epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

The Fight to Protect Our Phones

A Multi-Prong Approach to Spyware Reform

epic.org ELECTRONIC PRIVACY INFORMATION CENTER

About EPIC

The Electronic Privacy Information Center (EPIC) is a 501(c)(3) non-profit public interest research advocacy center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC advocates for privacy, algorithmic fairness, and government accountability.

Authors

Maria Villegas Bravo, EPIC Counsel
Alan Butler, Executive Director

Contributions by

Caitriona Fitzgerald, Deputy Director
Jeramie Scott, Director, Surveillance Oversight Program
Calli Schroeder, Director, AI & Human Rights Program
Megan Iorio, Director, Platform Governance & Accountability Program

Acknowledgements

EPIC would like to thank the Spyware Accountability Initiative for providing funding that supported our work on this project. We thank the uncredited EPIC colleagues who helped with this report. Special thanks to members of the U.S. Surveillance Tech Coordination Group, fellow Spyware Accountability Initiative grantees, and Neil Richards, Koch Distinguished Professor of Law, WashU Law, for their work, which informed this project. We thank the Center for Democracy & Technology, Jennifer Brody at Freedom House, and Michael De Dora at Access Now for their review and feedback on an early version of Part III. We also wish to thank our generous donors, who make our work possible as an independently funded organization.

Table of Contents

EXECUTIVE SUMMARY

This report serves as a background primer on government surveillance of individuals through the deployment of spyware. It provides both a strategic assessment of the accountability levers for spyware under current laws and recommendations for future improvements. Our goal is to clearly articulate the risks that government use of spyware poses to fundamental rights and to focus attention on how to mitigate these risks.

The first part of the report outlines the landscape, defines spyware, describes the harms it causes, and details efforts to curb its proliferation. The second part of the report summarizes state laws across the United States that could provide legal mechanisms to limit the harms caused by spyware use. These laws are detailed in the appendices. The report concludes by outlining a positive vision for future spyware regulation.

Spyware is software that enables remote access to a device without the consent or knowledge of the device owner, user, and/or administrator. It is most often deployed to surveil cellphones. It can be downloaded on a device even if a user does not take an affirmative action, such as clicking on a malicious link or attachment. Everyone is potentially vulnerable to these invasive systems. More often, though, social engineering is used to trick individuals into giving up sensitive information, such as account login information, which is then used to infect the device with spyware.

Once spyware is on a device, it can:

- Monitor activities on the device in real time;
- Access user data stored on the device;
- Exfiltrate data to external servers and/or disclose it to third parties; and
- Control or manipulate the device (by activating microphones or cameras, disabling security features, altering system settings, altering and/or fabricating information, and more).

Some examples of this technology include NSO Group's Pegasus, DarkMatter Group's Karma, Intellexa's Predator, Paragon's Graphite, Novispy, Candiru, and Hacking Team's Remote Control System.

Government spyware deployment comes at great cost to privacy, free speech, and free association. There is no way to deploy spyware without violating Americans' First and Fourth Amendment rights. Phones are an extension of ourselves, acting as a nexus between our social lives, work, financial information, and other interests. The Fourth Amendment protects the reasonable expectation of privacy over the treasure troves of information found on devices and in the cloud servers they are connected to. To obtain this information otherwise, law enforcement must apply for a search warrant. In particular, the deployment of spyware captures wire, oral, and electronic communications, thereby implicating the Wiretap Act and its "super warrant" requirements. Therefore, to deploy spyware, government officials should be applying for a wiretap authorization or, at a minimum, a probable cause warrant. But there is little transparency into the government's use of spyware, leaving us to guess whether these requirements are actually enforced.

There is no way to meaningfully mitigate these harms when deploying spyware. Even if law enforcement is applying for a wiretap authorization, there is no way to draft a sufficiently particularized search warrant when the software categorically vacuums up all data on devices and listens in on phone calls. Furthermore, phone calls, text messages, contact lists, and social media posts encompass various forms of speech and association protected under the First Amendment.

Beyond the threat to Constitutional rights and statutory protections, spyware also poses significant counterintelligence risks. Spyware has been used to target American government officials, including members of Congress, their staff, and State Department officials. There is no way to fully protect devices and the sensitive information contained therein from this threat.

Many existing laws can curb both law enforcement deployment of spyware and spyware developers' exploitative hacking methods. EPIC's review of state laws found three categories of laws that, as they exist now, could be leveraged to address different parts of the spyware problem:

- Wiretapping laws;
- Computer crime laws; and
- Intrusion upon seclusion and/or invasion of privacy common law claims.

To adequately address the malicious nature of spyware, however, lawmakers must **ban its acquisition and deployment** by government actors. In situations where lawmakers cannot or will not ban spyware entirely, strong safeguards must be in place for the limited exceptions to a ban:

- Legislation must include clear, specific definitions of spyware to ensure proper scoping. Definitions should **focus on the software's function** and identify common elements of its deployment.
- Legislation should include a **broad definition of protected devices**—the best practice would be to include all cellphones, as well as any computer infrastructure accessed or compromised in the chain between the perpetrator and the target computer.
- Lawmakers must remember that devices are owned by individuals and ensure that laws surrounding spyware **center on victims and their ability to obtain redress** for violations of the law and their rights.
- **Every step of the spyware lifecycle must be regulated**: development, acquisition, deployment, and after the infection has left a device.

We all share a fundamental right to privacy. The corrosive force of spyware-enabled surveillance is not inevitable, and we have the tools to stop this encroachment into our devices and lives.

INTRODUCTION

Take a moment to think about how much your cellphone knows about you. How many hours have you spent in front of that screen in the last day? Did you exchange messages or make a video call to a loved one? Have you searched for information about a health condition or read specific news articles about current events? Were you sending confidential emails on your work account? Even when you were off your cellphone, was there any point during the day when your phone was more than 10 feet away from you? When was the last time you went anywhere without it?

There is no device in the world better suited to surveillance than a modern cellphone. In 2024, 98% of Americans had a cellphone, and all but 7% of those were smartphones.[1] These devices collect precise location data not only with horizontal accuracy (i.e., latitude and longitude) but also with vertical accuracy precise enough to pinpoint the specific floor of the building the device is on.[2] Cellphones are a pocket-dwelling gateway that could, if properly probed, reveal your whole life story. The Supreme Court of the United States has gone so far as to describe cellphones as "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[3] Unfettered access to your devices would reveal your deepest secrets, your relationships, your activities, your words, and your habits in high resolution.

Enter spyware.

Spyware can make all of these granular data points accessible to malicious actors on an ongoing basis, creating a digital private investigator that follows you everywhere. The idea of spyware is not new—indeed, digital surveillance tools have existed since the dawn of computer networking—but current spyware is both extremely sophisticated and in high demand by criminal groups and government intelligence services alike. The malicious use of spyware is expanding beyond the shadowy world of federal spies and criminals. Spyware is now marketed to state and even local government agencies. People are often unsure what technical and legal protections are available to them. Individuals frequently have trouble even confirming whether they

have been a target of spyware, since verifying a spyware infection can usually be done only by technical experts specializing in forensic device analysis.

This report serves as a background primer on government surveillance of individuals through the deployment of spyware and includes a strategic assessment of accountability levers for spyware under current laws as well as areas for future improvement. The first part of the report outlines the landscape, defines spyware, describes the harms it poses, and explains steps taken to curb its proliferation. The second part of the report summarizes state laws across the United States that could provide legal mechanisms to limit the harms of spyware use. These laws are detailed in the appendices. The third part lays out an in-depth, positive vision for spyware regulation and identifies specific states with the highest potential for impact litigation under their existing laws.

EPIC recommends a complete prohibition on the acquisition and use of spyware by state government entities. For states that are not considering a full ban on government spyware use, EPIC outlines an alternative proposed policy model that bans the use of spyware except in extremely limited circumstances, laying out various concrete definitions and safeguards to address each step in the spyware lifecycle: development, government acquisition, deployment, and oversight provisions. These proposed safeguards provide much-needed protections short of a full ban.

The wide-scale use of spyware by state and local governments is not a foregone conclusion. We can take proactive steps now to curtail the use of spyware at the state level and to protect human rights, privacy, and our democratic values.

The Spyware Landscape

[redacted] Defining the problem.

THE SPYWARE LANDSCAPE

Section 1. Defining a Moving Target

Spyware is a category of software that enables remote access to a device without the consent or knowledge of the device owner, user, and/or administrator.[4] Some examples of spyware systems include NSO Group's Pegasus,[5] DarkMatter Group's Karma,[6] Intellexa's Predator,[7] Paragon's Graphite,[8] Novispy,[9] Candiru,[10] and Hacking Team's Remote Control System.[11] This report focuses on the threats posed by the remote deployment of spyware by government actors, without user knowledge, to facilitate complete access to and control of an infected device.

Each company that develops spyware uses different attack vectors, monitoring capabilities, and methods of evading detection. This section lists common attributes of spyware, various categories of surveillance software that share capabilities with spyware but are outside of the scope of the report, and customers in the spyware industry.

Various methods are used to infect devices with spyware, and each comes with its own risks. Spyware installation also usually includes instructions to hide the traces of its download to obfuscate its existence.[12]

Zero-click attacks

Spyware can infect devices without any action from the victim, like clicking a suspicious link.[13] Sophisticated spyware tools use "zero-click" attacks that exploit vulnerabilities in servers, such as Apple's iCloud or WhatsApp's backend, to remotely execute malicious code on a targeted device and gain unrestricted access to it.[14] Malicious actors can also use radio-enabled devices, such as cell-site simulators (aka Stingrays), to directly inject malicious files or code into seemingly innocuous network traffic.[15] These zero-click attacks, however, are more expensive than traditional attack vectors.[16]

Social engineering and phishing

Other techniques, like social engineering[17] and phishing[18], are more widely used to lure victims into clicking links that download malicious software to their devices or to prompt individuals to give up their device login details to a malicious actor.[19]

Compromising AI agents

An emerging threat vector is exploiting a target's use of AI agents. Traditional large language models (LLMs) like ChatGPT or Gemini are complex mathematical formulas that process natural language and generate responses to user prompts.[20] Agentic AI is a new form of LLM that not only generates responses to user prompts but can also take direct action, such as initiating tasks, using external software, collaborating with other AI agents, and completing complex, multi-step objectives, such as booking flights online and setting up calendar invitations.[21] These AI agents can even directly interact with a device's administrative back end. Since the device user delegates the task of opening webpages and clicking links to the AI agent, and also provides account login information to these agents, a hacker can insert instructions into the algorithm to direct it to a malicious website that will download spyware onto the device.[22]

Once a spyware deployer has infected a targeted device, they have sweeping abilities to invade and monitor the device user's personal life. This can include the ability to:

- Monitor activities on the device in real time;
- Access user data stored on the device;
- Exfiltrate data to external servers and/or disclose it to third parties; and
- Control or manipulate the device (by activating microphones or cameras, disabling security features, altering system settings, altering and/or fabricating information, and more).[23]

The ability to infect and control devices and the data accessible through them poses substantial risks to victims and anyone else whose data is accessible from the victim's device. Indeed, in the hacking community, this level of access is tantamount to "owning" a device. With the above suite of capabilities, spyware deployers can view messages before they are sent on end-to-end encrypted channels, listen in on (secure) phone calls, capture pictures or videos using the device's camera, and review any data stored on the device. Some spyware even allows its user to remotely pilot the infected device, such as by turning on microphones or cameras to record the environment around the device. Importantly, while these infections can be used as a one-time intelligence gathering search, they are typically used as continuous monitoring tools. Documented examples include continuous monitoring exceeding 260 days.[24]

The ability to infect and control devices and the data accessible through them poses substantial risks to victims and anyone else whose data is accessible from the victim's device.

Universal Forensics Extraction Devices (UFEDs) like Cellebrite,[25] Magnet Forensics' Graykey,[26] and MSAB's XRY[27] use many of the same techniques to bypass encryption on devices and exfiltrate data to third parties. The key difference between UFEDs and the spyware covered in this report is the ability to remotely install spyware and monitor devices on an ongoing basis. UFEDs typically require physical control of the device and begin their attacks through a wired connection.[28] As of the publication of this report, the companies that provide UFEDs allege that they are not able to engage in continuous data extraction.[29] Continuously, surreptitiously monitoring devices as

the device owner lives their life is a key spyware element that allows law enforcement to acquire granular information on targets, intercept calls, and follow an individual's life in real time.

This report focuses on spyware used by government actors, in particular, rather than the entire universe of commercially available spyware products that might be used maliciously. This broader category of commercial spyware products (generally referred to as "stalkerware" or "spouseware"), like SpyFone,[30] Catwatchful,[31] mSpy,[32] and FlexiSPY,[33] shares some features with the spyware discussed in this report. Stalkerware can continuously monitor devices and activate device components such as microphones, but typically requires physical access to the device for the initial installation.[34] Stalkerware also, as the name implies, frequently implicates private actors using the technology to monitor, harass, and intimidate intimate partners and family members in domestic violence situations.[35] Stalkerware technology is also specifically advertised for employment monitoring, intimate partner monitoring, and child monitoring.[36] However, this report focuses on government spyware use to surveil individuals. While non-government use of stalkerware can cause grave harm, especially when it facilitates domestic violence, it does not implicate the same fundamental rights issues as does government abuse of the same capabilities.

Spyware and other advanced surveillance tools are most commonly used by intelligence services around the world. Because of this, Part I of this report frequently cites examples of intelligence agency use of surveillance technologies; however, this report's survey of laws and recommendations for policy going forward is focused primarily on the potential use of spyware by law enforcement at the federal, state, and local levels and the necessary legal responses. Intelligence agency use of highly intrusive surveillance tools is limited by the size of the intelligence community and its authorities, as well as the immense cost of zero-click exploits. Expanding the acquisition and deployment of spyware to the hundreds of thousands of law enforcement officials across the United States poses exponential risks to fundamental rights and democratic institutions. EPIC's research and recommendations in Parts II and III focus on law enforcement's use of the technology at the state and local levels to begin addressing these exponential harms.

Spyware use is already becoming pervasive amongst government actors. In 2025, the Department of Homeland Security revived its $2 million contract between Immigration and Customs Enforcement (ICE) and the company Paragon, whose flagship product is its spyware software, Graphite.[37] The Federal Bureau of Investigation (FBI) also began testing NSO Group's Pegasus software as early as 2018, spending nearly five million dollars over the course of its test pilot.[38] In fact, the FBI supposedly stopped using Pegasus in 2021 when sanctions against NSO Group were enacted,[39] but subsequent reporting by the New York Times has revealed a contract dated November 2021 that indicates the advertised pause in use may never have happened.[40] The Saudi government used Pegasus to track and ultimately facilitate the murder of journalist Jamal Khashoggi in 2018.[41] Greece has used spyware against its civilians as recently as 2022.[42] So have Serbia,[43] Mexico,[44] Italy,[45] India,[46] and countless others.[47] Recent reporting indicates that spyware companies have targeted sub-national markets within countries, such as the Ontario Provincial Police in Canada, to further expand sales of these systems.[48] Going back further, it is clear that spyware developers have been trying to entrench themselves in the American law enforcement market for over a decade. Local police forces, district attorneys, and state law enforcement agencies have all been targeted as customers by foreign spyware developers as early as 2012.[49]

These incidents are common yet egregious examples of how spyware has been used to target journalists, activists, and political opponents of government regimes. It is not only authoritarian countries using this technology—many countries considered more "free" or "democratic" also use these highly intrusive tools in ways that violate fundamental human rights.

Section 2. Spyware Undermines Fundamental Privacy and Speech Rights

Spyware differs from traditional law enforcement surveillance techniques because it enables the surreptitious, total monitoring of a person's digital and physical life, as well as the lives of those who interact with them, in a single click. This surveillance is fundamentally more intrusive than tapping an individual phone call or searching through one e-mail account.

> Government use of spyware poses serious threats to fundamental rights, particularly privacy, free speech, and free association.

