversial" frequently shifts, and is context- and viewpoint-dependent, it's important that these views are able to be shared. Some of the most significant national conversations of this decade have happened online. Defunding the police may be a controversial topic, but that doesn't mean it should be censored. "Drain the Swamp," "Black Lives Matter," or even "All Lives Matter" may be similarly controversial, but censoring this content would not fix real-world problems.

Online platforms' censorship has been shown to amplify existing imbalances in society. The result has been, more often than not, that platforms are more likely to censor disempowered individuals and communities' voices. Without Section 230, any online

service that did continue to exist would, more than likely, opt for censoring more content—and that would inevitably harm marginalized groups more than already dominant voices.

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.[100]

Recommendations

1. Congress should reject any proposed amendments to Section 230.

Deepfakes

When images, video, or audio are created by computers and feature real people, the result is often called a "deepfake." The term was coined in 2017 by an individual using "deep learning" AI tools to paste celebrity faces into pornographic videos. While the term deepfake is often used by the public and elected officials to describe any edited or altered video or image, individuals have been doctoring photos, splicing new video into historical footage, and altering news stories since long before machine learning existed. Indeed, many techniques commonly labeled as "deepfakes" are routine editing.

In the last few years, the evolution of deep learning into generative AI has made deepfakes easier to create and more realistic. The technology has been used to depict public figures, including elected officials and celebrities, saying things they did not say or doing things they did not do. Additionally, some researchers and members of the intelligence community have collected evidence that foreign intelligence operatives use deepfake photos to create fake social media accounts from which they have attempted to recruit Western sources or influence events.[101] [102] [103]

Concern about deepfakes broadly falls into two categories: false political speech and harassment of individuals by distributing sexualized imagery. It's tempting to legislate both categories simultaneously, but the problems are different, and good legislation will tackle them differently.

Legislation tackling false political speech must accept that the First Amendment protects some false and misleading speech. In particular, it would be a mistake to attach penalties only when videos and images are edited with a computer, or with specific technology, like generative AI. A law that targets only edits made with

generative AI would create an environment of fear for normal, everyday publishing and editing tasks, and would be unlikely to slow down disinformation campaigns.

Harassment with fake sexualized imagery is a more narrowly defined problem, and to the people being harassed it is a much more urgent one. “Nudify” apps and websites are widely available and advertised despite rules against them on many of the biggest platforms. Some of the most public examples of their use involve high schoolers deploying them to humiliate their classmates, with schools and authorities unsure how to stop them. Because the problem can be more narrowly defined, legislation targeting this kind of harassment is more likely to survive the courts.

Deepfakes have gotten more sophisticated, including audio deepfakes of people’s voices created using machine learning. While the harms from these scams are real, imposing intermediary liability for third party content is not guaranteed to stop them. Additionally, such measures are almost certain to sweep up protected speech, creating additional legal challenges.

Recommendations

1. Congress should reject any legislation regarding deepfakes that does not properly define the category.
2. Congress should take a tailored approach to legislating deepfakes, treating harassment with sexualized imagery as a separate problem from disinformation. Disinformation regulation should be agnostic to specific technology used and follow the standard set by existing First Amendment accommodations to false speech.

Mandated Content Moderation

Speech in the United States is not required to have a particular political bent or meet a government definition of neutrality. Section 230 was designed to enable these fundamental freedoms granted by the First Amendment; it has done so for decades and continues to do so today.

In two early cases over Internet speech, courts allowed civil defamation claims against Prodigy, an early online service that moderated content, but not against its competitor Compuserve, which did not.[104] A judge reasoned that since Prodigy deleted some messages for “offensiveness” and “bad taste,” Prodigy was responsible for the posts it didn’t screen. Former Rep. Chris Cox has called this decision “surpassingly stupid” and cites it as his motivation for introducing the law that would later become Section 230.[105]

Internet platforms can and must moderate content because that is what their users expect.

Without content moderation, many websites and apps would be rendered useless by "spam" messages, or hecklers who want to sabotage the site.

Many internet users greatly benefit from moderated platforms. Users can:

- Find or create affinity and niche communities that are dedicated to specific subject matters or viewpoints and exclude others;
- Choose environments that shield them from certain kinds of legal speech, including hateful rhetoric and harassment;
- Choose services that attempt to filter out misinformation by relying on sources the user trusts; and
- Seek platforms that proactively filter out spam content.

This kind of content moderation, which Section 230 is meant to protect, has come under attack. However, the Supreme Court's recent decision in *NetChoice v. Moody* confirms that the First Amendment prohibits the government from mandating that online services adopt neutral content moderation policies. The high court ruled that online services have First Amendment rights to moderate their users' speech, just as newspapers, bookstores, and art galleries do.

Even if Congress were to amend Section 230 to require platforms to be "politically neutral," the First Amendment prohibits Congress from intruding on the services' ability to decide for themselves what user-generated content they will host.[106]

These top-down attempts to control internet content are unconstitutional, violate the First Amendment, and are not in keeping with the free expression valued by most Americans.[107] They are also impractical.

Congress should reject 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.[108] YouTube, Meta, and X (Twitter) should not be tasked with being the arbiters of truth.

Individual humans often cannot differentiate deliberate attempts to misinform from parody or satire; the algorithms used in filtering software are demonstrably even worse. Conditioning Section 230 protections on the truthfulness of the content a platform allows is neither useful nor constitutional.

Recommendations

1. Congress should reject legislative efforts to weaken or roll back Section 230.

CSAM, Sex Trafficking and Other Unlawful Content

Current law provides robust protections for victims of child sexual abuse material (CSAM). 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.[109] This system results in millions of reports being sent to law enforcement each year.[110] If companies willfully fail to report, they may be fined hundreds of thousands of dollars.[111]

Section 230 does not affect these stringent requirements. The statute does not bar prosecutions based on any federal criminal law, nor does it bar claims based on intellectual property law, certain communications privacy laws, or (as recently amended) certain anti-sex trafficking laws.[112] The immunities Section 230 offers are limited to federal civil law, and state criminal and civil law.

Opponents to Section 230 argue that the law should be further amended to strip away the limited immunities that companies and people have regarding third-party content. But these limited immunities should remain, as they protect all Americans' speech rights. We should not weaken Section 230 to give states and civil litigants a green light to hold internet intermediaries criminally and civilly responsible for CSAM on their services that they likely don't 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.

This will create fewer and less diverse avenues for online speech. Congress should instead focus on implementing comprehensive solutions that protect children in their day to day lives, as well as online.[113]

Recommendations

1. Congress should not alter Section 230.

Competition

The revival of antitrust law, at home and abroad, promises to restore the natural life cycle of tech, in which firms that grow topheavy and sluggish are displaced by nimbler new competitors, ending the long doldrums of bullying, privacy-invading giants that have captured our digital lives.

This muscular approach to antitrust enforcement and merger challenges has the dual benefit of directly addressing dangerous conduct and deterring bad conduct throughout the tech sector.

While this sea-change in enforcement priorities and approach has accomplished much already, it's still only a beginning. The best time to address monopolies is before they form, because once a sector is dominated by a single company, it becomes "too big to jail" (and firms that are too big to *jail* are also generally also too big to *care*).

That means that there's plenty of work to be done.

Continue to Reform Antitrust Law and Protect Innovation

As a crucial starting point, we hope the new administration will bring forward strong rules on privacy and interoperability and address abuses of dominance by continuing to reform antitrust law.[114]

Further—despite the concentration in social media, search, and other widely used services—the past few years have also seen the emergence of many promising federated social media services and upstart search engines. These show great potential, but will require careful safeguarding from anticompetitive tactics by the incumbents whose dominance they threaten.[115]

Interoperability

Social media sites, email providers, and other intermediaries benefit from "lock-in," which occurs when a customer becomes dependent on a product or service.[116] In turn, this increases the switching costs of end-users and business customers. Once end users are locked in, business customers are locked in, too. Both are then easy pickings for price-gouging, onerous terms of service, privacy invasions, and the plain risk of being held prisoner in a platform whose absentee owners no longer feel they must invest in fighting fraud, harassment, and other harmful conduct.[117]

Lower switching costs are critical to competition. For incumbent companies, the knowledge that users and business customers could depart at any moment is a source of discipline—they must clean up their acts or cope with a mass exodus. What's more, it's a powerful temptation for new market entrants and their investors, because it provides a viable pathway to entice away business customers and users by offering a superior experience.[118]

A Forwarding Address

One readily administered and easily understood form of interoperability is the "forwarding address." Services like Mastodon and protocols like RSS—which underpins podcasting—allow users to issue directives that notify other users that they have moved, and let them know where they can be found.[119]

This "forwarding address" pattern is crucial, because it means that the only way for an intermediary to retain a user or business customer is to be superior to the alternatives—not by making leaving so painful that users remain stuck on inferior platforms.