Government use of spyware poses serious threats to fundamental rights, particularly privacy, free speech, and free association. Collecting and accumulating information about a person necessarily confers power over them.[50] Indeed, the reason surveillance occurs in the first place, academic Neil Richards posits, is to be able to understand and control an individual's behavior by threatening intellectual privacy,[51] thereby gaining the ability to engage in blackmail,[52] the ability to discriminate (i.e. place individuals into categories for further ability to understand and control),[53] and the ability to better persuade individuals to the surveillor's ends.[54] Spyware poses an acute threat to intellectual privacy, the principle that "free citizens should be able to make up their own minds about ideas[, which] requires at a minimum, protecting the ability to think and read as well as the social practice of private conversations with confidants."[55] Protecting this bubble of privacy promotes "intellectual diversity, eccentric individuality, and the sense of both belonging to a group and being separate from it" as well as allowing individuals to refine political beliefs and develop new (and potentially unpopular) ideas.[56] Intellectual privacy is threatened when individuals fear surveillance (and/or are actually being surveilled), leading them to repress undesirable behavior and conform.[57]

The U.S. government has long leveraged the power imbalance between the watcher and the watched to malicious ends. In the past, the U.S. government leveraged ongoing monitoring campaigns to capture damaging information on Martin Luther

King Jr. with the goal of removing him from his place of prominence and power that made him effective at challenging the racist legal and cultural regime.[58] A more recent example includes the National Security Agency (NSA)'s surveillance program dedicated to discrediting enemies of the state by monitoring and outing their pornography habits.[59] The technology of the past provided a stilted picture of a person, cataloguing smaller aspects of a person's life, such as phone calls or internet usage. Spyware captures infinitely more—the most intimate details of your life in real time. So armed, the government can widen this power imbalance and more effectively control behavior.

Previously operating in the shadows, this power imbalance now exists in the public consciousness and affects how individuals behave. For example, the 2013 Snowden revelations disclosed the true extent of the NSA's shadowy grip on the flows of data in, out, and through the country, gaining spectacular public attention and prompting public understanding and fear of government surveillance like never before.[60]

The threat of surveillance measures alone is often enough to repress free speech and free association. This is what Professor Richards calls the "normalizing gaze of surveillance."[61] It endangers and stifles expressive and challenging actions, such as protests, as well as private communications among close friends and confidants. For example, a study by scholar Elizabeth Stoycheff following the Snowden revelations found that individuals avoided posting minority views on Facebook and that participants reported changing their technology use after becoming aware of the NSA's social media surveillance.[62] First Amendment scholar Jon Penney found that the views of controversial Wikipedia articles, such as terrorism-related topics like "dirty bomb," "suicide attack," and "Al Qaeda," significantly declined following the Snowden revelations.[63] These are topics that individuals likely believed would attract more government scrutiny. The effects of the threat of surveillance were remarkable, not only in the decrease in page views but also in their duration, with data showing consistent declines in page views across a 32-month period.[64] As awareness of spyware grows, journalists and activists are taking extreme steps to protect their digital security.[65] Sources are also more hesitant to speak with journalists due to fears of communications interception.[66]

The U.S. Constitution was purpose-built to stop the government's encroachment into Americans' lives and remains a first line of defense against surveillance harms.

The U.S. Constitution was purpose-built to stop the government's encroachment into Americans' lives and remains a first line of defense against surveillance harms. Because of the interconnection between the Constitution, U.S. common law, and evolving statutes regulating government surveillance, an understanding of Constitutional law firmly grounds the later statutory protections that stem from Constitutional ideals. The rights that protect individuals against unchecked surveillance are established primarily in the First and Fourth Amendments.

Historically, the Fourth Amendment is understood to work in tandem with the First Amendment to protect both privacy and speech.[67] The First Amendment was originally understood as a protection against prior restraint by the government, whereas the Fourth Amendment was created to prevent law enforcement encroachment on speech through violence and home intrusion.[68] This overlapping protection of privacy rights between the First and Fourth Amendments is crucial to understanding what, exactly, surveillance reform statutes protect Americans from.[69] Statutes protecting Americans from surveillance, such as wiretapping laws and limitations on facial recognition, are rooted in these fundamental rights to privacy enshrined in the Constitution.

A. Spyware and the Fourth Amendment

The Fourth Amendment is the pre-eminent "privacy" related provision in the Constitution. The Fourth Amendment reads:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[70]

Generally, law enforcement is prohibited from engaging in "unreasonable" searches or seizures, which in most cases means that surveillance that violates a person's "reasonable expectation of privacy" must be carried out pursuant to a probable cause warrant.[71] While the Fourth Amendment typically requires a warrant to authorize surveillance, courts have recognized exceptions to that rule in certain "exigent circumstances."[72]

The Fourth Amendment is scoped to surveillance within the United States of persons who have "substantial voluntary connections to the United States."[73] Intelligence gathering is subject to different standards because it is not focused on collecting evidence of crimes and, in many cases, is not targeted at persons in the United States. Under Executive Order 12333, the NSA is authorized to gather signals intelligence about "the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons and their agents" related to the national security of the United States.[74] The Fourth Amendment *does* protect Americans from unreasonable searches by federal intelligence agencies, though, and statutory protections are laid out in the Foreign Intelligence Surveillance Act (FISA). State and local law enforcement agencies (e.g., police departments), on the other hand, are primarily focused on investigating and prosecuting crimes. This falls squarely within the typical scope of Fourth Amendment governance. Critically for the spyware debate, the Supreme Court has held that the Fourth Amendment warrant requirement applies even if the law enforcement official is investigating a national security threat when it is geographically based in the United States.[75]

Core to the Fourth Amendment is the idea of "informational security."[76] In protecting persons, houses, effects, and papers, the Fourth Amendment, in practice, creates a reasonable expectation of privacy over the information stored within those categories.[77] For example, the protection of a house is not merely the protection of the physical property itself, but also of the activities that occur within it.[78] In two seminal cases—*Riley v. California* (2014) and *United States v. Carpenter* (2018)—the Supreme Court recognized that a reasonable expectation of privacy extended to the information stored on and accessible through cellphones as well as the historical location information generated by cellphones.[79]

There is a reasonable expectation of privacy in the digital contents of a cellphone, as well as in data accessible through a phone, such as data stored in a cloud service, and in any data accessible through a camera or microphone. Cellphones differ in "both a quantitative and qualitative sense" from other physical objects that may be subject to search and seizure.[80] They gather various categories of data, which can lead to inferences by association, and this data may date back to the purchase of the cellphone and even further, thanks to the advent of cloud computing servers, which store even more data. Cellphones even retain some information about data deleted off the device, stored in the backend as metadata.[81] To otherwise acquire the same data accessible through a single cellphone, law enforcement would need to draft applications for warrants to monitor phone calls, acquire ongoing location data at a granular level, and subpoena banks, cellphone companies, doctors' offices, and various other companies. Instead, law enforcement can invade a single device and collect all data types at once.

In addition, cellphones store incredibly detailed location logs of the user's movements over time. Cellphones routinely generate location data that can be used to track individuals down to the foot, including both horizontal and vertical position.[82] Cellphones also collect signals from other devices around them, including wireless networks and other radio beacons that help the phone pinpoint its precise location.[83] Because this data is so detailed and expansive, the Supreme Court found that cellphone location data warranted special protection. In *Carpenter,* the Court held that a warrant is required to obtain historical cellphone location data, even if that data is held by a third-party mobile carrier.[84]

> The scale and type of data accessible to law enforcement through a spyware-infected device allows law enforcement to "rummage" through a person's life in precisely the way the Fourth Amendment prohibits.

The scale and type of data accessible to law enforcement through a spyware-in fected device allows law enforcement to "rummage" through a person's life in precisely the way the Fourth Amendment prohibits.[85] Professor Andrew Guthrie Ferguson has identified four categories of harm stemming from law enforcement rummaging:

arbitrariness, overreach, intrusion into constitutionally secured interests, and exposure.[86] The Fourth Amendment protects individuals from arbitrary police action by limiting government enforcement power.[87] It also protects against police overreach by requiring particularity in warrants, limiting law enforcement from finding and using information irrelevant to its purported (or pretextual) goal.[88] Finally, the Fourth Amendment protects from law enforcement intrusions into and exposure of information that could lead to reputational and legal consequences.[89] In fact, for centuries before the Fourth Amendment's creation, the Anglo-American legal canon was narrowing down the grossly broad general warrant to what we now know as particularized or specific warrants due to these very harms.[90]

The use of spyware to monitor and access smartphone data constitutes unreasonable intrusions across all of these dimensions. Spyware infections are overinclusive because they capture innocent conduct and information on innocent people who may in no way be connected to the alleged crime the spyware is meant to detect. The digital nature of phones also reduces friction for law enforcement in vacuuming up as much data as possible. The advent of LLMs and other advanced technologies enables law enforcement to analyze far more of a person's life at a speed and scale previously thought impossible.[91]

> Spyware allows intelligence officials shockingly broad access to the granular, expressive content of the victim's life by weaponizing their devices against them in a way that traditional surveillance methods cannot.

Spyware allows intelligence officials shockingly broad access to the granular, expressive content of the victim's life by weaponizing their devices against them in a way that traditional surveillance methods cannot. Even if law enforcement acquired a device with traditional physical custody or intercepted communications via wiretapping, they would not magically acquire passwords to various accounts that would allow them to access bank accounts, health tracker apps, or password managers. Nor can traditional wiretaps remotely activate microphones while a phone is locked, allowing listeners to surreptitiously eavesdrop on conversations, or remotely turn cameras on to take

snapshots of a person and their surroundings without notice. However, using spyware, law enforcement could watch the keyboard on your screen as you enter your bank account password and view whatever you review, including transactions and bank account numbers. Law enforcement could take a picture of an acquaintance while you look something up on your phone mid-conversation at lunch. While you are none the wiser, law enforcement could download all the images on your phone.

Using spyware to monitor individuals is a search under the Fourth Amendment. The Supreme Court has made it clear that accessing data stored on cellphones, including data stored on cloud servers that are accessible through the cellphone, is a search and requires a probable cause warrant.[92] In fact, the use of spyware to collect private communications clearly implicates the Electronic Communications Privacy Act (ECPA), which prohibits the interception of wire, oral, and electronic communications without proper authorization.[93] And the use of spyware-infected devices to access remotely stored data implicates the Stored Communications Act, including its prohibition on unauthorized access to stored communications.[94] Because spyware allows law enforcement to intercept wire communications and thus is subject to ECPA, a simple warrant would be insufficient oversight of this surveillance technology and a clear violation of ECPA's stronger wiretap authorization requirements.

Most important, though, is the real-time dimension of spyware monitoring that sets it apart from other surveillance technologies like UFEDs. Under the Wiretap Act, the dividing line between a piece of data requiring a probable cause warrant vs. a regular court-ordered subpoena is whether the communication is in motion or at rest (i.e., stored on the device and not transiting between computers at the time of interception).[95] Even before *Carpenter*, real-time location tracking required a probable cause warrant.[96] The fact that spyware can access all of the aforementioned data on an ongoing basis, for hundreds of days at a time, creates a high risk of law enforcement overreach that violates not only the Wiretap Act, but also a person's sense of security in their devices and their Fourth Amendment rights.

Unregulated government use of spyware is inconsistent with the Constitution. The Fourth Amendment demands that such a technology be severely limited in scope and

function. Similar highly intrusive law enforcement data collection techniques and technologies have safeguards and oversight mechanisms in place to protect individuals from these corrosive practices. For example, ECPA requires wiretap orders, sometimes referred to as "super warrants," in cases where law enforcement seeks to continuously monitor phone calls.[97] These wiretap orders must not only be supported by probable cause and particularized to specific individuals, but law enforcement must also try other, less invasive means of investigation and demonstrate that they have not collected the sought-after communications before being allowed to engage in this highly intrusive method of monitoring.[98] There are also specialized courts at the federal level, like the Foreign Intelligence Surveillance Court (FISC), that provide direct judicial oversight of highly classified intelligence activities, including electronic surveillance, in recognition of the fact that those powers must be subject to independent oversight, even as they are protected from broad public disclosure.[99]

While spyware can be used to intercept wire, oral, and electronic communications, the use of spyware for intelligence purposes has not yet been publicly challenged in the U.S. due to a lack of evidence. One area where this technology may have been adjudicated is in the FISC, which oversees wiretap applications sought under FISA.[100] Under FISA, intelligence officials can obtain authorization to conduct physical or electronic surveillance of persons in the United States where there is probable cause to believe they are agents of a foreign power. Under the broader authorities granted by the controversial[101] later-added § 702, the Department of Justice (DOJ) and the FBI can authorize surveillance programs and demand data from internet providers and others designed to target non-U.S. persons abroad (even if the private communications of Americans are swept up in that net).[102] This programmatic surveillance authority has been challenged as threatening the privacy of domestic communications, and intelligence oversight bodies have disclosed significant violations of the targeting and minimization standards.[103] The adjudication process, though, is one of the most secretive in the nation.[104] There has been some improvement in transparency following the USA Freedom Act in 2015, which amended FISA.[105] On rare occasions, FISC opinions are declassified, shedding light on intelligence practices under these authorities.[106] Until the 2015 amendments, the FISC did not even require anyone to advocate on behalf of the surveillance target.[107]

If the intelligence community has taken steps to engage with oversight of spyware use, the public has seen no evidence of it.

While mandating warrants supported by probable cause for the use of spyware would be a meaningful step, it would be insufficient to fully protect individuals. After the Snowden revelations, it was found that the FISC approved 99% of wiretap applications.[108] Even traditional courts rarely, if ever, deny regular wiretap warrants.[109] Any warrant requesting authorization to deploy spyware would be overbroad. The Fourth Amendment requires both particularization and reasonableness.[110] The deployment of spyware necessarily captures all the data on a device, not just specific communications or particular files on a specified number of subjects. Adding to the issues of overbreadth, there are less invasive means to obtain the same information, suggesting a lack of reasonableness.[111] Because of the nature of spyware, it is impossible to particularize and restrict its use in a manner that is reasonable under the Fourth Amendment.

The Fourth Amendment requires government searches to be "reasonable," and both the Courts and Congress have previously found that the interception of real-time communications is too intrusive to be justified by a simple warrant. For example, Congress codified the stricter "wiretap" standard in 18 U.S.C. § 2516, which first applied to telephone communications in 1968[112] and was later extended to all electronic communications in 1986 with the passage of ECPA.[113] The scope of invasion caused by the installation of spyware is even broader, implicating not only the privacy of conversations but also the ability to speak and associate freely from the prying eyes of the government. Surveillance can create chilling effects on speech and association, affecting both those who are surveilled and those who are not. Beyond this chilling effect, the granular insight into individuals' devices is overbroad and disproportionate to the government's purported interest.

Even if a spyware warrant somehow complies with the particularization and reasonableness limitations of the Fourth Amendment, the Fourth Amendment standards, by themselves, do not adequately protect the speech interests of Americans. Fourth Amendment standards do not inquire into whether the investigation is politically motivated; they only require probable cause that a crime

occurred. Additionally, there have been major roadblocks to challenging surveillance under the Fourth Amendment, with the court system repeatedly throwing cases out on procedural grounds rather than reaching the merits.[114] For example, EPIC's mandamus petition to the Supreme Court regarding the NSA's bulk metadata collection program was thrown out nearly immediately.[115] Even in dicta, the courts have found that the mere existence of a proper warrant could properly protect a person's interest despite the weight of the evidence to the contrary.[116]

Academics have proposed analyzing mass surveillance of individuals through both the Fourth and First Amendments.[117] These rights work in tandem, with the First Amendment speaking more directly to protect against government actions that threaten dissenting voices and organizing efforts. *Riley*, *Carpenter*, and *United States v. Warshak*, while not explicitly engaging in a First Amendment analysis, all considered aspects of freedom of expression and associational freedom as determinative of a right to privacy, thereby requiring a warrant under the Fourth Amendment.[118] A First Amendment analysis could fill gaps left by the Fourth Amendment.