A "forwarding address" rule is also relatively easy to administrate. If a user insists that a platform has refused to supply forwarding services for them, and the platform disputes it, a regulator doesn't need to get to the bottom of who's telling the truth. The regulator can simply direct the platform to provide forwarding as dictated by the user, easily verify that it has been done, and move on to the next question.

End to End for Everything

The internet was founded on the "end to end" principle: that the job of a network intermediary is to deliver data from willing senders to willing recipients as quickly and reliably as possible, without regard to the intermediary's own preferences.[120]

Today, the applications that sit atop the end-to-end internet are anything but end-to-end. Search engines and e-commerce platforms preference the results they've been paid the most for over the best matches for a user query. Social media platforms downrank new items from accounts users have subscribed to, filling the void with "recommendations" that the platform has a financial interest in delivering (and charging publishers to "boost" their content in order to get it into their own subscribers' feeds). Email providers condemn messages to your spam folder, even when they come from people you know or newsletters you've subscribed to. Search for a beloved album on a music streaming service and you'll get a "playlist" that has the same title and some of the same tracks, but mixed in with these are tracks from other artists who've paid for inclusion, or who charge a lower royalty rate to the

platform.

These are plainly unfair and deceptive methods of competition. Congress and the Trump administration should put a stop to them, promulgating rules and undertaking enforcement actions that start from a simple premise: if a user asks for a piece of information, the service should deliver that requested information above and more prominently than suggestions, ads, boosted content, recommendations, or other material that might drive profit to the service.

As with a forwarding address policy, an end-to-end policy is highly administrable, because it's easy to test whether a firm is in compliance—simply perform a search for a specific item, or subscribe to a feed, or drag a message out of the spam folder, and observe what happens next.

Both of these policies also have the advantage of being capital-light. It is cheaper and easier to build a search that finds exact matches, or a social service that delivers the things the user has asked for, than it is to make one that uses complex rules to hide the ball from the user. Such a rule would not create a compliance moat that keeps new market entrants out.

Recommendations

1. The DOJ and FTC should vigorously apply the 2023 merger guidelines.
2. The DOJ should implement a policy in which otherwise lawful 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. The DOJ and FTC should place renewed emphasis on investigating and challenging single-firm conduct, such as monopolization, attempted monopolization, product tying, and raising rivals' costs.
4. The FTC should implement end-to-end and "forwarding address" policies that facilitate new market entry, reduce switching costs, and protect platform users from abuses by powerful intermediaries.
5. Congress should reform Section 1201 of the Digital Millennium Copyright Act, and the Computer Fraud and Abuse Act, to end the anti-competitive litigation Big Tech companies engage in to snuff out competitors.

Copyright

Copyright has been used for too long to chip away at the very idea of ownership. EFF urges Congress and the Trump Administration to restore balance to our intellectual property laws and ensure that the internet and digital technologies continue to empower consumers, creators, innovators, and scholars.

Bolstering Right to Repair

If you buy something, you should be able to truly own it— meaning you can learn how it works, repair it, remove unwanted features, or tinker with it to make it work in a new way. Independent repair businesses and owners of everything from tractors to cell phones have been pushing hard to restore their ability to repair their devices using the provider of their choice. This extended battle is due to an unintended consequence of Section 1201, which granted manufacturers a monopoly on the ability to understand the code in their devices, and on the ability to access it. This has posed huge obstacles for diagnosis, maintenance, and repair, to say nothing of cutting off independent innovation.

Many states have tried to mitigate this harm by restricting some anticompetitive activities and by mandating disclosure of necessary repair information. But only the federal government can truly address the core issue created by Section 1201.

Given the harms to competition and innovation, coupled with the lack of any principled rationale for Section 1201's interference, reform is needed to get this pseudo-copyright law out of the way of legitimate repairs.

Recommendations

1. Congress should exempt circumvention performed in the context of repairs from the prohibitions of Section 1201, including explicitly permitting the manufacture and sale of repair tools that circumvent access controls and repair services that involve circumvention.

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.[121] Statutory damages are determined by a jury, but do not require any evidence of the actual harm (if any) suffered by the copyright holder. No-proof damages are an outdated

artifact and a global outlier, as other countries either require rights holders to prove their damages or provide a legal framework that gives predictability to owners and users of creative work.[122]

Because of this law, potential penalties in civil copyright cases can be shockingly high. In 2019, a jury awarded *$1 billion* in statutory damages—nearly 10% of all recorded music revenues in that year—against internet service provider Cox Communications, in a suit by music labels that challenged Cox's responses to infringement by its users.[123]

Statutory damages vary widely from case to case, even when facts are similar, making it difficult for businesses and creative professionals 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.[124] 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.

Recommendations

1. Congress should amend the Copyright Act to limit the availability of statutory damages.
2. Congress should pass legislation to require parties in copyright litigation to prove actual harm, particularly in cases of secondary liability and in cases against individuals and small businesses.

Copyright Filter Mandates

Copyright filters are automated tools that purport to aid in copyright enforcement by scanning content uploaded by users and determining whether or not it infringes on copyright. Copyright filters have two main issues—for one, filters often determine that there is a "match" based on just a few seconds of material. For another, companies often allow the filters to remove content with no human review for context.

This is a huge problem because so much of speech depends on context.[125] For example, a filter may not tell the difference between two different pianists playing the same piece of public-domain music, and flag one as infringing on the other.[126] Those trying to teach music or film theory online similarly find themselves unable to use the best examples for their students because filters will not let them.[127] Filters simply do not know enough about human expression to tell when something is infringing and when it is not.

This has a deleterious effect on online speech and expression. It degrades the quality of people's work by forcing them to try to find workarounds to the filters. Certain critiques are discouraged and suppressed simply because no one can figure out how to make a living doing it with the existing filters. And it gives those who would be criticized a way to silence the criticism before anyone even hears it.[128]

Any law that mandates the use of filtering technology in the name of copyright enforcement will end up censoring speech in a fundamental way. We already see this with the voluntary filters used by online platforms. If they were required by law, censorship would only get worse.

Requiring unproven, unaudited technology to be universally distributed would also create a large risk for online security. If a critical vulnerability is found after software has been approved and widely implemented, companies would have to choose between turning it off and giving up their safe harbor protection—risking massive liability—or leave their users vulnerable. No one wins in that scenario, and users lose the most.

Filter mandates are harmful to free expression, privacy and security. Any proposal that would require filtering—either directly or indirectly —is not fit for purpose and should be rejected.

Recommendations

1. Congress should not mandate copyright filters, explicitly or via "tech-neutral" policies.
2. Congress should not make existing safe harbors against intermediary liability contingent upon using or "accommodating" filters.

No One Should Own the Law: Copyright in Standards Adopted Into Law

We should all have the freedom to read, share, and comment on the laws we must live by.

But a few well-resourced private organizations have made a business of charging money for access to building and safety codes, even when those codes have been incorporated into law.

These organizations convene volunteers to develop model standards, encourage regulators to make those standards into mandatory laws, and then sell copies of those laws to the people (and city and state governments) that must follow and enforce them.

They've claimed it's their copyrighted material. But court after court has said that you can't use copyright in this way—no one "owns" the law.[129] [130] The Pro Codes Act undermines that rule and the public interest, changing the law to state that the standards organizations that write these rules "shall retain" a copyright in it, as long as the rules are made "publicly accessible" online.[131]

That's not nearly good enough. These organizations already have so-called online reading rooms where materials aren't searchable, aren't accessible to print-disabled people, and condition your ability to read mandated codes on agreeing to onerous terms of use, among many other problems.

The Pro Codes Act would trade away our right to truly understand and educate our communities about the law for cramped pseudo-public access to it. Congress must not let well-positioned industry associations abuse copyright to control how you access, use, and share the law.

Recommendations

1. Congress should reject the Pro Codes Act, as it did in the 118th Congress.

Digital Ownership

As the things we buy increasingly exist either in digital form or as devices with software, we also find ourselves subject to onerous licensing agreements and technological restrictions.

When you buy a physical work such as a book or album you can lend it, copy it, resell it, or give it away. This idea, known as "first sale" doctrine, is rooted in the fundamental legal principle that personal property can be freely resold, lent, or given away by its owner. And you should be able to do the same with digital works that you buy.

Unfortunately, courts have limited the first sale doctrine to physical copies of a work—such as a hard copy of a book, a CD, or a print of a photograph—and held that it does not apply to digital copies of those same works, based on irrelevant technological distinctions.

When the owner of a physical work gives, sells, or lends it to another person, no new copy is created, and the original owner loses access to the work because only one person can have it at a time. For technical reasons, transferring a digital file results in the creation of a new copy of the file, even if the original owner deletes it from their device.

By relying on this functionally irrelevant technological distinction, courts have

dramatically shifted the balance between the interests of copyright holders and the public, benefitting rights holders at the public's expense.

Because of this, consumers who click a "Buy" button to purchase digital media often find to their dismay that they have bought nothing but fleeting access to a work. Where the owner of a movie on Blu-Ray disc can sell, trade, donate, or even rent out their copy, one who "buys" the same movie as a digital download is prevented from doing any of these things, and what's more, they risk losing access at any time if the seller ceases its support or goes out of business. Libraries in particular are forced to agree to onerous contracts to be allowed to lend copies of digital media. As more and more media is available only in digital form, libraries are losing the power to make learning accessible to their communities.

Recommendations

1. Congress should amend Section 109 of the Copyright Act to make clear that the first sale doctrine applies to both digital and physical copies.
2. Congress should also clarify that federal law does not override state laws aimed at improving libraries' access to digital media.

Site Blocking

Site blocking—or prohibiting access to internet sites and services via court order—is a deeply flawed approach to copyright enforcement. Previous Congresses and administrations have rejected such site-blocking proposals, and the fundamental problems with this approach have not changed.

These problems include the costs to intermediaries and law-abiding internet users, the near certainty of blocking lawful, protected speech, and the harms of mandating an infrastructure of censorship at the heart of the U.S. internet. These harms far outweigh any possible benefit to rights holders.

Nonetheless, major movie and television studios, among others, continue to call for extraordinary new site-blocking powers: court orders issued upon an accusation of copyright infringement that would conscript potentially hundreds of U.S. and foreign infrastructure providers into helping make the accused sites disappear from the internet.

Copyright holders already have strong legal tools at their disposal to combat online infringement. Courts routinely issue orders to interrupt the hosting or accessing of infringing sites and the processing of payments in order to protect rights holders profits. In fact, despite the economic effects of the COVID-19 pandemic, the U.S.

Copyright Office recently reported that the creative industries' financial recovery has been stronger than predicted.[132]

People in the U.S. and most liberal democracies are accustomed to seeing the internet as neutral infrastructure that largely functions the same way for all its users. Given a link to a website, people in the United States don't expect the link to work for their friends or colleagues located in another city, state, or country, but have it fail to load or be told it's blocked by their government or internet service provider themselves. This direct experience of censorship is one people in countries like China and Russia are used to, and we should be very wary of eroding the infrastructure of a free and open internet.

Recommendations

1. Instead of continuing to pursue the fundamentally flawed approach of site-blocking, policymakers should ensure the vigorous enforcement of antitrust laws against gatekeeping monopolies in technology, media, and entertainment markets, and protect creators' right and ability to organize for fair compensation and labor standards.

Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA), passed in 1986 to target serious computer break-ins, makes it a crime to "access" a computer connected to the Internet "without authorization," or to "exceed authorized access."[133] Problematically, this overbroad language does not define several key terms. Since its enactment, prosecutors and private litigants have frequently tried to use the CFAA as a general-purpose tool for punishing ordinary behavior on the Internet, including enforcing computer use policies such as websites' boilerplate terms of service.

The CFAA also chills the essential work of independent security researchers, who frequently access computers in violation of use policies to uncover and correct serious vulnerabilities that endanger everyone. Further, the CFAA is so broad that private parties use threats of litigation to block outside innovators who want to build apps that add functionality to platforms and also to chill journalists and critics who report activities and vulnerabilities on popular platforms.

Recent Limitations on the CFAA's Scope

In recent years, there has been notable progress in limiting the CFAA's core vagueness, although there is still more to be done. In 2021, the Supreme Court ruled on its first CFAA case, *Van Buren v. United States*, and rejected one aspect of this overbroad interpretation.[134] It held that an employee's mere violation of his employer's computer use policy did not constitute "exceeding authorized access" under the CFAA. The Court adopted what it called a "gates-up-or-down" approach: either a user is authorized to access certain information or they are not, and the statute's prohibition is limited to someone who "accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him." The *Van Buren* decision was bolstered by the Ninth U.S. Circuit Court of Appeals' opinion in *HiQ Labs, Inc. v. LinkedIn Corp.*, which found that accessing a fully public website cannot be "without authorization" under the CFAA because no authorization is required.[135]

Finally, a 2022 guideline issued by the Department of Justice restated the limits from these cases, and directed federal prosecutors to refrain from bringing criminal CFAA charges where they cannot show harm to the public interest, or where the conduct at issue was done "solely" for the purpose "good faith security research."[136]

Further Opportunities for Reform

Despite this progress, the CFAA represents a dangerous tool for selective prosecution and harassment. For example, despite its charging policy, the Department of Justice has still prosecuted journalists reporting on the public interest, and tech companies have attempted to silence critics and researchers using the CFAA.[137] [138]

In Congress, there have been both efforts to expand and restrict the scope of the CFAA. Rep. Zoe Lofgren's "Aaron's Law" would institute common-sense reforms to narrow the CFAA and limit overcriminalization.[139] Other bills include language 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. The Department of Justice should issue an explicit statement that violating a computer use policy cannot create liability under the CFAA.
2. The Trump Administration should amend the DOJ charging policy to only enforce the CFAA against actual computer break-ins—involving the circumvention of effective technological barriers—that result in serious harm.
3. Congress should repeal laws such as Aaron's Law that overcriminalize the CFAA.
4. Congress should investigate the use of the CFAA in the private sector to control access to user data, limit interoperability, and other anti-competitive behaviors.

Patents

The U.S. patent system should fulfill its constitutional mandate: promoting innovation and economic growth. Unfortunately, the patent system today, especially in software and technology, impedes far more innovation than it spurs.

Our recommendations are informed by years of experience engaging with the technology-using public, technical experts, small businesses, and everyday tech users, all of whom share firsthand accounts of how patents have impacted their lives. These recommendations would create a more balanced and focused patent system that would support innovators, and expose bad actors who exploit litigation solely for profit.

Patent Trolls

Most patent disputes in U.S. courts are instigated by "patent trolls." These entities are also referred to as patent-assertion entities (PAEs) or non-practicing entities (NPEs). Generally speaking, these companies produce no products or services, but instead focus exclusively on demanding money from other productive companies. Many patent trolls maintain empty or virtual offices in strategically-chosen venues.[140]

In the first half of 2024, 1,727 patent infringement lawsuits were filed in U.S. federal courts; 925 of those, or 53%, were filed by some type of patent troll.[141] Within the tech sector, patent trolls account for an alarming 88.6% of all patent litigation.[142]

These lawsuits are a massive drain on U.S. businesses, particularly small, internet-based businesses. One comprehensive study estimated that patent trolling costs U.S. businesses $29 billion annually in direct costs, such as legal fees and settlement payouts.[143] When indirect costs are included, the total wealth lost annually due to patent trolls approaches $60 billion.[144]

Patent trolls undermine the constitutional intent of patents. The purpose of granting patents—a 20-year government-enforced monopoly—is to "promote the progress of science and the useful arts."[145] Yet, patent trolls generally do not offer products or services, and their lawsuits do little to advance innovation or progress. Instead, settlements from these suits are divided up among attorneys and litigation funders, with little if any benefit to the original patent inventors.