B. Spyware and the First Amendment

The First Amendment confers a broader zone of protection and generally protects the right to free speech and free association. The First Amendment "protects ideas and dissent in a way that the Fourth Amendment does not,"[119] especially in that it protects individuals in public as well as in private. The First Amendment reads:

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; **or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble**, and to petition the government for a redress of grievances. [120]

The First Amendment applies when there is legally protected speech (or association), and when a government practice burdens that speech or association.[121] Once a Court finds that the First Amendment applies, then it will analyze whether the government's action is justified.[122] Courts apply different levels of scrutiny to this government interest based on the type of protected speech or association at issue and the kind of

burden being imposed.[123] For example, viewpoint-based burdens generally receive strict scrutiny —the highest level of scrutiny, which is very hard to meet— whereas burdens that only incidentally affect speech generally receive intermediate scrutiny — an easier standard to meet.[124]

Cellphones contain both expressive speech and associational information, both of which are protected by the First Amendment. Government surveillance actively chills speech and association, both by preventing individuals from engaging in practices that express their beliefs and by pressuring them to affirmatively conform to majority views even when those views contradict their personal beliefs. This effect is supercharged when the government uses information from this surveillance to imprison or otherwise harm individuals. These harms do not go away merely because law enforcement has a warrant stating why they are targeting a specific individual.

Phones contain private communications between individuals, personal thoughts on political topics, social media posts where they learn about new topics, news articles showing opinions that conflict with the government's actions, and an internet history of what individuals have been reading recently.[125] Phones contain contact lists, follows, and interactions with individuals on social media platforms, as well as logs of communications with other individuals (calls, texts, emails, and otherwise).[126] Together, these data points form a dense network of data protected under the First Amendment.

Government surveillance chills speech and association—that is, individuals who fear government surveillance and/or know they are being surveilled stop engaging in practices that echo their beliefs.[127] However, chilling effects aren't merely repressive—they also produce conforming behavior. First Amendment scholar Jon Penney's work draws on a long history of social science research on the effects of surveillance on conformity, showing how surveillance and threats to reputation can produce compliance.[128] For example, an experiment attempting to study the effects of different office environments on worker productivity ultimately failed because workers, under the scientist's surveillance, worked more diligently than usual to avoid reprisal.[129] Several other studies confirm the idea that surveillance produces conforming behavior, even when participants knew the surveillance was artificial and that no one

was actually watching them.[130] Surveillance, then, is a powerful "tool of social control" that enhances the "power of social norms" when people are being observed.[131]

Governments have rationalized the use of intrusive monitoring tools by raising concerns about criminals "going dark" and using increasingly more secure communications to evade law enforcement monitoring. Terrorism, child sexual abuse material, and threats of imminent harm are put forward as justifications for spyware use, but often act as a pretext for governments to acquire highly intrusive surveillance tools like spyware before using them against the general population.[132] The Trump Administration's political weaponization of law enforcement and national security tools to chill protected speech has been brought to the forefront in 2025. They have shown their willingness to interpret terrorism broadly[133] and define their political opponents as criminals to remove access to, among other things, non-profit tax exemption status and student loan forgiveness.[134]

Underscoring the pretextual nature of this justification, the vast majority of confirmed cases of spyware infection have targeted journalists, activists, and political dissidents.[135] This tool is actively used to censor politically unpopular beliefs and threats to governments. This chilling of political speech is unacceptable and will not be stopped merely because spyware is used only when a search warrant is successfully authorized.

Despite the clear overlap of privacy and speech protections, most disputes over surveillance practices have been brought under the Fourth Amendment. But an important line of cases has focused on the overlapping interests of privacy, speech, and association in the First and Fourth Amendments. In 1958, the Supreme Court decided a seminal case on freedom of association and the right to associate in private, finding that a search warrant was not a sufficient basis to compel the disclosure of a NAACP chapter's membership list.[136] And, in subsequent Fourth Amendment privacy cases, the Court recognized that "Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech."[137]

Merely acquiring a probable cause warrant under the Fourth Amendment does not go far enough to address the myriad First Amendment harms to journalists, activists, government actors, and individuals targeted with this technology. It should not be sufficient for a law enforcement officer to claim probable cause to believe they will discover evidence on a phone in order to install spyware. There are far less intrusive means of gathering evidence, including traditional wiretaps to collect specific communications or data, or warrants to physically seize the phone and review historical data. Allowing ongoing monitoring of the phone's activities under the lower warrant standard would essentially eviscerate the Wiretap Act. At the very least, wiretap-style authorizations with exhaustion requirements and narrow interception limits would begin to address some of the threats to privacy, free speech, and free association. However, a complete prohibition on the technology would best protect Americans' interests.

Section 3. The Profound Psychological Effects of Granular Surveillance

Spyware's grave harms to Constitutional rights are exemplified by the profound psychological effects of surveillance on survivors of these intense monitoring campaigns. These enumerated rights to free speech, free association, and privacy exist to allow individuals to participate in society without fear of repercussions. Cellphones are the nexus of a person's social, work, financial, and personal life that spyware gains full access to. When these devices are invaded, individuals feel as if they themselves have been violated. The avoidant and conforming behaviors produced by government surveillance are not just rational actors changing their behavior as automatons. These behavioral changes are often the result of severe psychological distress.

A recent study found profound and multifaceted effects on mental health in 16 confirmed survivors of monitoring campaigns powered by spyware.[138] Mere self-censorship and conformity morphed into acute psychological distress, chronic stress, and social isolation. These attacks "fundamentally eroded [spyware victims'] trust in digital environments" and instilled a "pervasive sense of insecurity and vulnerability."[139] Most participants altered their approach or reduced their engagement

with work they believed led to state-sponsored surveillance, with two even discontinuing their line of work entirely.[140] All 16 of the victims scored high on the Harvard Trauma Questionnaire, indicating the presence of Post Traumatic Stress Disorder symptoms.[141] These symptoms included frequently feeling on guard, difficulty sleeping, feeling irritable or having outbursts of anger, and recurring thoughts or memories of the terrifying events.[142] One notable effect on users is the loss of agency caused by spyware's unique zero-click attacks.[143] There is very little these individuals could have done to protect themselves from these attacks, leading to a "profound sense of powerlessness" that fuels their psychological distress.

One participant stated, "It's not just remembering what happened. It's the feeling that comes with it…that the world is not safe, that people are malicious. You remember the attack, and then you immediately think, 'I can't trust anyone.' The memory itself is a reminder that you are fundamentally unsafe."[144] Another participant noted, "My phone is no longer a tool, it's a threat I have to manage."[145]

"My phone is no longer a tool, it's a threat I have to manage."

Section 4. Legal Redress for Spyware Abuses Faces Significant Barriers

Spyware has been used time and time again to facilitate abuses by governments, including censorship, imprisonment, torture, and extrajudicial killings.[146] This technology is fundamentally dangerous and a threat to democratic society. If it is to be used at all, the government must strictly control its use and subject it to independent oversight and control to protect against abuse and infringements of Constitutional rights. Yet there has been a troubling lack of transparency and oversight into the use of spyware, specifically, and, more generally, into the use of new surveillance technologies as they emerge.

In the past 30 years, the Supreme Court has made it very difficult, if not impossible, to challenge advanced surveillance systems by requiring specific allegations of use and harm, even though there is a stunning lack of transparency around these tools.[147] This trend goes beyond spyware, affecting any new systems of surveillance. Without

evidence to substantiate claims that individuals have been subject to surveillance, courts are refusing to hear cases. A lawsuit by Amnesty International challenging the NSA's practice of bulk collection of nearly all communications transiting in and out of the United States (pre-dating the Snowden revelations by 5 years) was dismissed for lack of evidence to challenge the amendments to FISA.[148] The Supreme Court outright denied EPIC's mandamus petition for the Court to review the very same bulk metadata collection program.[149] The ACLU case challenging substantially the same behavior under § 215 of FISA succeeded at the Second Circuit Court of Appeals, though, and the law was amended quickly after.[150] However, this lack of evidence is a key part of how the intelligence community and law enforcement writ large engage in surveillance. In fact, intelligence community operations are often obfuscated even from other parts of the government. In the Amnesty International case, the Solicitor General famously assured the Supreme Court Justices that any individuals targeted by 702 would be notified if that evidence was used to prosecute them.[151] Later, the office had to file a correction when the DOJ informed them that targets were not actually being notified when evidence derived from Section 702 surveillance was used against them in criminal cases.[152]

Victims of spyware are particularly vulnerable to having their cases dismissed due to a lack of evidence that courts would accept. Often, they cannot even confirm that spyware is being used against them because there is no transparency or notification about its use. Governments are secretive about the military and intelligence products and services they use.[153] Spyware victims are not notified of the surveillance—even after the fact—because law enforcement argues that putting surveillance targets on notice nullifies its utility. Without government disclosures, it is even harder for individuals to confirm whether they are being spied on, since spyware is, by its nature, difficult for victims to detect. There are rare instances when specialized spyware research groups, labs, engineers, or safety teams can confirm that a person has been subject to spyware-enabled monitoring and inform them of it.[154] Therefore, victims are often unaware that their communications, movements, and other information have been recorded at all, much less in millions of granular data points. We cannot be sure how many instances of spyware go entirely undetected.

Even if an individual has been criminally convicted after spyware was used to surveil them, it is unlikely that law enforcement will confirm that the individual was targeted. Law enforcement often hides the manner in which they gather evidence by engaging in parallel construction.[155] To skirt warrant requirements and other procedural safeguards, law enforcement will gather further evidence using approved means that point to the same conclusions as information previously collected with legally questionable methods.[156]

Beyond the lack of transparency in spyware use, there is also limited oversight of its acquisition. It is unclear whether the U.S. Government is developing spyware itself or merely contracting out, and to what extent.[157] There are some safeguards in place regarding federal procurement,[158] but there are still no transparency measures that publicly reveal how spyware is developed or acquired. It is unclear how often (or even which) government agencies purchase spyware tools. In addition, these limited safeguards only apply to federal government agencies, not to the states.

There are various avenues to challenge the acquisition and use of spyware, but these challenges are limited by the court's willingness and ability to hear cases on the merits. One way to address these challenges is to leverage the Fifth Amendment. The Fifth Amendment prohibits the deprivation of "life, liberty, or property" by the government without due process of law. Due process is not a box-checking exercise, nor is it limited to a narrow, pre-determined set of requirements.[159] Instead, due process is a malleable concept that "calls for such procedural protections as the particular situation demands."[160] A part of due process includes being aware of (and able to challenge) any invasion of rights, particularly where that invasion may be used against an individual, as when information obtained through spyware is used to censor, harass, convict, or further impact a victim.

Section 5. Spyware Poses a Major Counterintelligence Threat

The development and deployment of commercial spyware also pose major counterintelligence and national security risks. First, spyware systems exploit security vulnerabilities in software and hardware to undermine the security of government and critical infrastructure systems.[161] Second, spyware is used to target U.S. military and other leaders. Third, even the spyware used by vetted government contractors creates a new target for malicious hackers (e.g., hacking the spyware systems and servers gives access to target data). And fourth, the development of spyware systems to attack consumer devices undermines trust in consumer products, many of which are designed and sold by U.S. companies.

> "Cybersecurity experts agree that there is no backdoor available only to "good actors."

When the government contracts for or procures spyware systems, it both supports and relies on the development of security vulnerabilities that weaken our cybersecurity posture and, thereby, our national security. Cybersecurity experts agree that there is no backdoor available only to "good actors."[162] For example, in 2017, a series of attacks referred to as "WannaCry" and "NotPetya" led to "the loss of billions of dollars for governments and private companies across the globe."[163] These attacks leveraged a "vulnerability found in the Microsoft Windows operating system" that the "United States had discovered … many years earlier" but refused to disclose to the company. The U.S. chose instead to use that vulnerability for intelligence gathering rather than notify Microsoft and have it patched for all global users.

Experts within the White House have recognized the risks posed by these vulnerabilities and the need to manage the risks for decades. And yet, the interest in maintaining hacking capabilities has superseded those interests, leading to devastating attacks. In 2016, the White House announced the formal release of its Vulnerabilities Equities Process (VEP), which was a decision-making process the Intelligence Community had developed to evaluate whether to disclose a known vulnerability so

that the software developer could fix the problem.[164] This process, while necessary, has proved insufficient to align the incentives of the intelligence community. The VEP provides for interagency review of decisions to disclose or not, but forcing that conversation internally is not enough to ensure that broader cybersecurity interests are given proper weight; it is too easy for intelligence interests to prevail behind closed doors. Congress recognized the need for greater transparency and public awareness of these issues when it created a public reporting requirement in 2019.[165] But more needs to be done to strengthen the process, including putting civilian cybersecurity experts (i.e., CISA) in the lead and expanding reporting and transparency requirements to include information on both the number of vulnerabilities retained and those purchased by federal agencies.[166] There is also a particular problem that arises in the context of spyware and other vendor-provided vulnerabilities, because vendor contracts typically include non-disclosure agreements that can exempt those vulnerabilities from the VEP entirely.[167]

The commercial ecosystem surrounding these security vulnerabilities, especially "zero-click" attacks, creates powerful incentives to find more holes in our digital infrastructure and to keep companies from patching them.[168] This behavior severely undermines claims made by spyware vendors about ethical use and efforts to "protect" privacy and other interests.[169] Both Apple and WhatsApp have sued NSO Group, the creator of notorious spyware Pegasus, for unlawfully hacking their servers to gain access to target devices.[170] Even as these holes are continually patched, new vulnerabilities are unearthed, and companies and consumers are caught in a never-ending game of whack-a-mole. The U.S. government's use of spyware means it relies on these vulnerabilities, incentivizing it to leave its citizens exploitable and necessarily undermining its own national security.

The U.S. government itself is targeted and victimized by these tools. Military officials, diplomats, and other government personnel are already major counterintelligence surveillance targets, and their devices are not safe from spyware threats. In fact, in 2021, at least nine State Department personnel devices were infected with spyware.[171] Senator John Hoeven, Congressman Michael McCaul, and their staffs were also targeted with Intellexa's Predator in 2023.[172] Various foreign leaders, including French

President Emmanuel Macron, have also been targeted by spyware.[173] In addition to the personal risk to those individuals, spyware can be used to exfiltrate highly classified and sensitive information over a long period of time, putting our national security at risk. While some companies have agreements with the U.S. Government to remove the capability to target U.S.-based devices,[174] there is no guarantee that these agreements are being followed due to a lack of oversight.[175] Even if some spyware companies honor these agreements, others have not made the same promise.[176] In fact, the former general manager of a U.S. defense contractor that attempted to buy NSO Group in 2022[177] sold "cyber-exploit components" to a Russian broker who sells to the Russian government.[178] These cyber-exploit components are the same type of "zero-day" vulnerabilities that spyware developers use to infect devices.

The expansion of this commercial spyware ecosystem also creates new points of vulnerability, as criminal hackers can target the spyware vendors rather than develop these complex, expensive systems themselves. In 2021, the Pegasus Project investigated a leak of over 50,000 phone numbers that were found to be potential targets of NSO Group's clients.[179] This leak exposed the targeting of, among others, French President Emmanuel Macron,[180] Dubai's Princess Latifa,[181] and family members of journalist Jamal Khashoggi.[182]

In addition to counterintelligence risks, the creation and maintenance of these vulnerabilities undermine trust in essential infrastructure used by hundreds of millions of people every day. For example, Apple advertises itself as a privacy protective company, implementing encryption and strong safeguards to ensure that user data is protected.[183] Consumers rely on the promises made by platforms that claim to be privacy-forward and entrust their data to these companies.[184] Journalists take great pains to protect the identities of their sources and rely on security measures, such as end-to-end encryption, to safeguard their livelihoods.[185] Reducing trust in critical telecommunications infrastructure will drive customers away from these pillars of the American economy. The fewer vulnerabilities that exist, the more individuals can trust that their devices will not become government spies in their pockets.[186]

Section 6. The U.S. Has Begun to Make Progress on the Federal Level

Despite an international reputation for its massive spying industrial complex,[187] the United States has taken a leading role in the efforts to curb the use and proliferation of commercial spyware. Specifically, the U.S. has developed policies, prohibitions, and sanctions to curtail the efforts of global spyware developers and their (frequently nation-state) clients.