When examined in court, most patent troll claims are exceptionally weak. A study from 2010, when court rules were generally more favorable to patent troll lawsuits than they are today, found that heavily litigated software patents—often associated

with patent trolls— only won 10.7% of cases.[146] In contrast, patents litigated only once (typically not patent troll cases) won nearly 50% of the time.[147]

At EFF, we frequently hear from small businesses or individuals who are threatened by patent claims over routine internet-based activities. For instance, we've heard from people threatened with patents for running online photo contests, using off-the-shelf package tracking software, creating picture menus, crowd-funding, or a "scavenger hunt" app for kids.[148] These claims are typically baseless, yet the patent trolls that assert them rarely face penalties. The high cost of patent defense allows trolls to use even weak or invalid patents to coerce settlements.

Recommendations

1. Congress should pass legislation protecting downstream users from patent claims over technology they did not make or sell, such as the automatic stay process considered in the 2015 Innovation Act.[149]

Defenses Against Bad Patents: *Alice v. CLS Bank*

Starting in the late 1990s, the U.S. Court of Appeals for the Federal Circuit, which oversees patent appeals in the U.S., largely did away with any limits on what could be patented. The court allowed patents on anything yielding a "useful result," even if that result was simply a number. Over the next 15 years, the U.S. Patent Office issued, and courts enforced, a variety of ridiculous patents, especially in software.

Patent trolling hit unprecedented levels during this period. The most egregious patent trolls deployed new tactics, like sending demand letters to small businesses all over the country for using standard printer features such as e-mail and scanning.[150] In 2014, Congress held hearings on abusive patent demand letters. In the words of then-Rep. Lee Terry, the purpose was to address "instances where bad actors extort money from innocent parties under the pretense of asserting intellectual property rights."[151]

In June 2014, the Supreme Court issued a landmark patent ruling, Alice v. CLS Bank, that finally set limits on the flood of overly broad tech-related patents that had been allowed by the Federal Circuit.[152] Alice held that adding computer language to an abstract idea doesn't make it patentable. The unanimous opinion, written by Chief Justice Roberts, made it clear that U.S. patent law does not permit monopolies on basic methods of organizing human activity simply by adding computer or internet-related claims.

In the 10 years since the Alice decision, U.S. courts have invalidated hundreds of

the most problematic software patents, including patents on basic business or cultural practices like "matchmaking."[153] Courts threw out patents on practices such as upselling (via a computer), crowdfunding (on a website), tracking packages (via email), and many others.[154]

At EFF, we launched the "Saved by Alice" project, which tracks small businesses that have overcome outrageous patent claims thanks to Alice.[155] Since Alice, courts have rejected many software patents at early stages, enabling small companies to operate without facing massive patent defense costs or risking bankruptcy.[156] While Alice has not solved all problems in the patent system, it has prevented many cases from dragging on, forcing defendants into costly and unwarranted settlements.

Patent trolls and a few large patent-holding corporations are pushing to eliminate the Alice precedent. That's the goal of the Patent Eligibility Restoration Act, or PERA, introduced in 2022 and again in 2023, which seeks to overturn Alice, dismantling over a decade of effective case law that has helped judges weed out the worst software patents.[157] PERA would also overturn the Myriad Genetics case, a Supreme Court ruling that sharply limits the patenting of human genes.[158]

PERA, or any legislation dismantling the Alice two-step test, would re-open the floodgates to the worst patent troll behavior. Allowing patents on basic internet functions is a mistake that stifles both innovation and free speech.

Recommendations

1. Congress should oppose efforts to overturn the Alice precedent, such as the Patent Eligibility Restoration Act.
2. Congress should conduct an objective and public study on the impact software patents have on the software industry and small developers.

Defenses Against Bad Patents: 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. Among these, inter partes review (IPR), has become an essential tool for weeding out low quality patents, and restoring balance to a system tilted in favor of patent owners.

The real threat to many innovators is not an inability to secure a patent monopoly—it's the overwhelming costs of defending against low-quality patents. The public at large also benefits when improperly granted patents are removed from the system. IPR offers a streamlined way for patent defendants to fight back against

questionable patent claims.

The cost of filing an IPR, while still significant, is far less than the cost of litigating in district court. This makes it possible for smaller entities to defend themselves against invalid patents, rather than capitulate due to prohibitive legal costs. For example, EFF filed an IPR to challenge a patent asserted against podcasters, raising over $80,000 from more than 1,300 individual donors, including podcast creators and passionate users.

The PTAB has, at times, imposed barriers to filing IPRs, such as restrictions based on technicalities like the timing or existence of a parallel court case.[159] The Trump Administration should ensure that the patent office continues to hear IPR petitions in a timely and fair manner whenever they meet the statutory requirements.

The IPR system, however, faces opposition. Patent trolls and others who profit from patent infringement allegations view IPR as a threat. They have lobbied for changes that would overturn or weaken it, such as the PREVAIL Act (S. 2220), which EFF opposes.[160] [161]

Recommendations

1. The U.S. Patent and Trademark Office Director should preserve and strengthen the IPR system by expanding the PTAB's authority during IPR proceedings to provide greater public benefit. For instance, the PTAB could allow *Alice*-based invalidity arguments based on Section 101 of the patent law. Currently, PTAB only considers prior art arguments, meaning challenges based on earlier technology that would invalidate a patent.

Increasing Transparency in Patent Ownership

Currently, U.S. patent law lacks strong requirements for full transparency in patent ownership. The USPTO allows—but does not mandate—ownership updates. Consequently, patent ownership often remains opaque, complicating litigation and enabling patent trolls to obscure their identities. This lack of transparency creates unfair legal and financial obstacles for defendants who don't even know who is making the infringement allegations against them.

The 2021 Pride in Patent Ownership Act proposed mandatory disclosure of patent ownership, which EFF supported as a first step toward addressing these issues.[162] Unfortunately, the bill was not passed.

Patent trolls routinely conceal ownership and financing, including hiding the identity

of non-U.S. based owners who profit from U.S. patent litigation. In 2022, a Delaware U.S. District Court judge investigated a patent troll called IP Edge and several related shell companies. IP Edge enlisted individuals to be "owners" of these entities in exchange for small percentages of settlement revenues. One individual struggled to explain the patent his own company had litigated. The patent ownership had been transferred from Nokia, the Finnish cell phone giant that was the original inventor, to a French government fund, and eventually to IP Edge.[163]

Cases like these show the need for strict transparency requirements in patent litigation, where PAEs should be required to disclose true ownership and funding sources, to prevent exploitation and uphold the system's integrity.

Recommendations

1. Congress should pass a strengthened version of the Pride in Patent Ownership Act that requires disclosure of patent ownership and USPTO record-keeping for all patent assignments.
2. Federal judges overseeing patent cases should promote transparency through local rules and investigate suspicious patent ownership.

Ensuring Fair Venue Distribution in Patent Litigation

Patent cases are concentrated in plaintiff-friendly districts, especially the Western and Eastern Districts of Texas. Of 3,108 patent litigations filed in 2023, more than 36% were filed in these two districts.[164] The patent cases heard in the Western and Eastern Districts of Texas were more than 87% NPE cases, a much higher ratio than in other common patent venues.[165] This shows that "forum shopping," often driven by NPEs making strategic judge selections, remains prevalent. The problem persists despite the 2017 Supreme Court decision in TC Heartland v. Kraft Foods, which restricts suits to locations where a defendant is incorporated or has a regular place of business.[166]

In November 2021, Senators Thom Tillis and Patrick Leahy sent a letter to U.S. Chief Justice John Roberts expressing concern about the extreme concentration of patent cases in the Western District of Texas.[167] One judge in that venue "openly solicited cases at lawyers' meetings and other venues and urged patent plaintiffs to file their infringement actions in his court," they wrote.[168] "This single judge has also repeatedly ignored binding case law and abused his discretion in denying transfer motions."[169]

Following this letter, an administrative change was made to randomly assign patent cases in the Western District of Texas. While this change has modestly dispersed case filings, concerns about fair judicial practices remain.

Recommendations

1. Congress should continue to monitor forum shopping in patent litigation.

Conclusion

In 2025 and beyond, the Electronic Frontier Foundation will continue to champion user privacy, free expression, and innovation. We look forward to sharing our expertise on these issues and more with the Trump Administration and Congress. As technology rapidly advances, EFF will remain committed to building a better, more humane, and more just digital world.

ENDNOTES

1 Brendan Gilligan and Matthew Guariglia, *The White House is Wrong: Section 702 Needs Drastic Change, EFF Deeplinks Blog (April 4, 2024),* https://www.eff.org/deeplinks/2024/04/white-house-wrong-section-702-needs-drastic-change.

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

3 50 U.S.C. § 1801, et seq.

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 R Street, Demand Progress, Freedom Works & Electronic Frontier Foundation, *Strengthening Congressional Oversight of the Intelligence Community (Sept. 13, 2016),* https://www.eff.org/files/2016/09/13/strengthening_congressional_oversight_of_the_ic_white_paper_sept_2016.pdf.

7 50 U.S.C. § 1881, et seq.

8 Office of the Director of National Intelligence, *Annual Statistical Transparency Report: Regarding the Intelligence Community's Use of National Security Surveillance Clearance CY2023,* https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf (last accessed Jan 2, 2025).

9 *Id.*

10 Dave Maass & Matthew Guariglia, *San Francisco Police Accessed Business District 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.

11 Justin Jouvenal & Spencer S. Hsu, *Facial Recognition Used to Identify Lafayette Square Protestors Accused of Assault, Washington Post (November 2, 2020),* https://www.washingtonpost.com/local/legal-issues/facial-recognition-protests-lafayette-square/2020/11/02/64b03286-ec86-11ea-b4bc-3a2098fc73d4_story.html.

12 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/.

13 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/ (Nov. 19, 2020).

14 S. 681, Facial Recognition and Biometric Technology Moratorium Act of 2023 (118th Congress), https://www.congress.gov/bill/118th-congress/senate-bill/681.

15 U.S. Customs & Border Protection, "Border Searches of Electronics at Ports of Entry FY 2023 Statistics" (July 5, 2024), https://www.cbp.gov/sites/default/files/2024-07/border_search_of_electronic_media_-_fy2023_statistics_final_publication_no_3769-0724.pdf.

16 Border Searches, EFF Issues Page, https://www.eff.org/issues/border-searches.

17 H.R. 9567, Protecting Data at the Border Act (118th Congress), https://www.congress.gov/bill/118th-congress/house-bill/9567

18 S. 2957, Protecting Data at the Border Act (117th Congress), https://www.congress.gov/

bill/117th-congress/senate-bill/2957

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

20 Stevie Glaberson, Emerald Tse, & Emily Tucker, *Raiding the Genome: How the United States government Is Abusing Its Immigration Powers to Amass DNA for Future Policing* at 15, Center on Privacy & Technology at Georgetown Law (2024).

21 *Id.*

22 Knight First Amendment Institute, Case Page Doc Society v. Blinken, https://knightcolumbia.org/cases/doc-society-v-blinken.

23 Sophia Cope and 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.

24 Dave Maass, U.S. *Border Surveillance Towers Have Always Been Broken, EFF Deeplinks Blog (Oct. 21, 2024),* https://www.eff.org/deeplinks/2024/10/us-border-surveillance-towers-have-always-been-broken.

25 U.S. Customs & Border Protection, "Privacy Impact Assessment Update for the Border Surveillance Systems (BSS)," (Aug. 21, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp022-bss-september2018.pdf.

26 Texas Historical Commission, Site visit notes, https://www.documentcloud.org/documents/25239962-loma-alta-site-ast-orr-docs.

27 Teledyne FLIR, *Free Grant Assistance Available,* https://www.flir.com/uis/grant-assistance/?srsltid=AfmBOopSYxDNCmWEJX_Asn4fkGHKCo-AFvwa3MyFXzOllRnEpvSYcjp-.

28 Federal Emergency Management Agency, *Homeland Security Grant Program,* https://web.archive.org/web/20240301224634/https://www.fema.gov/grants/preparedness/homeland-security.

29 Top Prosecutors in CA, NY and DC Are Speaking Up For End-to-End Encryption,

https://www.eff.org/deeplinks/2022/11/top-prosecutors-ca-ny-and-dc-are-speaking-end-end-encryption.

30 Karen Gullo, *Location Data Tracks Abortion Clinic Visits. Here's What to Know, EFF Deeplinks Blog (Mar. 15, 2024),* https://www.eff.org/deeplinks/2024/03/location-data-tracks-abortion-clinic-visits-heres-what-know; Joseph Cox, *Inside the U.S. Government-Bought Tool That Can Track Phones at Abortion Clinics, 404 Media (Oct. 23, 2024),* https://www.404media.co/inside-the-u-s-government-bought-tool-that-can-track-phones-at-abortion-clinics/.

31 Matthew Guariglia, *Fourth Amendment is Not For Sale Act Passed the House, Now it Should Pass the Senate, EFF Deeplinks Blog (Apr. 18, 2024),* https://www.eff.org/deeplinks/2024/04/fourth-amendment-not-sale-act-passed-house-now-it-should-pass-senate.

32 Carleen M. Zubrzycki, *The Abortion Interoperability Trap, Yale Law Journal (October 18, 2022),* https://www.yalelawjournal.org/forum/the-abortion-interoperability-trap

33 Department of Health and Human Services, Proposed Rule on Health Data, Technology, and Interoperability: Patient Engagement, Information Sharing, and Public Health Interoperability, Regulations.gov (August 5, 2024), https://www.regulations.gov/document/HHS-ONC-2024-0010-0001.

34 While the proposed exception is written to be specific to reproductive health information (as defined in the OCR HIPAA Privacy Rule), we believe it should also apply to gender-affirming care, which is also legal in some states but criminalized in others.

35 89 Fed. Reg. 63498, 63804 (Aug. 5, 2024) (to be codified at 45 C.F.R. § 171.206(a)(1)).

36 Department of Health and Human Services, HIPAA Privacy Rule to Support Reproductive Health Care Privacy, Federal Register (April 26, 2024), https://www.federalregister.gov/documents/2024/04/26/2024-08503/hipaa-privacy-rule-to-support-reproductive-health-care-privacy.

37 Id. 45 CFR Parts 160 and 164.

38 Attorney General Ken Paxton Sues Biden Administration Over Illegal Rule that Would Weaken State Law Enforcement and Investigation Authority, Attorney General of Texas Press Release (September 4, 2024), https://www.texasattorneygeneral.gov/news/releases/

attorney-general-ken-paxton-sues-biden-administration-over-illegal-rule-would-weaken-state-law.

39 H.R. 4639, Fourth Amendment is Not For Sale Act (118th Congress), https://www.congress.gov/bill/118th-congress/house-bill/4639.

40 H.R. 3420, My Body, My Data Act (118th Congress), https://www.congress.gov/bill/118th-congress/house-bill/3420.

41 See Supra Note 36.

42 End-to-end encryption describes a form of encrypted messaging in which only the sender and the intended recipient can read the message.

43 House Judiciary 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.

44 Loredana Crisan, *Launching Default End-to-End Encryption on Messenger, Facebook (December 6, 2023),* https://about.fb.com/news/2023/12/default-end-to-end-encryption-on-messenger/.

45 *Apple Advances User Security with Powerful with Powerful New Data Protections, Apple (December 7, 2022),*https://www.apple.com/newsroom/2022/12/apple-advances-user-security-with-powerful-new-data-protections/.