In 2023, the federal government enacted Executive Order 14093 (hereinafter "Spyware Executive Order"), prohibiting the acquisition and use of commercial spyware in certain circumstances and stating that the government has a "fundamental national security and foreign policy interest in countering and preventing the proliferation of commercial spyware."[188] The Spyware Executive Order creates oversight mechanisms to interrogate federal government use of commercial spyware, due diligence processes for federal government procurement, and review systems when the government learns that spyware has been used to engage in human rights abuses (by any government entity or otherwise, including the U.S. government) or poses a counterintelligence threat to the United States.[189]

In conjunction with the Spyware Executive Order, the State Department and Commerce Department have banded together to enforce sanctions against companies that perpetrate or facilitate human rights abuses. Three major companies have already been sanctioned.[190] These companies were placed on the Department of Commerce's entity list—which names companies that U.S. entities may not do business with—while employees and their families received sanctions on visas to travel to the United States.

The Computer Fraud and Abuse Act[191] (CFAA) has also proven effective in penalizing spyware deployment in some cases. Congress enacted the CFAA to protect computer infrastructure, devices, and data from hacking and other forms of unauthorized access.[192] For example, in 2019, WhatsApp sued NSO Group for compromising its servers with spyware under the CFAA, and they won a key victory in 2025.[193] In the course of targeting its spyware victims, NSO Group had sent malicious code via

WhatsApp servers (protected computers) to targeted devices, in violation of WhatsApp's terms of service.[194] NSO Group was found liable and received a $167 million judgment and a permanent injunction.

Individual victims can also use the CFAA, particularly the unauthorized access and use of a computer provision, to hold spyware companies accountable. For example, a case brought by a group of journalists against NSO Group[195] and another case by political activists against spyware purveyor DarkMatter Group[196] are currently being litigated.

Section 7. There Should Be a Focus on Spyware Accountability Work at the State Level

A. Spyware Vendors Are Already Targeting State Law Enforcement Agencies

While the federal government has adopted specific policies regarding spyware use and procurement, states have not yet addressed these issues directly. The Spyware Executive Order's prohibitions apply only to federal law enforcement agencies such as the FBI and ICE. They do not necessarily apply to use or acquisition by state and local law enforcement. The only aspects of federal spyware regulation that may affect state-level government actions are the sanctions imposed by the Commerce Department. If an entity is on the entity list, no American entity, including government actors, can engage in business with it.

Unfortunately, the federal intelligence markets are flush with spyware options. For every big-name spyware company, like NSO Group and Paragon, there are hundreds of software companies developing new spyware,[197] not to mention in-house government engineers developing it without relying on commercial vendors. It appears that spyware vendors are targeting rank-and-file police markets for new customers. In fact, NSO Group has already pitched its spyware to local police forces in the United States.[198] There is also evidence suggesting that the Ontario Provincial Police is already using spyware.[199] The French Narcotraffic Law,[200] as well as a recently passed Austrian law, have expanded the use of spyware and explicitly authorized it.[201]

While spyware can cost millions of dollars and is out of reach for more rural areas, state and local governments have repeatedly given police departments the ability to buy advanced surveillance technology[202] through billion-dollar budgets.[203] Advocates should not wait to develop state-level policy until after victims have been targeted with spyware. Before these technologies are entrenched in everyday policing, advocates should proactively prevent the acquisition of spyware.

B. State Policymakers Have Shown Interest in Strengthening Surveillance Oversight

Since spyware regulation is still relatively nascent, there has been little to no policy attention given to the issue at the state level. This creates an opportunity for privacy advocates to frame arguments early and head off the use of spyware by state and local law enforcement. Early and sustained intervention is critical to securing the necessary protections before state entities are tempted to further enable spyware use. If civil society does not proactively take control of this discussion, the police and technology lobbyists will. In the context of consumer privacy legislation, technology lobbyists have exploited understaffing and short legislative sessions among many state legislators to push their own agenda into policy discussions.[204] Civil society must take advantage of any possible leverage in this field, including arriving first.

Passing laws that curtail law enforcement power at the state level, while difficult, is possible. For example, Oregon and Maryland have laws restricting the sale of precise location data,[205] which law enforcement officers often buy instead of subpoenaing it from cellphone providers.[206] Montana has closed the data broker loophole entirely, requiring law enforcement to apply for a search warrant supported by probable cause or an investigative subpoena before accessing records from data brokers.[207] In addition, several states have passed laws requiring the use of body cameras as an additional layer of oversight for police activity.[208] Finally, some states have also limited the use of facial recognition technologies.[209] There is a willingness to pass laws that restrict law enforcement power if the right narrative is woven.

Leveraging Existing Laws

[redacted] Wiretapping laws, computer crime laws, intrusion upon seclusion claims, and specific spyware laws.

LEVERAGING EXISTING LAWS

While spyware may be an emerging, rapidly advancing surveillance technology, it exists within the context of a long history of government surveillance oversight. Many existing laws can be used to curtail both law enforcement use and commercial development of spyware. EPIC has identified several key state laws that could be leveraged to help rein in these dangerous systems. In this part of the report, we identify four categories of state laws that spyware use could implicate: wiretapping laws, computer crime laws, intrusion upon seclusion claims, and "spyware" laws (laws that may include the word "spyware" but more accurately address other privacy concerns than the threats discussed here). For each category, we provide a summary of its scope and features, along with key examples of state laws.

Section 1. Regulation of Law Enforcement's Wiretapping Capabilities

- The unauthorized interception of wire, oral, and/or electronic communications is prohibited under federal criminal law.[210]
- Nearly all states have adopted additional wiretapping statutes regulating law enforcement conduct. In states that have not adopted a specific wiretapping statute regulating law enforcement conduct, the federal Wiretap Act applies.
  - Arkansas, Kentucky, Maine, and Michigan are the only states without state-specific laws regulating law enforcement wiretapping. For example, Arkansas' communications interception law generally prohibits the interception of wire, oral, and electronic communications by anyone, except (in part) when law enforcement is acting pursuant to the federal ECPA.[211]
  - Some state laws regulating wiretapping capabilities strictly limit the types of investigations for which law enforcement can apply for and execute wiretap authorization warrants. For example, in North Dakota, law enforcement may only apply for and execute wiretap authorization warrants in relation to certain drug offenses.[212]
  - For all other investigations where law enforcement wants to engage in wiretapping, they must rely on the federal ECPA.
- Wiretapping provisions typically have a broad prohibition on interception that is qualified by a specific exemption for certain authorized law enforcement interceptions. Importantly, communications in motion, at rest, and metadata of communications are treated differently, as modeled by the Wiretap Act at the federal level.
  - Communications in motion are communications intercepted while in transit between computers and are governed by laws that follow the ECPA.
  - Communications at rest are accessed when they are stored on a computer and are governed by laws such as the Stored Communications Act (SCA) and related statutes.

  - The collection and disclosure of metadata from communications, such as the identities of senders and recipients and timestamps of phone calls, are governed by the Pen Register Act and related statutes.
  - States vary widely as to whether they have adopted specific laws related to the ECPA, the SCA, and/or the Pen Register Act.
- The scope of covered communications is subject to complex interpretive questions when statutory definitions are applied to new technologies. For example, the statutory protections for stored e-mails under the SCA vary depending on where the message is stored, how long it has been stored, and whether it has been opened.[213]
- Many states also prohibit the creation and distribution of interception devices. This provision, however, typically includes an exemption for interception devices created specifically for law enforcement use or under government contract. [214]
- Defenses to wiretapping liability typically include:
  - Being a party to the communication.
  - Consent.[215]
  - All states with civil liability provisions include a defense of good-faith reliance on a court order.

Procedural Safeguards

- Wiretap laws are purpose-built to safeguard against the improper collection and disclosure of private communications by law enforcement.
- Wiretapping laws not only create criminal liability for civilian unlawful interception, but also establish strict limitations on when law enforcement can obtain authorization to intercept communications.
- The authorization orders issued under wiretap statutes are commonly referred to as "super warrants" because they require more than probable cause. Wiretap orders require a strict set of oversight and mitigation procedures, including exhaustion of alternative methods, time limitations, minimization of non-target communications, and other overlapping oversight measures.[216]

- Communications in motion are protected more than communications at rest, and both are protected more than metadata (i.e., active phone calls vs. emails stored in a database vs. timestamps of calls). Intercepting communications in motion typically requires a wiretap authorization; accessing communications at rest requires a warrant; and collecting metadata can typically be done with a subpoena or court order.

Common Features of Wiretap Authorization Warrants

- **Exhausting less intrusive means**: Law enforcement needs to try other, less invasive, investigative means. Only when evidence shows that those methods did not work or that the case at issue is too dangerous to proceed without a wiretap can a judge grant a warrant.
- **Notice**: Within a certain amount of time after the denial of a warrant or the end of an interception period, targets must be notified of the interception time period and whether or not communications were intercepted.
- **Ongoing oversight**: Law enforcement has to send the authorizing judge status reports during the interception period.
- **Watching the watchers**: Annual reports are typically submitted to the relevant Attorney General on the number of approved warrants and other information.
- **Preservation of privilege**: The interception typically does not destroy the privilege of communications such as those between attorneys and clients.
- **Suppression remedies**: Evidence collected through wiretapping can be suppressed in criminal cases if law enforcement did not comply with the law.
- **Time limits**: Interceptions, as well as any extensions, are time-limited, typically to 30 days.
- **Narrow authority**: Many states limit the use of wiretaps to certain crimes, such as murder or drug-related offenses.
- **Private Right of Action**: Many states, but not all, include an explicit private right of action against law enforcement that fails to comply with the law.
- **Geographic limitations**: Some states have jurisdictional parameters on who can be targeted.[217]

Notable Differences in State Wiretap Laws

- Several states go beyond the federal ECPA and offer stricter protections. For example, Massachusetts,[218] New Jersey,[219] and Washington[220] impose more stringent time limits on the intercept period for warrants than the ECPA's 30-day initial interception period.[221] Maryland and Massachusetts explicitly prohibit the interception of communications for the purpose of investigating crimes related to reproductive health decisions.[222]
- While all these states include a private right of action, Pennsylvania's is notable for waiving sovereign immunity, allowing removal of individuals from office for violations of the law, and providing injunctive relief. [223]
- Georgia, on the other hand, is an example of a state with weak protections. There are no time limitations, no notification requirements, and no private rights of action.[224] Similarly, Montana does not limit the time period of the interception nor provide a private right of action;[225] however, Montana does require notification prior to or contemporaneous with the execution of the warrant (unless a delay is requested through court procedure).[226]

Section 2. Computer Crime Laws

- Computer crime laws are purpose-built to stop the exploitation of computers, including by hacking and other intrusions into private devices. These laws typically criminalize accessing a computer without authorization or exceeding existing authorization.
- Many laws follow the CFAA, but there is a wide variety of computer crime (and trespass) theories, such as those that require intent to commit fraud or that require some form of damage to the computer for liability to attach.

Common Features of Computer Crime Laws

- Laws that closely follow the CFAA still vary. Some states prohibit both use of a computer without authorization and use exceeding authorization (which can include insider threats), but many states only prohibit use "without authorization."
- Many states include crimes that punish damage to computers and any data stored therein, copying (or "stealing") data from computers without authorization, and the installation of "contaminants" (e.g., software, viruses, malware, etc.).
- Few states define which computers are protected by the law or what constitutes exceeding authorization. About half of the states cover the issue of venue, generally noting that if the exploited computer is within the state or if the attacker's computer is located within the state, then the state can prosecute.
- Many states have a law enforcement carveout, protecting law enforcement from criminal liability for violating these laws.

Notable State Law Divergences

- California: This CFAA analogue was successfully used to find NSO Group liable in the *WhatsApp v. NSO Group* case.
- Arkansas, Nevada, Oklahoma, Pennsylvania, and Texas: Attorney General has the authority to investigate computer crimes.
- Virginia's law is an example of a state that includes a vast catalogue of behavior that could constitute a computer crime.[227] Many states include computer fraud and computer trespass in their computer crime laws. Virginia goes further, adding prohibitions on, among other things, spam, invasion of privacy, and theft of computer services.

Section 3. Intrusion Upon Seclusion

- Intrusion upon seclusion is part of U.S. common law, grounded in the idea of invasion of privacy. The common law right to privacy developed in the United States in the early 20th century and was famously distilled into four distinct torts by William Prosser: disclosure of private facts, intrusion upon seclusion, false light, and appropriation of likeness.[228] Some states only formally adopted "invasion of privacy" generally, whereas others adopted one or more of the individual torts.
- **Restatement 2d of torts § 652B**: One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.
- The mere act of intrusion into a private "place" is the harm; disclosure to third parties is not an element of the intrusion tort.

The Case for Spyware Constituting an Intrusion Upon Seclusion Claim

- **Intentional intrusion (physical or otherwise):** Spyware is used to intentionally hack into personal devices. Several states categorize hacking as a type of trespass.[229]
- **Solitude/seclusion /private affairs:** Under the Fourth Amendment, there is a reasonable expectation of privacy in the contents of cellphones and in data accessible through them.[230] Regardless of the Fourth Amendment, people generally do not make the contents of their private devices available to the public or others. Therefore, phones and their contents are sufficiently secluded.
- **Highly Offensive to the Reasonable Person:** The highly private nature of data stored on personal devices (including photos, messages, financial information, and location data) makes an intrusion highly offensive.

Notable Differences

- Wiretapping is explicitly a proper basis for intrusion upon seclusion under the District of Columbia's common law invasion of privacy doctrine.[231]

Section 4. "Spyware" Laws

- These laws, even when they use the term "spyware," do not regulate spyware as scoped by this report. The laws in this category focus on systems that track a user's internet browsing behavior, typically for the purpose of serving ads.

Examples

- American Legislative Exchange Council (ALEC) Model Bill: Computer Spyware Protection Act[232]
  - This law, while using the term spyware, focuses on ad tracking and cyberstalking. Technically, spyware as scoped in this report could fit into this bill's definition of spyware. Spyware can track a device owner's internet history and behavior, record all keystrokes made by a device user, extract personally identifiable information from the hard drive, and prevent (through intentionally deceptive means) efforts to block the installation of such malicious software, among various other elements.
  - However, this bill, as adopted in each state, has an exemption for the use of such malicious software for "detection or prevention of the unauthorized use of or fraudulent or other illegal activities in connection with a network, service, or computer software, including scanning for and removing computer software prescribed under this chapter," making it unfit for checking law enforcement use.
- Alaska: Deceptive Acts or Practices Relating to Spyware[233]
  - This law prohibits the use of software that analyzes website access from a device to create deceptive pop-up advertisements. It is not relevant to spyware as scoped in this report.

A Positive Vision for Spyware Regulation

[redacted] A rubric for effective spyware regulation.

A POSITIVE VISION FOR SPYWARE REGULATION

State laws are an essential part of privacy safeguards that protect individuals against surveillance and abuse. But these laws need to be updated and adapted over time as new surveillance technologies are developed and deployed. EPIC has established evaluation rubrics to help set minimum standards for privacy protection in state laws and to facilitate constructive debate over new proposals to strengthen oversight.

This part of the report includes an evaluation rubric for effective spyware regulation that policymakers, journalists, and others can use to assess the strength of spyware bills and the need for new or updated protections. This rubric covers several key topics, including prohibitions on specific uses, standards for limited authorizations, data minimization requirements, impact assessment and testing obligations, procedural obligations for both developers and deployers, and robust oversight mechanisms.

At a minimum, if a state is interested in regulating spyware, it should establish baseline protections and oversight mechanisms, as outlined in the Spyware Executive Order, to restrict commercial spyware.[234] This Order generally prohibits government entities from acquiring or putting into operational use commercial spyware that poses a significant threat to national security and/or has been used to engage in human rights abuses.

But states can—and should—do more.

Section 1. A New Regulation Purpose Built for Spyware

These recommendations were drafted with U.S. state law frameworks in mind and would be most easily implemented in that context. Still, the general concepts can be adapted to a broader range of jurisdictions. Furthermore, these recommendations focus specifically on the use of spyware by law enforcement, rather than by intelligence agencies or private actors.