46 Monika Y, *Your RCS Conversations Are Now Fully End-to-End Encrypted, Google (August 3, 2023),* https://support.google.com/messages/thread/229405182/your-rcs-conversations-are-now-fully-end-to-end-encrypted

47 Gennie Gebhart, *Victory: Zoom Will Offer End-to-End Encryption to All its Users, EFF Deeplinks Blog (June 17, 2020),* https://www.eff.org/deeplinks/2020/06/victory-zoom-will-offer-end-end-encryption-all-its-users.

48 Stephen Birarda, *Meet DAVE: Discord's New End-to-End Encryption For Audio & Video, Discord (September 14, 2024),* https://discord.com/blog/meet-dave-e2ee-for-audio-video.

49 Logan Koepke, Emma Weil & Urmila Janardan, *Mass Extraction: The Widespread Power of U.S. Law*

Enforcement to Search Mobile Phones, Upturn (Oct. 20, 2020), https://www.upturn.org/reports/2020/mass-extraction/.

50 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.

51 Erica Portnoy, *Why Client-Side Scanning Breaks Encryption, EFF Deeplinks Blog (November 1, 2019),* https://www.eff.org/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption.

52 Bugs in our Pockets: The Risks of Client-Side Scanning. Journal of Cybersecurity, 10(1), 2024 https://arxiv.org/abs/2110.07450.

53 S. 1207 EARN IT Act (118th Congress), https://www.congress.gov/bill/118th-congress/senate-bill/1207.

54 Sarah Krouse, *U.S. Wiretap Systems Targeted in China-Linked Hack, Wall Street Journal (October 5, 2024),* https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b.

55 *E.O. 14093: Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security, White House Briefing Room (March 27, 2023),* https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/.

56 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/.

57 Jason Kelley, *The Kids Online Safety Act is Still a Huge Danger to Our Rights Online,* EFF Deeplinks Blog (May 2, 2023), https://www.eff.org/deeplinks/2023/05/kids-online-safety-act-still-huge-danger-our-rights-online.

58 Corynne McSherry, *A Broad Federal Publicity Right is a Risky Answer to Generative AI Problems,* EFF Deeplinks Blog (July 18, 2023), https://www.eff.org/deeplinks/2023/07/broad-federal-publicity-right-risky-answer-generative-ai-problems.

59 Corynne McSherry et al., *Privacy First: A Better Way to Address Online Harms,* EFF Deeplinks Blog (November 14, 2023), https://www.eff.org/wp/privacy-first-better-way-address-online-harms#Legislation.

60 Gennie Gebhart, *EFF's Recommendations for Consumer Data Privacy Laws,* EFF Deeplinks Blog (June 17, 2019), https://www.eff.org/deeplinks/2019/06/effs-recommendations-consumer-data-privacy-laws.

61 Jason Kelley and Sophia Cope, *The Protecting Kids on Social Media Act is a Terrible Alternative to KOSA, EFF Deeplinks Blog (August 28, 2023),* https://www.eff.org/deeplinks/2023/08/protecting-kids-social-media-act-terrible-alternative-kosa.

62 Hayley Tsukayama, *Support the "My Body, My Data Act" Act, EFF Deeplinks Blog (May 18, 2023),* https://www.eff.org/deeplinks/2023/05/eff-supports-my-body-my-data.

63 Mario Trujillo, *Americans Deserve More Than the Current American Privacy Rights Act, EFF Deeplinks Blog (April 16, 2024),* https://www.eff.org/deeplinks/2024/04/americans-deserve-more-current-american-privacy-rights-act.

64 S. 4400, National Biometrics Information Privacy Act of 2020 (116th Congress), https://www.congress.gov/bill/116th-congress/senate-bill/4400.

65 Molly Buckley, EFF to Fifth Circuit: Age Verification Laws Will Hurt More Than They Will Help, EFF Deeplinks Blog (Oct. 4, 2024), https://www.eff.org/deeplinks/2024/10/eff-fifth-circuit-age-verification-laws-will-hurt-more-they-help.

66 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.

67 Thorin Klosowski, *How to Figure Out What Your Car Knows About You (And Opt Out of Sharing When You Can), EFF Deeplinks Blog (March 15, 2024),* https://www.eff.org/deeplinks/2024/03/how-figure-out-what-your-car-knows-about-you-and-opt-out-sharing-when-you-can.

68 Offices of Senators Ron Wyden and Edward J. Markey, *Letter to the FTC (July 26, 2024),* https://www.wyden.senate.gov/imo/media/doc/wyden-markey_auto_privacy_letter_to_ftc.pdf.

69 Kashmir Hill, *Automakers Are Sharing Consumers' Driving Behavior With Insurance Companies, New York Times (March 13, 2024),* https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html.

70 See Supra Note 68.

71 Catalina Sanchez, *Car Makers Shouldn't Be Selling Our Driving History to Data Brokers and Insurance Companies, EFF Deeplinks Blog (June 4, 2024),* https://www.eff.org/deeplinks/2024/06/car-makers-shouldnt-be-selling-our-driving-history-data-brokers-and-insurance.

72 Hayley Tsukayama, Eva Galperin, Catalina Sanchez, *Modern Cars Can Be Tracking Nightmares. Abuse Survivors Need Real Solutions., EFF Deeplinks Blog (July 16, 2024),* https://www.eff.org/deeplinks/2024/07/modern-cars-can-be-tracking-nightmares-abuse-survivors-need-real-solutions.

73 Adam Schwartz, *FTC Bars X-Mode from Selling Sensitive Location Data, EFF Deeplinks Blog (January 23, 2024),* https://www.eff.org/deeplinks/2024/01/ftc-bars-x-mode-selling-sensitive-location-data.

74 Hayley Tsukayama, *FTC's Rite Aid Ruling Rightly Renews Scrutiny of Face Recognition, EFF Deeplinks Blog (December 20, 2023),* https://www.eff.org/deeplinks/2023/12/ftcs-rite-aid-ruling-rightly-renews-scrutiny-face-recognition.

75 Matthew Guariglia, *The FTC Forces Ring to Take User Privacy Seriously, EFF Deeplinks Blog (June 13, 2023),* https://www.eff.org/deeplinks/2023/06/ftc-forces-ring-take-user-privacy-seriously.

76 See Supra Note 59.

77 Kit Walsh, *Fighting Automated Oppression: 2024 in Review, EFF Deeplinks Blog (December 30, 2024),* https://www.eff.org/deeplinks/2024/12/fighting-automated-oppression-2024-review-0

78 Rindala Alajaji and Hayley Tsukayama, *Triumphs, Trials, and Tangles from California's 2024 Legislative Session, EFF Deeplinks Blog (October 30, 2024),* https://www.eff.org/deeplinks/2024/10/triumphs-trials-and-tangles-years-california-legislative-session

79 Locke Lord LLP, *Death by a Thousand Cuts: Right of Publicity in the Age of AI, JD Supra (May 31, 2023),* https://www.jdsupra.com/legalnews/death-by-a-thousand-cuts-right-of-8578503/.

80 Zachary Small, *Sarah Silverman Sues Open AI and Meta Over Copyright Infringement, New York Times (July 10, 2023),* https://www.nytimes.com/2023/07/10/arts/sarah-silverman-lawsuit-openai-meta.html?smid=nytcore-android-share.

81 Kit Walsh, *How We Think About Copyright and AI Art, EFF Deeplinks Blog (April 3, 2023),* https://www.eff.org/deeplinks/2023/04/how-we-think-about-copyright-and-ai-art-0.

82 *Broadband in the U.S.: Consumer Reports' New Survey Reveals Challenges for Consumers*, Consumer Reports (August 3, 2021), https://www.consumerreports.org/media-room/press-releases/2021/08/broadband-in-the-us-consumer-reports-new-survey-reveals-challenges-for-consumers/.

83 Bennett Cyphers, *The Case for Fiber to the Home, Today: Why Fiber is a Super Medium for 21st Century Broadband*, EFF Deeplinks Blog (October 16, 2019), https://www.eff.org/wp/case-fiber-home-today-why-fiber-superior-medium-21st-century-broadband.