BAN THE ACQUISITION AND USE OF SPYWARE

- The use of spyware is fundamentally incompatible with the Fourth and First Amendments. Individuals should have the right to be free from unlawful spyware intrusions. Lawmakers should ban the acquisition and use of all spyware, including by any government actors.
- Any prohibition or limitation on the use of spyware should be backed by strong enforcement, including criminal penalties and civil liability for unauthorized use.
- In states where a full ban is not possible, the exceptions should still be strictly limited to specific serious criminal investigations and include oversight mechanisms at least as strong as the Wiretap Act. While these safeguards can help to protect individual rights against abuses, only a complete ban will adequately protect privacy and free speech.

RIGHTS OF SURVIVORS OF SPYWARE INFECTIONS

- Anyone whose data was targeted and/or intercepted should receive notice that their data was sought and/or acquired. At the very minimum, the judge issuing or denying the spyware warrant authorization should send notice to the target device owner and anyone whose data was intercepted, and serve them:
  - (1) Notice of the entry of the order or the application for an order denied
  - (2) The date of the entry of the order or the denial of an order
  - (3) The target device and the data sought from the deployment of spyware.
  - (4) The time period of authorized or disapproved interception. During the named period, what actions were taken (i.e., exfiltration of data, remote activation of a camera, etc)[235]
- Anyone whose data was targeted should have the right to access the intercepted communications and any records created by law enforcement and/or the spyware system and/or developer and/or deployer in the process of engaging in the interception targeting the individual and the applications and orders.

CONCRETE DEFINITIONS

- **Spyware:** Definitions should focus on the software's function (gaining remote access to and control of computers and their stored data without the device owner's consent). In addition to defining spyware by its general function, state regulations should identify common elements of spyware (such as remote access, control of key functionalities including microphones and cameras, data exfiltration, and alteration of existing data, among others) to ensure that the law is comprehensive enough to protect against future threats. The regulation should apply regardless of whether the spyware was developed by a private company or by a governmental entity, including local, state, federal, and/or foreign governments.
- **Protected devices:** State law should make clear which devices are protected from hacking. The law should broadly define the category of devices subject to protection. An example of a strong, expansive definition of protected computers can be found in the CFAA.[236] As to the scope of protected devices, best practice would be to include all cellphones, as well as any computer infrastructure accessed or compromised in the chain between the perpetrator and the target computer.
- **Developers:** Deployers are the entities that design, create, maintain, modify, or update the spyware system, which is then provided to the deployer. Developers and deployers may be the same entity, or there may be multiple developers for one spyware system.
- **Deployers:** Deployers are entities that use spyware to infect target devices, interact with target devices, and/or direct others to do the same. Developers and deployers may or may not be the same party.
- **Deployer specification:** Laws need not limit the Deployer definition to a specific aggressor (e.g., civilian or government), but the law should not exempt government actors from liability or procedural obligations.
- **A note on definitions:** Carve-outs from these definitions should be limited to instances where necessary to achieve the purposes of the regulation. Exceptions should be narrowly-tailored and clearly justified.

ENFORCEMENT MECHANISMS

- Individuals and organizations should be able to enforce their rights through a private right of action.
  - Anyone who is targeted by spyware and anyone whose communications were intercepted in the process of targeting someone else should have the right to sue both the deployer(s) and the developer(s) for noncompliance with the law.
  - A nonprofit organization should be able to bring an action on behalf of itself or any of its members, or on behalf of the general public, seeking relief from the use of spyware in violation of the law.[237]
  - A public interest organization should be able to bring an action on behalf of the interests of an individual or class of individuals, seeking relief from the use by any person of spyware in violation of the law if the individual or class of individuals in question could bring an action themselves for relief from violation of the law.[238]
- Regarding developers, there should be statutory damages available, including additional damages for intentional/repeated violations of the law.
- The Attorney General and/or other relevant oversight agency/government body should have investigative and enforcement authority.
  - The authority to terminate use of the spyware system should be explicitly authorized.
  - The security clearance (if any is required) and/or other authority to review the contents of spyware-collected data should be explicitly authorized by the oversight body chosen.
  - Injunctive relief and the ability to impose additional requirements on both developers and deployers should be available.
  - Adequate funding and staffing for enforcement and/or oversight bodies should be appropriated.

SAFEGUARDS AT EACH STEP OF THE SPYWARE LIFECYCLE

1) Development Stage:

- Any prohibitions or regulations regarding the development of spyware should not include a carveout for spyware developed under a government contract or other agreement to be used by law enforcement, intelligence, or other governmental agencies.
- The law should require spyware developers to include audit logging features that track each deployment. These logs should consist of, at minimum, identification of the particular spyware that was deployed, information on when the spyware was deployed, who deployed the spyware (specific individual as well as affiliation), who approved the deployment, for how long, what data was collected, the device targeted, and what computers the spyware transited through to reach the target device (i.e., IP addresses or other identifying information).

2) Acquisition Stage:

- **Privacy and Human Rights Impact Assessments**
  - Developers must conduct ongoing assessments whenever a significant change is made to the spyware and should conduct annual assessments to account for new use cases. Deployers must also conduct privacy and human rights impact assessments when determining whether to acquire spyware and before deployment.
  - Where possible, these assessments should be conducted by qualified third parties. Regardless of whether they are third-party or in-house assessors, assessors must have the necessary technical, legal, and ethical expertise and independence to honestly evaluate without fear of retaliation.
  - These assessments must be maintained and made available to relevant enforcement bodies, government oversight bodies, and international fora upon request.
  - Assessments must include, at a minimum:
    - What personal data may be collected or processed, both specific and categories, including any inferences that may be drawn from the data;

- The potential sources of personal data collection;
- Purposes for data collection;
- Contexts of deployment;
- Processes in place to approve deployment;
- What third parties the data may be made available to, and for what purposes;
- How the collected data will be stored and security measures in place, including retention and deletion procedures;
- Potential benefits to the developer, deployer, individual, public, or other stakeholders likely to result from the collection, processing, or disclosure of the data;
- Potential harms to individuals, society, and human rights that may result from the collection, processing, or disclosure of the data, including ranking both the likelihood and severity of each harm;
- Any opportunities to increase transparency and oversight of the spyware;
- Risk mitigation measures that have been or may be implemented to address potential harms;
- Any alternative, less-invasive methods to achieve the legitimate goals of the developer or deployer; and
- What individuals participated in conducting the assessment, and their qualifications.

- The government body engaged in acquisition should engage third-party, independent testing to substantiate claims made by the company regarding privacy and human rights impact assessments.
- Employees who deploy spyware must be properly trained on appropriate use and safeguards, including the mitigation measures detailed in the privacy and human rights impact assessments.

- **Transparency**:
  - Developers and deployers should be required to make public (on their own websites and in a central repository) a plain-language summary of the results of required impact assessments (addressed below), how the risks were weighed against potential benefits, how risks were mitigated,

and procedures for ongoing testing and evaluation of the spyware, including procedures and policy documents relating to auditing the use of the technology.

- Exemptions to disclosure should be strictly limited to trade secrets and should not include overly broad or vague terms like "proprietary," "confidential," or "business" information.
- All disclosures must be clearly displayed, accessible, and in plain language understandable to a reasonable person.
- If a developer or deployer makes a material change to its public disclosures, it must provide the oversight body with notice of the change.

3) Deployment Stage

- Limit the geographic scope of law enforcement deployment of spyware. Best practice would be to limit the deployment of spyware to any target computer physically located within the jurisdiction of the competent authority that approves the warrant application (typically a judge).[239]
- Limit use of spyware to investigations of certain serious crimes (e.g., Serious Violent Felonies as defined in 18 U.S.C. § 3559 (c)(2)(F))
- A spyware wiretap authorization should be required to deploy spyware.
  - Spyware wiretap authorizations supported by probable cause that a serious violent felony has occurred must be required before spyware is deployed.
  - The following information must be included in the application for a spyware wiretap authorization, as well as the court order granting the request:
    - Reasonable time limitations (such as a maximum of 30 days or however long is necessary to acquire the communications sought by the warrant, whichever is shorter); best practice would be to limit the number as well as the total duration of extensions that can be given, and permit extension only when the statutory requirements for the original authorization continue to be met;
    - The application must specify the particularized target device and the particularized data being sought. It must specify the grounds for believing that use of the spyware will result in disclosure of

incriminating information. The application must establish probable cause with respect to each type of data sought. For example, if a law enforcement official seeks location data, the contents of communications, and the contacts list on a device, the official must establish probable cause for each category of information; and

- The applicant must try all less intrusive means of investigation before spyware can be authorized, and may resort to spyware only if all other investigative measures have failed or are shown to be futile for collecting the data sought. Warrant applications for spyware use must also include an exhaustion requirement, meaning applications must note which methods have been attempted, why they failed, why other, less intrusive means of surveillance would be futile, and how the use of spyware would acquire the targeted data when other methods failed.

- Procedure to apply for spyware wiretap authorization:
  - The application must be supported by probable cause and include all of the above information.
  - A judge must deny or grant the application based on the above factors.
  - Extensions of spyware wiretap authorizations must be limited.
  - Best practice would be to require spyware wiretap applications to go through multiple levels of review before reaching a judge. For example, some state wiretapping laws require law enforcement to submit wiretap warrant applications to the Attorney General or a state prosecutor, who must sign off on the application using the same criteria as the final-granting judge before it is officially submitted to a judge for review.

- There must be robust reporting requirements to ensure transparency and accountability in the deployment of spyware.
  - The spyware deployer must report to the judge throughout execution of the warrant, providing status updates, including, at minimum, how the spyware has been deployed, what data has been collected, and whether the targeted data has been collected.
  - Judges must report to a competent oversight body annually on the number of spyware authorizations requested, granted, and denied, the

number of devices accessed, and other information to help the oversight body monitor the use of spyware.

- Targets must be notified of infections to their devices:
  - Within a specific period after spyware use ends (90 days is standard for wiretap notifications and should be used for spyware as well), targets must be notified that spyware was used against them. As a best practice, targets should also be notified when an application requesting interception is denied.
  - Notice should include information on the specific spyware technology used; the contents intercepted; whether cameras, microphones, and/or other features were remotely activated; the time period when devices were infected; which devices were infected; the application for the warrant; the authorized warrant; the agency and personnel that deployed the spyware; and any other pertinent information.
- There should be requirements for a robust auditing ecosystem:
  - Audit logs must be created for every instance of spyware use by both deployers and developers. Logs should include, at a minimum, the individual(s) using the spyware, the actions taken (e.g., data exfiltration, remote camera activation), the target, and the data collected during the spyware's use.
  - These logs should be reviewed by the supervisors of the individual(s) who deployed the spyware within 10 days of the end of spyware use.
  - These logs should be reviewed by the judge who approved the initial warrant and/or any extensions, both before granting an extension and within 30 days of the end of the use of spyware.
  - These logs should be reviewed at least annually by a competent oversight body to ensure that spyware is used within the bounds of the law.
  - These audit logs should be made available if a civil or criminal lawsuit implicates the use of spyware.
- There must be enforceable provisions to terminate the use of spyware:
  - Any noncompliance with the authorization requirements and/or other procedural safeguards enumerated in the law must result in immediate cessation of spyware use.

  - If an oversight body receives credible evidence that spyware has been used to engage in human rights abuses, all deployers within that jurisdiction must stop use of the spyware entirely.[240]

- There must be robust safeguards surrounding the use of the collected data:
  - Rules on secondary use:
    - Information obtained through the execution of a spyware wiretap authorization shall be used only for the investigation described in the original application seeking the warrant.
    - Absent a subsequently issued spyware wiretap authorization, the database containing the spyware-collected data cannot be queried for any purpose not listed in the original order granting the execution of the warrant.
  - The data collected through the execution of the spyware-connected search warrant may not be used as evidence in legal proceedings unless the appropriate parties have been properly notified. Legal proceedings include, but are not limited to, civil lawsuits, criminal prosecutions, and proceedings before immigration court.
  - Any spyware-collected data introduced as evidence in legal proceedings may be suppressed through the applicable evidentiary rules if it was collected in violation of any of the provisions of this law.
- Data retention
  - Developers and deployers should have a duty of care to protect personal data against unauthorized access, use, destruction, modification, or disclosure.
  - Data should not be stored, held, or transferred in plain text form.
  - Developers and deployers must create and implement a standard operating procedure for detecting and responding to security incidents and breaches, including reporting the incident to relevant government regulators and affected individuals.
  - Both developers and deployers must create and implement a standard operating procedure for retention and deletion of any data collected throughout the execution of a spyware-connected warrant.

Section 2. Leveraging Existing Laws

In addition to proposing new laws wholesale, various existing laws mentioned in Part II could be amended to bolster the current protections against spyware. Lawsuits can also be brought under these laws against both government officials who surveilled victims and the spyware developers who provided the means and instrumentalities to do so. Overall, the varying state-level computer hacking laws would require the most work to harmonize them with the federal CFAA. However, state-level wiretapping laws are generally more consistent with the federal Wiretap Act and can often be applied to spyware in their current state. States whose wiretap regulations are not yet aligned with the baseline Wiretap Act protections can be amended to mirror its time limitations, notification requirements, and other safeguards.

A. Expanding Computer Crime Laws

All states have some kind of computer crime law, and while several include CFAA analogues, many go further and include various specific computer crimes. The CFAA is a purpose-made statute to address hacking and the exploitation of digital infrastructure, and has already been successfully used to find NSO Group liable for hacking WhatsApp's servers. Many state laws go into more detail than the CFAA, focusing on access to and theft of data, damage to devices, and installation of "contaminants." [241]

The CFAA covers a broad range of hacking activity by addressing accessing a computer "without authorization" as well as when "exceeding authorized access," includes a broad technical definition of computer, and can be used in litigation both by the end target of the spyware and by any entities that own servers and other network trafficking computers along the chain of computers between the deployer and the spyware target. However, both the CFAA and many state computer crime laws include a law enforcement carveout. In their current state, laws with these carveouts can only target the spyware developer and any non-governmental third party assisting in its development and deployment.

State laws based on the CFAA, such as Iowa's,[242] often lack the "insider threat" model captured by the federal definition's inclusion of "exceeding authorized access." Spyware developers often create lawful pathways to access servers, such as creating a WhatsApp account, but then find ways to exploit that lawful access to target other devices.[243] This exploitation of lawful access points is an important threat model to consider when regulating spyware, so, at a minimum, state laws should include language addressing "exceeding authorized access" rather than merely prohibiting unauthorized access to computers.

States should pass laws to prohibit more specific crimes that reflect the dangers facing computer owners in the 21st century. First and foremost, the law enforcement carveouts should be removed. Second, state laws should expand their language to match strong laws like Virginia's with a wide variety of causes of actions. Importantly, state computer crime laws should prohibit the installation of computer "contaminants," such as viruses, keyloggers, and other foreign code.[244] Furthermore, computer crime laws can be improved by explicitly expanding the definition of protected computers to include any computer infrastructure accessed or compromised in the chain between the deployer and the target computer.

B. Harmonizing Wiretap Laws

State wiretap laws generally conform to key components of the Wiretap Act, including the warrant application procedure, warrant application requirements, punishments for noncompliance, and other provisions. The Wiretap Act is strong because it includes a private right of action, layered oversight mechanisms, and mitigation procedures that limit the time and manner in which law enforcement can intercept communications.

Many states, however, depart from the Wiretap Act and erode the procedural protections. For example, many states include unlimited extension time periods for warrants. Others omit the notification requirements and private right of action entirely. State wiretap laws that do not meet the floor of protection provided by the Wiretap Act should be amended to include, at a minimum, the following:

- Short time limitations and a limit on the number of extensions available;
- States that do not have time limitations should institute them. States that do not limit the number of extensions available for each interception period should set a limit of 3 extensions to mirror Connecticut's wiretap law.;
- A right to notification within an explicit time period after interception;
- A private right of action for individuals who were targeted without proper compliance with the Wiretap Act and/or whose communications were intercepted in the process of executing the wiretap authorization warrant;
- Criminal liability for law enforcement who do not comply with the Wiretap Act;
- The ability to suppress evidence in criminal trials that was collected through improper wiretapping; and
- Limit the use of wiretaps to specifically enumerated, severe crimes.