84 Doug Dawson, *The Future of Broadband*, Pots and Pans (April 12, 2024), https://potsandpansbyccg.com/2024/04/12/the-future-of-broadband/.

85 *Fiber: Inextricably linked with 5G Connectivity*, Wireless Infrastructure Association (August 19, 2020), https://wia.org/fiber-inextricably-linked-with-5g-connectivity/.

86 Becky Chao, Claire Park and Joshua Stager, *The Cost of Connectivity*, The New America Foundation (July 15, 2020), https://www.newamerica.org/oti/reports/cost-connectivity-2020/.

87 Michael Philpott et al, *Global Fiber Development Index: 2020,* OMDIA, https://worldbroadbandassociation.com/wp-content/uploads/2021/08/FDI-White-Paper-Final_151020.pdf.

88 Nicole Ferraro, *Louisiana to Award 95% of BEAD Funds for Fiber*, Light Reading (November 19, 2024), https://www.lightreading.com/broadband/louisiana-to-award-95-of-bead-funds-for-fiber?utm_campaign=Newsletters&utm_medium=email&utm_source=sendgrid&mc_cid=2e4c81f095&mc_eid=41c87332a3.

89 Christopher Mitchell, *United Fiber Tackles Missouri's Most Rural - Community Broadband Bits Podcast 240*, Community Networks (February 14, 2017), https://communitynets.org/content/united-fiber-tackles-missouris-most-rural-community-broadband-bits-podcast-240.

90 2016 Broadband Progress Report, Federal Communications Commission (January 29, 2016), https://www.fcc.gov/document/fcc-releases-2016-broadband-progress-report.

91 Timothy Karr, *Net Neutrality Violations: A History of Abuse*, Free Press (July 9, 2021), https://www.freepress.net/blog/net-neutrality-violations-history-abuse.

92 Mike Dano, *AT&T Test Gaming Traffic Prioritization Amid Net Neutrality Debate*, Light Reading (July 28, 2022), https://www.lightreading.com/oss-bss-cx/at-t-tests-gaming-traffic-prioritization-amid-net-neutrality-debate.

93 Isabelle Bousquete, *Carriers Look to Offer Fast-Lane Access on 5G Networks*, Wall Street Journal (November 3, 2023), https://www.wsj.com/articles/carriers-look-to-offer-fast-lane-access-on-5g-networks-0ab57bcc.

94 Chao Jun Liu and Cooper Quintin, *Internet Service Providers Plan to Subvert Net Neutrality. Don't Let Them, EFF Deeplinks Blog (April 19, 2024),* https://www.eff.org/deeplinks/2024/04/internet-service-providers-plan-subvert-net-neutrality-dont-let-them.

95 *Overwhelming Bipartisan Public Opposition to Repealing Net Neutrality Persists, University of Maryland School of Public Policy (April 28, 2018),* https://publicconsultation.org/united-states/overwhelming-bipartisan-public-opposition-to-repealing-net-neutrality-persists/.

96 Chao Jun Liu, Ernesto Falcon, and Katharine Trendacosta, *Network Usage Fees Will Harm European Consumers and Businesses, EFF Deeplinks Blog (December 6, 2022),* https://www.eff.org/deeplinks/2022/12/network-usage-fees-will-harm-european-consumers-and-businesses.

97 David Abecassis et al., *The Impact of Tech Companies' Network Investment on the Economics of Broadband ISPs, Analysys Mason (October 2022),* https://membership.incompas.org/Files/2022%20Tech%20Investment/FINAL%20Analysys%20Mason%20Report%20-%20Impact%20of%20tech%20companies'%20network%20investment%20on%20the%20economics%20of%20broadband%20ISPs.pdf.

98 Chao Jun Liu and Ernesto Falcon, *There is Nothing Fair About the European Commission's "Fair Share" Proposal, EFF Deeplinks Blog (June 16, 2023),* https://www.eff.org/deeplinks/2023/06/there-nothing-fair-about-european-commissions-fair-share-proposal.

99 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.

100 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.

101 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.

102 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.

103 Dan Merica, *Sophistication of AI-backed Operation Targeting Senator Points ot Future of Deepfake Schemes*, Associated Press (September 26, 2024), https://apnews.com/article/deepfake-cardin-ai-artificial-intelligence-879a6c2ca816c71d9af52a101dedb7ff.

104 *Section 230: Legislative History, EFF Issue Page,* https://www.eff.org/issues/cda230/legislative-history

105 Corbin Barthold, *Section 230 Heads to the Supreme Court, Reason (November 4, 2022),* https://reason.com/2022/11/04/section-230-heads-to-the-supreme-court/

106 *See Supra Note 98.*

107 David Greene*, In These Five Social Media Cases, Supreme Court Set Foundational Rules for the Future, EFF Deeplinks Blog (Aug. 14, 2024),* https://www.eff.org/deeplinks/2024/08/through-line-suprme-courts-social-media-cases-same-first-amendment-rules-apply.

108 *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")*

109 18 U.S.C. § 2258A.

110 35.9 million reports of suspected CSAM were made to the CyberTipline in 2023. National Center for Missing and Exploited Children, *CyberTipline 2023 Report,* https://www.missingkids.org/CyberTiplinedata.

111 18 U.S.C. § 2258A(e).

112 47 U.S.C. § 230(e).

113 Prevent Child Abuse America, *Child Sexual Abuse Prevention*, https://preventchildabuse.org/what-we-do/child-sexual-abuse-prevention/.

114 Bennett Cyphers and Cory Doctorow, "Privacy Without Monopoly," EFF White Paper https://www.eff.org/document/privacy-without-monopoly-data-protection-and-interoperability.

115 Cindy Cohn and Rory Mir, "The Fediverse Could Be Awesome If We Don't Screw it Up," EFF Deeplinks Blog, https://www.eff.org/deeplinks/2022/11/fediverse-could-be-awesome-if-we-dont-screw-it; Rory Mir, "What You Should Know When Joining Bluesky," EFF Deeplinks Blog, https://www.eff.org/deeplinks/2024/12/what-you-should-know-when-joining-bluesky.

116 Rory Mir, "Crowdstrike, Antitrust, and the Digital Monoculture," EFF Deeplinks Blog, https://www.eff.org/deeplinks/2024/07/crowdstrike-antitrust-and-digital-monoculture.

117 Cory Doctorow, "As Platforms Decay, Let's Put Users First," EFF Deeplinks Blog, https://www.eff.org/deeplinks/2023/04/platforms-decay-lets-put-users-first.

118 "How to Ditch Facebook Without Losing Your Friends (Or Family Or Customers Or Communities)," EFF Video, https://www.eff.org/deeplinks/2022/09/how-ditch-facebook-without-losing-your-friends-or-family-customers-or-communities.

119 Zander Arnao, *Cory Doctorow on Why Interoperability Would Boost Digital Competition, Chicago Policy Review (April 12, 2023),* https://chicagopolicyreview.org/2023/04/12/cory-doctorow-on-why-interoperability-would-boost-digital-competition/.

120 Cory Doctorow, *To Save the News, We Need an End-to-End Web,* EFF Deeplinks Blog (June 12, 2023),

https://www.eff.org/deeplinks/2023/06/save-news-we-need-end-end-web.

121 17 U.S.C. § 504(c).

122 Pamela Samuelson, Phil Hill, and Tara Wheatland, Statutory Damages: A Rarity in Copyright Laws Internationally, But for How Long? (2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2240569.

123 Blake Brittan, Major Labels Ask US Supreme Court to Reconsider $1 bln Cox Copyright Case, Reuters (August 21, 2024), https://www.reuters.com/legal/litigation/major-labels-ask-us-supreme-court-reconsider-1-bln-cox-copyright-case-2024-08-21/.

124 Pamela Samuelson and Tara Wheatland, "Statutory Damages in Copyright Law: A Remedy in Need of Reform," William & Mary Law Review, Vol. 51, p. 439, 2009, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1375604.