C. What to do with "Spyware" Laws?

The states that passed the ALEC model bill should amend the law to remove carveouts for law enforcement and government contracts, ensuring that law enforcement entities cannot evade wiretap authorization and warrant requirements by using commercially available technology.

D. Expanding the Ability to Sue

Both state level computer crime laws and wiretap laws should be amended to include organizational standing, including both (i) membership organizations suing on behalf of themselves, their members, and/or the general public; and (ii) organizations suing on behalf of the interest of an individual or class of individuals that could bring an action themselves for relief from violation of the law. Washington D.C.'s consumer protection statute[245] includes this broad category of standing to ensure that organizations with specialized knowledge and resources can bring cases on their own behalf or on behalf of others.

Under the DC Consumer Protection Procedures Act, a public interest organization is defined as "a nonprofit organization that is organized and operating, in whole or in

part, for the purpose of promoting interests or rights of consumers."[246] In lieu of Article III standing requirements, a public interest organization must only have a "sufficient nexus" to the interest of the consumers it represents, which need not be the "primary purpose" of the organization.[247] A "subsidiary purpose" is sufficient.[248]

Organizational standing in the spyware context would be revolutionary. Without notification requirements, individual targets do not know their device was infected in the first place, nor by whom or with what technology. Even with the notification requirements in place, individuals may not have the technical ability and/or capacity to gather the highly technical evidence to prove that the spyware was developed and/or deployed in violation of the law.

Civil society organizations like the threat labs that engage in forensic analysis of devices and/or those who track human rights abuses among technology companies have the appropriate evidence and wherewithal to bring claims against spyware developers and deployers for violations of the law, even if they don't know all affected targets individually. Amending the law to give these organizations standing to sue for violations would ensure that this notoriously surreptitious and highly technical practice is kept in check.

Section 3. Impact Litigation

States that already have strong computer crime and wiretap laws should be targeted for impact litigation.

For computer crime laws, organizations should target Maryland, Pennsylvania, and California for test cases, as these states have the most safeguards and are located in Circuits that have ruled favorably on Fourth Amendment cases. California's Comprehensive Computer Data Access and Fraud Act has already been successfully used in the WhatsApp case.[249] The success of the CFAA in both the Northern District of California and the District of Oregon indicates that state computer crime laws that closely mirror its language should be similarly successful. [250]

For wiretap laws, organizations should target states such as Pennsylvania, California, and Maryland, which have strong procedural safeguards and private rights of action. Organizations may also submit relevant evidence to Attorneys General in states like Montana, where Attorneys General have investigative and enforcement authority over wiretapping laws.

Section 4. Exploring and Connecting New Areas of the Law

In addition to the laws described above, other areas of law could be leveraged to address spyware use. For example, product liability law could be used to target the spyware development within the United States. Furthermore, several organizations are already attempting to track the financing of major spyware companies, in part to assess potential financial crimes.[251] These organizations are notifying both the appropriate authorities and investors of private equity groups that buy these technologies without knowing the major human rights abuses they can, and have, caused.

Conclusion

[redacted]

CONCLUSION

Spyware will never be an appropriate or proportionate approach to the purported goal of fighting crime if the cost is eliminating privacy, free press, and free expression. Spyware enables serious violations of privacy and speech rights and no government entity (federal, state, local, tribal, or otherwise) should be allowed to deploy these systems for law enforcement purposes. We are still early enough to make meaningful change at the state level to prevent the acquisition and deployment of spyware before the industry can get their foot in the door. Even if states cannot or will not pass laws fully banning the intrusive practice, this report provides an ecosystem of protective safeguards that can limit the harms created by this technology. The corrosive force of spyware-enabled surveillance is not inevitable, and we have the tools to stop this encroachment into our devices and lives.

ENDNOTES

[1] Olivia Sidoti et al., *Mobile Fact Sheet*, Pew Rsch. Ctr., https://www.pewresearch.org/internet/fact-sheet/mobile/.

[2] Susan Landau, *A Radical Proposal for Protecting Privacy: Halt Industry's Use of 'Non-Content*,' Lawfare (Sept. 8, 2023), https://www.lawfaremedia.org/article/a-radical-proposal-for-protecting-privacy-halt-industry-s-use-of-non-content; *see also*, FCC Fact Sheet, *Improving Wireless 911 Caller Location,* Sixth Further Notice of Proposed Rulemaking, PS Dkt. No. 07-114 (Mar. 6, 2025), https://docs.fcc.gov/public/attachments/DOC-410028A1.pdf; FCC, *Indoor Location Accuracy Timeline and Live Call Data Reporting Template* (Jul. 26, 2021), https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/911-services/general/location-accuracy-indoor-benchmarks (noting that the vertical accuracy information is typically collected for 911 triangulation purposes. It is unclear how this data is shared, but there is the distinct possibility that it was sold pre-2022).

[3] *Riley v. California*, 573 U.S. 373, 385 (2014).

[4] Exec. Order No. 14093, 88 Fed. Reg. 18957, 18962 § 5(b) (Mar. 27, 2023) [hereinafter "Spyware Exec. Order"].

[5] Amnesty Int'l, *Forensic Methodology Report: How to catch NSO Group's Pegasus* (Jul. 18, 2021), https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/ [hereinafter "Amnesty FMR"].

[6] Op. & Order, *Alhathloul v. DarkMatter Grp.*, No. 3:21-cv-01787-IM (D. Or. Aug 12, 2025), https://www.eff.org/document/alhathloul-v-darkmatter-opinion-and-order-motion-dismiss.

[7] *Case Study: The Predator Files,* Amnesty Int'l. (Oct. 2023), https://securitylab.amnesty.org/case-study-the-predator-files/.

[8] Bill Marczak et al., *Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations,* Citizen Lab (Mar. 19, 2025), https://citizenlab.ca/2025/03/a-first-look-at-paragons-proliferating-spyware-operations/ [hereinafter "Virtue or Vice?"].

[9] *"A Digital Prison:" Surveillance and the Suppression of Civil Society in Serbia,* Amnesty Int'l. (Dec. 16, 2024), https://www.amnesty.org/en/latest/news/2024/12/serbia-authorities-using-spyware-and-cellebrite-forensic-extraction-tools-to-hack-journalists-and-activists/.

[10] Bill Marczak et al., *Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*, Citizen Lab (Jul. 15, 2021), https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/.

[11] Bill Marczak et al., *Hacking Team and the Targeting of Ethiopian Journalists*, Citizen Lab (Feb. 12, 2014), https://citizenlab.ca/2014/02/hacking-team-targeting-ethiopian-journalists [hereinafter "Hacking Team"].

[12] *Pegasus – Product Description*, DocumentCloud, https://embed.documentcloud.org/documents/4599753-NSO-Pegasus/ (linked from Amnesty FMR *supra* note 5).

[13] N.J. Cybersecurity & Commc'ns Integration Cell, *The Future of Malware Exploit: Zero-Click Attacks* (May 9, 2024), https://www.cyber.nj.gov/Home/Components/News/News/1315/214; Bill Marczak & John Scott-Railton, *Graphite Caught: First Forensic Confirmation of Paragon's iOS Mercenary Spyware Finds Journalists Targeted*, Citizen Lab (Jun. 12, 2025), https://citizenlab.ca/2025/06/first-forensic-confirmation-of-paragons-ios-mercenary-spyware-finds-journalists-targeted/ [hereinafter "Graphite Caught"].

[14] *See, e.g.*, Press Release, Apple, *Apple sues NSO Group to curb the abuse of state-sponsored spyware* (Nov. 23, 2021), https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/; Nicole Perlroth, *WhatsApp Says Israeli Firm Used Its App in Spy Program*, N.Y. Times (updated Jan. 15, 2021), https://www.nytimes.com/2019/10/29/technology/whatsapp-nso-lawsuit.html.

[15] *Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools,* Amnesty Int'l. (Jun. 22, 2020), https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/.

[16] Joseph Cox, *The DEA Didn't Buy Malware From Israel's Controversial NSO Group Because It Was Too Expensive*, VICE (Sept. 11, 2019), https://www.vice.com/en/article/dea-didnt-buy-malware-nso-group-too-expensive/.

[17] Social engineering is the act of "deceiving an individual into revealing sensitive information . . . or committing fraud by associating with the individual to gain confidence and trust." *Social engineering*, Glossary, NIST Comput. Sec. Res. Ctr., https://csrc.nist.gov/glossary/term/social_engineering (last visited Oct. 31, 2025).

[18] Phishing is a digital form of social engineering, where an entity sends "a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person" in an attempt to gain sensitive information such as account information. *Phishing*, Glossary, NIST Comput. Sec. Res. Ctr., https://csrc.nist.gov/glossary/term/phishing (last visited Oct. 31, 2025).

[19] *Avoiding Social Engineering and Phishing Attacks*, CISA Blog (Feb. 1, 2021), https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks; *see also*, *Spyware Detection and Analysis: Methodologies Limitations and Future Directions*, Internet Research Lab (Mar. 19, 2025), https://irl.works/blog/2025/03/19/spyware-detection-analysis.html; *Malvertising*, Malwarebytes, https://www.malwarebytes.com/malvertising (last visited Oct. 24, 2025).

[20] *Working Paper on Large Language Models (LLMs),* Int'l. Working Grp. on Data Prot. in Tech. (Dec. 27, 2024), https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20241206-WP-LLMs.html?nn=253562.

[21] *See* Ravit Dotan, *What AI agents really are and why system prompts are more important*, Substack: AI Treasure Chest (Sept. 18, 2025), https://techbetter.substack.com/p/what-ai-agents-really-are-and-why; *see also* Yam Atir, *The Rise of Agentic AI*, Belfer Ctr. (Jun. 2025), https://www.belfercenter.org/research-analysis/rise-agentic-ai-infrastructure-autonomy-and-americas-cyber-future.

[22] Agentic Browser Security: Indirect Prompt Injection in Perplexity Comet, Brave (Aug. 20, 2025), https://brave.com/blog/comet-prompt-injection/; *see also* Lukas Aichberger et al., *Attacking Multimodal OS Agents with Malicious Image Patches*, arXiv preprint arXiv:2503.10809 (Mar. 13, 2025), https://arxiv.org/pdf/2503.10809.

[23] *Spyware and State Abuse: The Case for an EU-Wide Ban,* EDRi 8 (Jun. 2025), https://edri.org/wp-content/uploads/2025/06/EDRi_Spyware-position-paper.pdf; *see also,* Joseph Cox, *NSO Group Pitched Phone-Hacking Tech to American Police*, VICE (May 12, 2020), https://www.vice.com/en/article/nso-group-pitched-phone-hacking-tech-american-police; Joseph Cox, *NSO Group Pitched Its Spyware to the Secret Service*, VICE (Jul. 23, 2020) (includes a brochure for NSO Group's Pegasus), https://www.vice.com/en/article/nso-group-pitched-its-spyware-to-the-secret-service; Bill Marczak et al., *Hacking Team and the Targeting of Ethiopian Journalists*, Citizen Lab (Feb. 12, 2014), https://citizenlab.ca/2014/02/hacking-team-targeting-ethiopian-journalists (includes a brochure for Hacking Team's Remote Control System).

[24] Compl., *Dada et al., v. NSO Grp. Techs. Ltd.*, No. 5:22-CV-07513-JD, at 27 (N.D. Cal. Nov. 30, 2022).

[25] Natalia Krapiva & Hinako Sugiyama, *What spy firm Cellebrite can't hide from investors*, Access Now (updated Jan. 13, 2023), https://www.accessnow.org/what-spy-firm-cellebrite-cant-hide-from-investors/; *EPIC v. ICE (Mobile Forensics)*, EPIC, https://epic.org/documents/epic-v-ice-mobile-forensics/ (last updated Mar. 19, 2019).

[26] Magnet Forensics, *Magnet Graykey*, https://www.magnetforensics.com/products/magnet-graykey/ (Last visited Oct. 31, 2025).

[27] Zach Campbell & Lorenzo D'Agostino, *How the EU supplied Morocco with phone-hacking spyware*, Disclose (Jul. 25, 2022), https://disclose.ngo/en/article/how-the-eu-supplied-morocco-with-phone-hacking-spyware.

[28] *Cellebrite Statement About Amnesty International Report,* Cellebrite (updated Feb. 25, 2025), https://cellebrite.com/en/cellebrite-statement-about-amnesty-international-report/ (Cellebrite claims that it does not do real time continuous monitoring though generally there is limited transparency around such tools.).

[29] *Id.*

[30] Press Release, FTC, *FTC Bans SpyFone and CEO from Surveillance Business and Orders Company to Delete All Secretly Stolen Data* (Sept. 1, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-bans-spyfone-ceo-surveillance-business-orders-company-delete-all-secretly-stolen-data [hereinafter "FTC Bans SpyFone"].

[31] Zack Whittaker, *Data Breach Reveals Catwatchful 'Stalkerware' is Spying on Thousands of Phones*, TechCrunch (Jul. 2, 2025), https://techcrunch.com/2025/07/02/data-breach-reveals-catwatchful-stalkerware-spying-on-thousands-android-phones/.

[32] The Best Phone Tracker for Parental Control, mSpy, https://www.mspy.com (last visited Oct. 31, 2025); see also Pieter Arntz, Dangerous Monitoring Tool mSpy Suffers Data Breach, Exposes Customer Details, Malwarebytes Labs (Jul. 12, 2024), https://www.malwarebytes.com/blog/news/2024/07/dangerous-monitoring-tool-mspy-suffers-data-breach-exposes-customer-details.

[33] *The World's Most Powerful Monitoring Software for Computers, Mobile Phones and Tablets,* FlexiSPY, https://www.flexispy.com; *see also Why Choose FlexiSPY,* FlexiSPY, https://www.flexispy.com/en/why-choose-flexispy.htm; Joseph Cox, *Meet FlexiSPY, The Company Getting Rich Selling 'Stalkerware' to Jealous Lovers,* VICE (Apr. 21, 2017), https://www.vice.com/en/article/meet-flexispy-the-company-getting-rich-selling-stalkerware-to-jealous-lovers.

[34] *FTC Bans SpyFone, supra* note 30.

[35] *Stalkerware: Phone Surveillance & Safety for Survivors*, Nat'l. Network to End Domestic Violence Tech Safety Project, https://www.techsafety.org/spyware-and-stalkerware-phone-surveillance.

[36] *See, e.g.*, *FlexiSPY*, https://www.flexispy.com.

[37] It is not confirmed that ICE's contract is for Graphite, specifically. It is unclear what other Paragon product ICE would be acquiring, though. Jack Poulson, *Exclusive: ICE Reactivated its $2 million Contract With Israeli Spyware Firm Paragon, Following its Acquisition by U.S. capital*, Substack: All-Source Intelligence (Sept. 1, 2025), https://jackpoulson.substack.com/p/exclusive-ice-has-reactivated-its.

[38] *See Letter Regarding NSO Group Pegasus Program*, FBI: 22-cv-1539-309 at 13 (Dec. 4, 2018), https://int.nyt.com/data/documenttools/fbi-nso-pegasus-foia/0d5bfa4c062e32d0/full.pdf; *see also* Mark Mazzetti & Ronen Bergman, *A Front Company and a Fake Identity: How the U.S. Came to Use Spyware It Was Trying to Kill.*, N.Y. Times (Apr. 2, 2023), https://www.nytimes.com/2023/04/02/us/politics/nso-contract-us-spy.html; *see also* EPIC, *EPIC Seeks Records on Federal Government's Connections to Hacking Firm NSO Group* (Oct. 30, 2021), https://epic.org/epic-seeks-records-on-federal-governments-connections-to-hacking-firm-nso-group/.

[39] Addition of Certain Entities to the Entity List, 86 Fed. Reg. 60759, 61993 (Nov. 4, 2021), https://www.federalregister.gov/documents/2021/11/04/2021-24123/addition-of-certain-entities-to-the-entity-list.

[40] Mazzetti & Bergman, *supra* note 38.

[41] Khashoggi's phone was turned over to Turkish authorities before it could be analyzed, so it cannot be confirmed or denied whether his personal devices were targeted by spyware. Both his wife and a fellow Saudi Activist, Omar Abdulaziz, were targeted with NSO Group's flagship product in the time period before the extrajudicial torture and killing of Khashoggi. *See, e.g.*. Bill Marczak, et al., *The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil* (Oct. 2018), https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil; Compl., *Khashoggi v. NSO Group et al.*, Civil Action No. 1:23-cv-779 (E.D. Va. Jun. 15, 2023) (the widow of Jamal Khashoggi providing evidence of a Pegasus infection on her device); Press Release, *Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally*, Amnesty Int'l. (Jul. 19, 2021), https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/ [hereinafter "NSO Data Leak"] (other family members of Khashoggi also targeted); David D. Kirkpatrick, *Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says*, N.Y. Times (Dec. 2, 2018), https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html.

[42] Letter from Eleftherios Chelioudakis, Executive Director, Homo Digitalis, to Michael O'Flaherty, Commissioner for Human Rights, Council of Europe (Aug. 13, 2024), https://homodigitalis.gr/en/posts/133506/; *see also*, *Greece's surveillance scandal must shake us out of complacency*, Amnesty Int'l. (Jan. 26, 2023), https://www.amnesty.org/en/latest/news/2023/01/greeces-surveillance-scandal-must-shake-us-out-of-complacency/.

[43] Janko Marković, *Revealing NoviSpy: Technical Analysis of a Serbian Android Spyware*, SHARE Fondacija (May 29, 2025), https://sharefoundation.info/en/revealing-novispy-technical-analysis-of-a-serbian-android-spyware/; *see also, Serbia: Civil Society Threatened by Spyware,* Amnesty Int'l (Nov. 28, 2023), https://securitylab.amnesty.org/latest/2023/11/serbia-civil-society-threatened-by-spyware/.

[44] John Scott-Railton, et al., *Citizen Lab*, *New Pegasus Spyware Abuses Identified in Mexico* (Oct. 2, 2022), https://citizenlab.ca/2022/10/new-pegasus-spyware-abuses-identified-in-mexico/.

[45] *Virtue or Vice? supra* note 8; *see also Graphite Caught*, *supra* note 13.

[46] *India: Damning new forensic investigation reveals repeated use of Pegasus spyware to target high-profile journalists,* Amnesty Int'l. (Dec. 28, 2023), https://www.amnesty.org/en/latest/news/2023/12/india-damning-new-forensic-investigation-reveals-repeated-use-of-pegasus-spyware-to-target-high-profile-journalists/.

[47] Surveillance Watch, https://www.surveillancewatch.io/?menu=entities (last visited Jul. 25, 2025) (Surveillance Watch tracks monetary transactions between governments and spyware companies, indicating other possible deployers).

[48] *Virtue or Vice?, supra* note 8.

[49] *See* Shawn Musgrave, *Hacking Team Had Ties to Local Police Departments Across the U.S.*, VICE (Jul. 23, 2015), https://www.vice.com/en/article/hacking-team-had-ties-to-local-police-departments-across-the-us; Shawn Musgrave, *Hacking Team Gave Spyware Demos to Police Agencies Across the Nation*, VICE (Jul. 29, 2015), https://www.vice.com/en/article/hacking-team-gave-spyware-demos-to-police-agencies-across-the-nation.

[50] Neil Richards, *Why Privacy Matters* 143 (Oxford Univ. Press 2022).

[51] *Id.*

[52] *Id.*; Notably, FBI penned letter to Martin Luther King suggesting he kill himself and threatened to reveal information about his infidelity which they learned of through surveillance. Sam Briger, *Documentary Exposes How The FBI Tried To Destroy MLK With Wiretaps, Blackmail*, NPR (Jan. 18, 2021), https://www.npr.org/2021/01/18/956741992/documentary-exposes-how-the-fbi-tried-to-destroy-mlk-with-wiretaps-blackmail; The NSA had a surveillance program aimed explicitly at monitoring targets' online porn consumption habits to be able to later discredit them. *Echoing Dirty Past, NSA Sought to Reveal Porn Habits to Discredit Targets*, ACLU (Nov. 27, 2013), https://www.aclu.org/news/national-security/echoing-dirty-past-nsa-sought-reveal-porn-habits-discredit-targets; Neil Richards, *The Dangers of Surveillance*, 126 *Harv. L. Rev.* 1934 (2013).

[53] *See generally, Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem*, EPIC 7-12 (Nov. 2022), https://epic.org/ftc-rulemaking-on-commercial-surveillance-data-security/.

[54] *See, e.g.,* 'The Great Hack': Cambridge Analytica is Just the Tip of the Iceberg, Amnesty Int'l. (Jul. 24, 2019), https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/.

[55] Richards, *supra* note 50 at 144.

[56] *Id.* at 145.

[57] Jonathan W. Penney, *Chilling Effects* (Cambridge Univ. Press, forthcoming 2026) (on file with author).

[58] *The FBI's War on King - King's FBI File*, APM Reports, https://features.apmreports.org/arw/king/d1.html#:~:text=Beginning%20in%201962%2C%20the%20FBI,journalists%2C%20church%20leaders%20and%20others (Last visited Oct. 31, 2025).

[59] Richards, *supra* note 50 at 140.

[60] *See, e.g.,* EPIC, *About Edward Snowden*, https://archive.epic.org/privacy/nsa/snowden/ (last visited Oct. 31, 2025); *see also* Luke Harding, *The Snowden Files: The Inside Story of the World's Most Wanted Man,* 171 et seq. *(*Random House LLC 2014) (describing the media firestorm and international political outrage following the publishing of the Snowden stories); Glenn Greenwald et al., *Edward Snowden: the Whistleblower Behind the NSA Surveillance Revelations*, The Guardian (Jun. 11, 2013), https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

[61] Richards, *supra* note 50 at 126; see also Jeramie Scott, Social Media and Government Surveillance: The Case for Better Privacy Protections for Our Newest Public Space, 12 J. Bus. & Tech. L. 157 (2017).

[62] Elizabeth Stoycheff, Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring, 93 Journalism & Mass Commc'n Q. 296 (Mar. 8, 2016), https://journals.sagepub.com/doi/abs/10.1177/1077699016630255; Lee Rainie & Mary Madden, Americans' Privacy Strategies Post-Snowden, Pew Rsch. Ctr. (Mar. 16, 2015), https://www.pewresearch.org/internet/2015/03/16/americans-privacy-strategies-post-snowden/.

[63] Penney, *supra* note 57 at 23.

[64] *Id.* at 26 et seq.

[65] *See*, *With Liberty to Monitor All: How Large-Scale U.S. Surveillance Is Harming Journalism, Law, and American Democracy,* Hum. Rts. Watch 3–5 (2014), https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and; *see also, ACLU v. Nat'l Sec. Agency*, 493 F.3d 644, 696 (6th Cir. 2007) (Gilman, J., dissenting) (discussing the chilling effect of surveillance on attorney-plaintiffs); *see also*, *Journalist on the Move?*, Electronic Frontier Found. Surveillance Self-Defense, https://ssd.eff.org/playlist/journalist-on-the-move (last visited Oct. 31, 2025); *Leak to us*, Int'l Consortium of Investigative Journalists, https://www.icij.org/leak/ (last visited Oct. 31, 2025); *see also* Harding *supra* note 60 at 61-83, 106-125 (describing the extensive security measures Edward Snowden took to contact Glenn Greenwald and Laura Poitras, including requesting they install PGP encryption on his computer before discussing any sensitive information, creating opaque barriers between computers and the rest of the room when entering passwords by wearing a dark red hood, and requesting that Greenwald, Poitras, and their teams meet him in a hotel in Hong Kong).

[66] Jamie Schuman, *The NSA's Shadow*, Rep.s Comm. for Freedom of the Press (2014), https://www.rcfp.org/journals/news-media-and-law-winter-2014/nsas-shadow/; Geoffrey King, *The NSA Puts Journalists Under a Cloud of Suspicion,* Comm. to Prot. Journalists (Feb. 2014), https://cpj.org/2014/02/attacks-on-the-press-surveillance-storage/.

[67] William J. Cuddihy, *The Fourth Amendment: Origins and Original Meaning,* 602–435 (Oxford Univ. Press 2009).

[68] *Id.*

[69] *See Griswold v. Connecticut,* 381 U.S. 479, 483 (1965) ("[T]he First Amendment has a penumbra where privacy is protected from governmental intrusion.").

[70] U.S. Const. amend. IV.

[71] *Katz v. United States,* 389 U.S. 347, 360-61 (1967).

[72] Wayne R. Lafave et al., *Criminal Procedure* (7th ed. 2025).

[73] Stephen Perez Jr., *Immigration & the Fourth Amendment*, Restore the Fourth (Apr. 10, 2025), https://restorethe4th.com/immigration-the-fourth-amendment/ (citing *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990)) (noting that the Fourth Amendment applies to anyone within the geographical borders of the United States. The protection under the Fourth Amendment is not limited to citizens or those with "lawful" immigration status. This does mean, though, that the Fourth Amendment does not typically apply to government surveillance outside of U.S. boundaries, such as an intelligence or law enforcement agency using spyware to target a foreign individual abroad.); *but see,* Jonathan Mayer, *Government Hacking*, 127 Yale L.J. 570 (2018) (noting that the courts are divided over whether government hacking should be considered a search under the Fourth Amendment, and that federal agencies have a spotty record in complying with procedural requirements).

[74] Exec. Order 12333, 46 Fed. Reg. 59941 (1981); *see also, Executive Order 12333,* EPIC, https://epic.org/executive-order-12333/ (last visited Oct. 31, 2025).

[75] *United States v. U.S. District Court (Keith),* 407 U.S. 297, 320 (1972) [hereinafter "Keith Case"]. ("Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent.").

[76]Andrew Guthrie Ferguson, *Digital Rummaging,* 101 Wash. Univ. L. Rev. 1473 (2024) [hereinafter "Digital Rummaging"]; Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment,* 102 Cornell L. Rev. 547, 604 (2017) (defining "informational security" as "personal information that is secured in some manner from governmental intrusion").

[77] *Id.* at 1515-18.

[78] *Id.*

[79] *Carpenter v. United States*, 585 U.S. 296, 310 (2018) (citing *Riley v. California*, 573 U.S. 373 (2014)).

[80] *Riley,* 573 U.S. 373 at 403.

[81] Ian Walsh, *Revising Reasonableness in the Cloud*, 96 Wash. L. Rev. 117, 121–23 (2021).

[82] FCC, *Indoor Location Accuracy Timeline and Live Call Data Reporting Template* (Jul. 26, 2021), https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/911-services/general/location-accuracy-indoor-benchmarks (noting that the vertical accuracy information is typically collected for 911 triangulation purposes. It is unclear how this data is shared, but there is the distinct possibility that it was sold pre-2022).

[83] Susan Landau, *Location Surveillance to Counter COVID-19: Efficacy Is What Matters*, Lawfare (Mar. 27, 2020), https://www.lawfaremedia.org/article/location-surveillance-counter-covid-19-efficacy-what-matters.

[84] *Carpenter,* 585 U.S. at 301. This is notable because *Carpenter's* ruling pushed back against the third party doctrine, which held that there is no reasonable expectation of privacy in data that has been shared with third parties. *Carpenter* held that even if CSLI data is in possession of the mobile carriers (a third party), there is still a reasonable expectation in long term location data.

[85] *Digital Rummaging, supra* note 76 at 1510.

[86] *Id.*

[87] *Id.*

[88] *Id.*

[89] *Id.*

[90] Cuddihy, *supra* note 67.

[91] *See, e.g.,* EPIC*, EPIC v. Ice (Palantir Databases)*, https://epic.org/documents/epic-v-ice-palantir-databases/.

[92] *Riley v. California*, 573 U.S. 373 (2014); *Carpenter v. United States*, 138 S. Ct. 2206 (2018); *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

[93] Electronic Communications Privacy Act of 1986 (ECPA) 18 U.S.C. §§ 2510-2523 [hereinafter "ECPA"].

[94] 18 U.S.C. § 2701.

[95] *See* ECPA *supra* note 93; *see also* Stored Communications Act (SCA) 18 U.S.C. § 2701.

[96] *United States v. Jones*, 565 U.S. 400 (2012) (finding that attaching a physical GPS tracker to a car for 28 days was a search under the Fourth Amendment and requires a probable cause warrant).

[97] 18 U.S.C. § 2518.

[98] 18 U.S.C. § 2518(1)(c).

[99] EPIC, *Foreign Intelligence Surveillance Court (FISC)*, https://epic.org/foreign-intelligence-surveillance-court-fisc/ (last visited Oct. 31, 2025).

[100] EPIC, *FISA Court Statistics*, https://epic.org/foreign-intelligence-surveillance-court-fisc/fisa-stats/ (last visited Oct. 31, 2025).

[101] EPIC, *FISA Section 702: Reform or Sunset*, https://epic.org/campaigns/fisa-section-702-reform-or-sunset/ (last visited Oct. 31, 2025).

[102] 50 U.S.C. § 1881a.

[103] EPIC, *Surveillance Court Finds FBI Repeatedly Misused FISA Program to Conduct Unlawful Surveillance of Americans* (Apr. 29, 2021), https://epic.org/surveillance-court-finds-fbi-repeatedly-misused-fisa-program-to-conduct-unlawful-surveillance-of-americans/.

[104] *EPIC, supra* note 99.

[105] USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268.

[106] EPIC, *supra* note 100 (linking to all publicly available FISC court orders).

[107] While the Freedom Act of 2015 required FISC to appoint an amicus curiae on complex and significant legal issues, the court has discretion over whether that is appropriate.

[108] EPIC, *supra* note 101.

[109] EPIC, *Title III Wiretap Orders Stats*, https://epic.org/title-iii-wiretap-orders-stats/ (last visited Oct. 31, 2025).

[110] U.S. Const. amend. IV.

[111] Berger v. New York, 388 U.S. 41 (1967); see also Alan Butler, Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure before the Judicial Conference Advisory Committee on Criminal Rules (Nov. 5, 2014), https://archive.epic.org/privacy/surveillance/remote-access/EPIC-FRCP-Rule-41-Amendments-Testimony.pdf.

[112] *See* Title III of the Omnibus Crime Control and Safe Streets Act of 1968*; see also* H.R. Rep. No. 104-518 (1996).

[113] S. Rep. No. 99-541 (1986).

[114] *Infra* Part I, Section 4. Legal Redress for Spyware Abuses Faces Significant Barriers.

[115] *In re EPIC,* 571 U.S. 1023 (2013) (pet. denied); *see also* Adam Liptak, *Justices Reject Challenge to N.S.A. Program*, N.Y. Times (Nov. 18, 2013), https://www.nytimes.com/2013/11/19/us/justices-reject-challenge-to-nsa-program.html.

[116] *See, e.g.*, *Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013); *Klayman v. Obama*, No. 14-5004 (D.C. Cir. 2015).

[117] Kelsey Cora Skaggs, Surveilling Speech and Association: NSA Surveillance Programs and the First Amendment, Am. Const. Soc'y Sup. Ct. Rev. 1479, 1486 (2016); accord Ana Pajar Blinder, Don't (Tower) Dump on Freedom of Association: Protest Surveillance Under the First and Fourth Amendments, 111 J. Crim. L. & Criminology 799 (2021), https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=7709&context=jclc; Alex Abdo, Why Rely on the Fourth Amendment to Do the Work of the First?, 127 Yale L.J. F. 444 (Oct. 25, 2017), https://www.yalelawjournal.org/forum/why-rely-on-the-fourth-amendment-to-do-the-work-of-the-first.

[118] *Supra* note 92.

[119] *Supra* note 117.

[120] U.S. Const. amend. I (emphasis added).

[121] *See, e.g.,* Megan Iorio, *NetChoice v. Bonta: The Case That Threatens the Future of Privacy*, EPIC (Oct. 19, 2023), https://epic.org/netchoice-v-bontathe-case-that-couldthreaten-the-future-of-privacy/ (describing the way First Amendment law works*); see also* Abdo *supra* note 117.

[122] *Id.*

[123] *Id.*

[124] *Id.*

[125] Skaggs, *supra* note 117.

[126] *NAACP v. Alabama*, 357 U.S. 449 (1958).