125 Katharine Trendacosta, *Unfiltered: How YouTube's Content ID Discourages Fair Use and Dictates What We See Online, EFF Deeplinks Blog (December 10, 2020),* https://www.eff.org/wp/unfiltered-how-youtubes-content-id-discourages-fair-use-and-dictates-what-we-see-online

126 Micheal Andor Brodeur, Copyright Bots and Classical Musicians Are Fighting Online. The Bots Are Winning. Washington Post (May 21, 2020), https://www.washingtonpost.com/entertainment/music/copyright-bots-and-classical-musicians-are-fighting-online-the-bots-are-winning/2020/05/20/?arc404=true

127 Beato, Rick. Testimony to the Subcommittee on Intellectual Property Hearing Entitled "How Does the DMCA Contemplate Limitations and Exceptions like Fair Use?" 28 July 2020. https://www.judiciary.senate.gov/imo/media/doc/Beato%20Testimony.pdf

128 See Supra Note 115.

129 Joe Mullin, *Appeals Court Tells Georgia: State Code Can't be Copyrighted, EFF Deeplinks Blog (October 23, 2018),* https://www.eff.org/deeplinks/2018/10/appeals-court-tells-georgia-state-code-cant-be-copyrighted.

130 Corynne McSherry and Mitch Stoltz, *Supreme Court Affirms That No One Owns the Law, EFF Deeplinks Blog (April 27, 2020),* https://www.eff.org/deeplinks/2020/04/supreme-court-affirms-no-one-owns-law.

131 Corynne McSherry, *Access to Law Should Be Fully Open: Tell Congress Not to Be Fooled by the PRO Code Act, EFF Deeplinks Blog (October 25, 2023),* https://www.eff.org/deeplinks/2023/10/access-law-should-be-fully-open-tell-congress-not-be-fooled-pro-codes-act.

132 U.S. Copyright Office, The Resilience of Creativity (2024), https://copyright.gov/economic-research/resilience-of-creativity/.

133 18 U.S.C. § 1030

134 Van Buren v United States, EFF Case Page, https://www.eff.org/cases/van-buren-v-united-states.

135 hiQ v Linkedin, EFF Case Page, https://www.eff.org/cases/hiq-v-linkedin.

136 Andrew Crocker, DOJ's New CFAA Policy is a Good Start But Does Not Go Far Enough to Protect Security Researcher's, EFF Deeplinks Blog (May 19, 2022), https://www.eff.org/deeplinks/2022/05/dojs-new-cfaa-policy-good-start-does-not-go-far-enough-protect-security.

137 Andrew Crocker, *Is the Justice Department Even Following Its Own Policy in Cybercrime Prosecution of a Journalist?, EFF Deeplinks Blog (February 22, 2024),* https://www.eff.org/deeplinks/2024/02/justice-department-even-following-its-own-policy-cybercrime-prosecution-journalist.

138 Aaron Mackey, *Federal Court Dismisses X's Anti-Speech Lawsuit Against Watchdog, EFF Deeplinks Blog (April 5, 2024),* https://www.eff.org/deeplinks/2024/04/federal-court-dimisses-xs-anti-speech-lawsuit-against-watchdog.

139 H.R. 1918, "Aaron's Law" (114th Congress), https://www.congress.gov/bill/114th-congress/house-bill/1918

140 "*When Patents Attack*," National Public Radio (July 22, 2011), https://www.thisamericanlife.org/441/when-patents-attack.

141 Unified Patents, 2024 Patent Dispute Report: 2024 Mid-Year Report, Figure 2 (July 22, 2024), https://www.unifiedpatents.com/insights/2024/7/22/patent-dispute-report-2024-mid-year-report.

142 Unified Patents, Patent Dispute Report: 2023 in Review, Figure 11 (January 8, 2024), https://www.unifiedpatents.com/insights/2024/1/8/patent-dispute-report-2023-in-review.

143 James Bessen, *The Evidence is In: Patent Trolls Do Hurt Innovation, Harvard Business Review (July 2014),* https://hbr.org/2014/07/the-evidence-is-in-patent-trolls-do-hurt-innovation.

144 *Id.*

145 Article I, Section 8, Clause 8 of the United States Constitution.

146 Allison, John R. and Walker, Joshua H. and Lemley, Mark A., *Patent Quality and Settlement among Repeat Patent Litigants (September 16, 2010). Pages 3-4. Stanford Law and Economics Olin Working Paper No. 398, 99 Georgetown Law Journal 677 (2011),* https://ssrn.com/abstract=1677785

147 *Id.*

148 All examples detailed at EFF's "Saved By Alice" project, eff.org/alice.

149 Adi Kamdar, *The Innovation Act Is Back: Let's Finally Put a Stop to Patent Trolls, EFF Deeplinks Blog (Feb. 5, 2015),* https://www.eff.org/deeplinks/2015/02/innovation-act-back-lets-finally-put-stop-patent-trolls.

150 Joe Mullin, *Patent Trolls Want $1,000–For Scanning Documents, Ars Technica (Jan. 2, 2013).* https://arstechnica.com/tech-policy/2013/01/patent-trolls-want-1000-for-using-scanners/.

151 Congressional Record, Hearing Before the Subcommittee on Commerce, Manufacturing, and Trade of the Committee on Energy and Commerce, 113th Congress, (April 8, 2014), https://www.govinfo.gov/content/pkg/CHRG-113hhrg90884/html/CHRG-113hhrg90884.htm.

152 Alice Corp. v. CLS Bank Int'l | 573 U.S. 208 (2014), https://supreme.justia.com/cases/federal/us/573/208/.

153 Joe Mullin, *Patent Troll Gives Up, Can't Defend "Matchmaking" Patent Under New Law, Ars Technica, (Sept. 19, 2014),* https://arstechnica.com/tech-policy/2014/09/lumen-view-gives-up-on-matchmaking-patent-cant-defend-it-under-new-law/.

154 See Supra Note 134

155 See Supra Note 145

156 *Id.*

157 S. 2140, Patent Eligibility Restoration Act of 2023 (118th Congress), https://www.congress.gov/bill/118th-congress/senate-bill/2140.

158 Joe Mullin, *This Bill Would Revive The Worst Patents on Software – And Human Genes, EFF Deeplinks Blog (Sept. 15, 2023),* https://www.eff.org/deeplinks/2023/09/bill-would-boost-worst-patents-software-and-human-genes.

159 Joe Mullin, *When the U.S. Patent Office Won't Do Its Job, Congress Must Step In, EFF Deeplinks Blog (July 29, 2020),* https://www.eff.org/deeplinks/2020/07/when-us-patent-office-wont-do-its-job-congress-should-step.

160 S. 2440, Prevail Act (118th Congress), https://www.congress.gov/bill/118th-congress/senate-bill/2220/text.

161 Joe Mullin, *Congress Shouldn't Limit The Public's Right To Fight Bad Patents, EFF Deeplinks Blog (November 6, 2023),* https://www.eff.org/deeplinks/2023/11/publics-right-fight-bad-patents-must-be-protected.

162 S. 2774, Pride in Patent Ownership Act (117th Congress), https://www.congress.gov/bill/117th-congress/senate-bill/2774.

163 U.S. District Judge Colm Connolly, Memorandum Opinion and Order in case 21-cv-01362-CFC (November 27, 2023), https://www.eff.org/files/2024/09/09/1_22-cv-00413-cfc_34_primary_document.pdf; Joe Mullin, Judge's Investigation of IP Edge Results In Criminal Referrals, EFF Deeplinks Blog (November 4, 2023), https://www.eff.org/deeplinks/2024/11/judges-investigation-patent-troll-ip-edge-results-criminal-referrals.

164 See Supra Note 128, Figures 2 and 4

165 *Id, Figure 4*

166 TC Heartland LLC v. Kraft Foods Grp. Brands LLC, 581 U.S. 258 (2017).

167 Offices of Senator Thom Tillis and Patrick Leahy, *Letter Regarding Venue*, (November 2, 2021), https://www.courthousenews.com/wp-content/uploads/2022/10/tillis-leahy-letter-re-albright.pdf.

168 *Id*.

169 *Id*.