[127]Palash Volvoikar, *Think About Buying a Burner Phone When You Get Your Holiday Tickets This Year*, CNET (Oct. 17, 2025), https://www.cnet.com/tech/mobile/think-about-buying-a-burner-phone-when-you-get-your-holiday-tickets-this-year/.

[128] Penney, *supra* note 57, at 51 et seq.

[129] *Id.* at 52 (citing Fritz J. Roethlisberger & William J. Dickson, *Management and the Worker* (1939)).

[130] *Id.*

[131] *Id.* at 53 (quoting Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Penn. L. Rev. 477, 487 (2006)).

[132] *See, e.g.*, Joseph Cox, *Hacking Team Is Back with a Bold Pitch to Police*, Vice (Oct. 6, 2022), https://www.vice.com/en/article/hacking-team-is-back-with-a-bold-pitch-to-police (calling out advertising material of a spyware developer that notes its technology can defeat criminals using encryption and other technology that evade law enforcement); The EU is also using this erroneous justification to expand the data retention requirements of telecommunication companies regarding customer communications based on the fact that terrorists and criminals are using encryption. This approach would collect data from everyone in the EU, not just those criminals they aim to investigate and root out. to find only a tiny fraction of a the perceived them and lead to "insecurity by design." *Shedding Light: We Address the Flawed "Going Dark" Report*, Eur. Digit. Rights (EDRi) (Jan. 2024), https://edri.org/our-work/shedding-light-we-address-the-flawed-going-dark-report/.

[133] *See, e.g.*, Memorandum on Countering Domestic Terrorism and Organized Political Violence, White House (Sept. 25, 2025), https://www.whitehouse.gov/presidential-actions/2025/09/countering-domestic-terrorism-and-organized-political-violence/; Exec. Order, Designating Antifa as a Domestic Terrorist Organization, 90 Fed. Reg. 46317 (Sept. 25, 2025).

[134] *See* Stephanie Wade et al., *Gov. J.B. Pritzker Addresses Trump's Effort to Deploy National Guard in Illinois; Pentagon Authorizes Chicago Mission*, ABC7 Chicago (May 31, 2025), https://abc7chicago.com/post/gov-jb-pritzker-address-trumps-effort-deploy-national-guard-illinois-pentagon-authorizes-chicago-mission/17949147/;
Joseph Cox, *WSJ Reporter: Homeland Security Tried to Take My Phones at the Border*, VICE Motherboard (Jul. 21, 2016), https://perma.cc/BMN9-96LW; *Civil Rights & Civil Liberties Complaint Closure* (Jul. 11, 2017), *Knight First Amendment Inst. at Columbia Univ.*, https://perma.cc/2GDA-F7G6; Alex Nowrasteh, *The Trump Administration Shouldn't Designate Drug Cartels as Foreign Terrorist Organizations*, Cato Inst. (Feb. 5, 2025), https://www.cato.org/blog/trump-administration-shouldnt-designate-drug-cartels-foreign-terrorist-organizations; Exec. Order 14235, 90 Fed. Reg. 11885 (Mar. 7, 2025); Press Release, U.S. Dep't of Just., *Attorney General William P. Barr's Statement on the Death of George Floyd and Riots* (May 30, 2020), https://www.justice.gov/opa/pr/attorney-general-william-p-barr-s-statement-death-george-floyd-and-riots.

[135] *See, e.g., NSO Data Leak supra* note 41.

[136] *NAACP*, 357 U.S. 449.

[137] *See, e.g.,* United States v. U.S. District Court (Keith), 407 U.S. 297, 320 (1972) [hereinafter "Keith Case"].

[138] Aldera Alotaibi, *Digital Dictatorship: The Psychological Impact of State-Sponsored Cyberattacks on Gulf Cooperation Council Dissidents* (2024), https://etheses.whiterose.ac.uk/id/eprint/37331/1/Digital%20Dictatorship%20The%20Psychological%20Impact%20of%20State-Sponsored%20Cyberattacks%20on%20Gulf%20Corporation%20Council%20Dissidents.pdf.

[139] *Id.* at 51.

[140] *Id.* at 55.

[141] *Id.* at 58.

[142] *Id.* at 59.

[143] *Id.* at 71.

[144] *Id.* at 63.

[145] *Id.* at 62.

[146] *See, e.g.,* Pegasus Project: Rwandan Authorities Chose Thousands of Activists, Journalists and Politicians to Target with NSO Spyware, Amnesty Int'l (Jul. 2021), https://securitylab.amnesty.org/latest/2021/07/rwandan-authorities-chose-thousands-of-activists-journalists-and-politicians-to-target-with-nso-spyware/; Bill Marczak et al., The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil (Oct. 2018), https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/; Patrick Kingsley and Ronan Bergman, Israel Investigates Pegasus Spyware after Reports of Misuse, N.Y. Times (Feb. 7, 2022), https://www.nytimes.com/2022/02/07/world/middleeast/israel-pegasus-spyware.html.

[147] *Ashcroft v. Iqbal*, 556 U.S. 662 (2009) (acknowledging stricter standing requirements for plaintiffs).

[148] *Amnesty Int'l USA v. Clapper*, 638 F.3d 118 (2d Cir. 2011).

[149] *In re EPIC*, *supra* note 115.

[150] *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015).

[151]Press Release, Udall, Wyden, Heinrich Urge Solicitor General to Set Record Straight on Misrepresentations to U.S. Supreme Court in Clapper v. Amnesty (Nov. 21, 2013), https://www.wyden.senate.gov/news/press-releases/udall-wyden-heinrich-urge-solicitor-general-to-set-record-straight-on-misrepresentations-to-us-supreme-court-in-clapper-v-amnesty.

[152] *Id.*

[153] *E.g.*, EPIC submitted a FOIA request regarding the federal government's use of Pegasus/Phantom spyware but never received a reply. EPIC, *EPIC Seeks Records on Federal Government's Connections to Hacking Firm NSO Group* (Oct. 30, 2021), https://epic.org/epic-seeks-records-on-federal-governments-connections-to-hacking-firm-nso-group/.

[154] *See, e.g., How to Protect Your Account*, WhatsApp Help Center, https://faq.whatsapp.com/641700318302674; *If You Think Your iPhone Is Hacked*, Apple Support, https://support.apple.com/en-us/102174; Access Now, *Digital Security Helpline*, https://www.accessnow.org/help/; Amnesty Int'l, *Get Help*, https://securitylab.amnesty.org/get-help/.

[155] Bennett Cyphers, *Privileged Methods, Parallel Construction: How Government Secrecy Undermines the Fourth Amendment*, Lawfare (Apr. 23, 2018), https://www.lawfaremedia.org/article/newly-disclosed-documents-five-eyes-alliance-and-what-they-tell-us-about-intelligence-sharing.

[156] *Id.*

[157] Scarlet Kim et al., *Newly Disclosed Documents on the Five Eyes Alliance and What They Tell Us about Intelligence-Sharing Agreements* (Apr. 25, 2018), https://law.yale.edu/mfia/case-disclosed/newly-disclosed-documents-five-eyes-alliance-and-what-they-tell-us-about-intelligence-sharing; *see also*, James Ball, *US and UK struck secret deal to allow NSA to 'unmask' Britons' Personal Data*, The Guardian (Nov. 20, 2013), https://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data.

[158] *See* Spyware Executive Order, *supra* note 4; *see infra* Part I, Section 6. The U.S. Has Begun to Make Progress on the Federal Level.

[159] *Mathews v. Eldridge,* 424 U.S. 319 (1976).

[160] *Morrissey v. Brewer*, 408 U.S. 471, 481 (1972).

[161] Stephanie Kirchgaessner, *Ice Obtains Access to Israeli-made Spyware that Can Hack Phones and Encrypted Apps*, The Guardian (Sept. 2, 2025), https://www.theguardian.com/us-news/2025/sep/02/trump-immigration-ice-israeli-spyware; Ronen Bergman & Mark Mazzetti, *The Battle for the World's Most Powerful Cyberweapon*, N.Y. Times (Jan. 28, 2022), https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html; *see also Proliferation of Foreign Commercial Spyware Drives Increasing Counterintelligence Risk*, Cyber Threat Intel. Integration Ctr. (Dec. 2023), https://www.dni.gov/files/CTIIC/documents/products/Proliferation_of_Foreign_Commercial_Spyware_Drives_Increasing_Counterintelligence_Risk.pdf; Spyware Executive Order, *supra* note 4.

[162] *See, e.g.,* EPIC, *Encryption*, https://epic.org/issues/cybersecurity/encryption; *see also* EPIC, *EPIC Leads Civil Society Support for Post-Salt Typhoon FCC Cybersecurity Order* (Aug. 3, 2025), https://epic.org/epic-leads-civil-society-support-for-post-salt-typhoon-fcc-cybersecurity-order/; EPIC, *Data Retention*, https://epic.org/data-retention/.

[163] Amy Gaudon, *It's Time to Reform the U.S. Vulnerabilities Equities Process*, War Room (Sept. 2, 2021), https://warroom.armywarcollege.edu/articles/vep/.

[164] *Vulnerabilities Equities Policy and Process for the United States Government* (Nov. 15, 2017), https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF; While the document was published under the Trump Administration in 2017, the work began far earlier in the Obama administration. Michael Daniel, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities*, The White House Blog (Apr. 28, 2014), https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

[165] *See* 50 U.S.C. § 3316a.

[166] Gaudon, *supra* note 163.

[167] Josh Kenway & Michael Garcia, *To Patch or Not to Patch: Improving the US Vulnerabilities Equities Process*, Third Way (Jun. 1, 2021), https://www.thirdway.org/memo/to-patch-or-not-to-patch-improving-the-us-vulnerabilities-equities-process.

[168] *See, e.g., BLASTPASS: NSO Group iPhone Zero-Click, Zero-Day Exploit Captured in the Wild*, Citizen Lab (Sept. 7, 2023), https://citizenlab.ca/2023/09/blastpass-nso-group-iphone-zero-click-zero-day-exploit-captured-in-the-wild/.

[169] *See, e.g.,* Erika Kinetz & Paolo Santalucia, *US-backed Israeli Company's Spyware Used to Target European Journalists, Citizen Lab Finds*, Assoc. Press (Jun. 12, 2025), https://www.ap.org/news-highlights/spotlights/2025/us-backed-israeli-companys-spyware-used-to-target-european-journalists-citizen-lab-finds/ (referencing Paragon's claims that that it is an ethical company because of its US affiliation).

[170] See Privacy. That's Apple., Apple, https://www.apple.com/privacy/ (last visited Oct. 31, 2025); see also NSO Group Liable Under CFAA For Hacking WhatsApp Servers, NSO Attorneys Sanctioned For Discovery Misconduct, EPIC (Dec. 23, 2024), https://epic.org/nso-group-liable-under-cfaa-for-hacking-WhatsApp-servers-nso-attorneys-sanctioned-for-discovery-misconduct/.

[171] *See, e.g.,* Christopher Bing & Joseph Menn, *U.S. State Department Phones Hacked with Israeli Company Spyware-Sources*, Reuters (Dec. 3, 2021), https://www.reuters.com/technology/exclusive-us-state-department-phones-hacked-with-israeli-company-spyware-sources-2021-12-03; Filip Truță, *U.S. State Department iPhones Infected with Pegasus Spyware-Report,* Bitdefender Labs (Dec. 6, 2021), https://www.bitdefender.com/en-us/blog/hotforsecurity/us-state-department-iphones-infected-with-pegasus-spyware-report.

[172] *Global: 'Predator Files' Spyware Scandal Reveals Brazen Targeting of Civil Society, Politicians, and Officials,* Amnesty Int'l. (Oct. 9, 2023), https://www.amnesty.org/en/latest/news/2023/10/global-predator-files-spyware-scandal-reveals-brazen-targeting-of-civil-society-politicians-and-officials/.

[173] Sam Jones, S*panish prime minister's phone 'targeted with Pegasus spyware,'* The Guardian (May 2, 2022), https://www.theguardian.com/world/2022/may/02/spain-prime-minister-pedro-sanchez-phone-pegasus-spyware; *Pegasus Project: Macron among world leaders selected as potential targets of NSO spyware,* Amnesty Int'l. (Jul. 20, 2021), https://www.amnesty.org/en/latest/press-release/2021/07/world-leaders-potential-targets-of-nso-group-pegasus-spyware.

[174] *See* Ronen Bergman & Mark Mazzetti, *The Battle for the World's Most Powerful Cyberweapon,* N.Y. Times Mag. (updated Jun. 15, 2023), https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html.

[175] *Id.*

[176] While not a spyware company, Americans have already been targeted by surveillance technology that the U.S. government was potentially paying for. Recent reporting discovered a trove of phone numbers hacked using an exploit in the Signaling System 7, or SS7, which is a "decades-old set of protocols that allows phone networks to communicate with one another, routing messages and calls across borders." This technology was used to acquire cellphone IDs and facilitate location tracking. Gabriel Geiger et al., *How First Wap Tracks Phones Around the World*, Lighthouse Reports (Oct. 14, 2025), https://www.lighthousereports.com/methodology/surveillance-secrets-explainer/.

[177] Mark Mazetti & Ronan Bergman, *Defense Firm Said U.S. Spies Backed Its Bid for Pegasus Spyware Maker*, N.Y. Times (Jul. 10, 2022), https://www.nytimes.com/2022/07/10/us/politics/defense-firm-said-us-spies-backed-its-bid-for-pegasus-spyware-maker.html.

[178] Tom Uren, *Peter Williams, Ex-ASD, Pleads Guilty to Selling Eight Exploits to Russia*, Lawfare (Oct. 31, 2025), https://www.lawfaremedia.org/article/peter-williams--ex-asd--pleads-guilty-to-selling-eight-exploits-to-russia.

[179] *See, e.g.,* NSO Data Leak, *supra* note 41.

[180] Angelique Chrisafis et al., *Emmanuel Macron identified in leaked Pegasus project data,* The Guardian (Jul. 20, 2021), https://www.theguardian.com/world/2021/jul/20/emmanuel-macron-identified-in-leaked-pegasus-project-data.

[181] Craig Timberg & Drew Harwell, *Q&A: A Guide to 'Spyware'*, Washington Post (Jul. 18, 2021), https://www.washingtonpost.com/technology/2021/07/18/what-to-know-spyware-pegasus/.

[182] *Id.*

[183] *See Apple, Privacy. That's Apple.*, *supra* note 170. *See also* EPIC, *Case Page: Apple v. FBI,* https://epic.org/documents/apple-v-fbi-2/ (discussing the public perception and support of Apple after it refused to break encryption for the FBI in 2016).

[184] *See* Whitney Blair Wyckoff, *Poll: American Voters Overwhelmingly Want Privacy, Encryption,* FedScoop (Apr. 18, 2016), https://fedscoop.com/survey-most-americans-want-data-on-their-phone-to-stay-private/.

[185] *Supra* note 66.

[186] Hal Abelson, et al., *Bugs in Our Pockets: The Risks of Client-Side Scanning* (Oct. 14, 2021), https://arxiv.org/abs/2110.07450.

[187] EPIC, *About Edward Snowden*, https://archive.epic.org/privacy/nsa/snowden/ (last visited Oct. 31, 2025).

[188] *See* Spyware Executive Order, *supra* note 4.

[189] *Id.*

[190] *Addition of Certain Entities to the Entity List*, 86 Fed. Reg. 60759 (Nov. 4, 2021), https://www.federalregister.gov/documents/2021/11/04/2021-24123/addition-of-certain-entities-to-the-entity-list; *see also*, Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Enablers of the Intellexa Commercial Spyware Consortium (Sept. 16, 2024), https://home.treasury.gov/news/press-releases/jy2581.

[191] 18 U.S.C. § 1030.

[192] *Id.*

[193] Verdict, *Whatsapp v. NSO Group Technologies* Case No. 19-cv-07123-PJH (May 6, 2025); *see also* Maria Villegas Bravo, *When Courts Reach the Merits, Spyware Loses*, EPIC (May 8, 2025), https://epic.org/when-courts-reach-the-merits-spyware-loses/.

[194] *Id.*

[195] *Dada et al. v. NSO Group*, No. 4:22-cv-05229 (N.D. Cal. remanded and currently at motion to dismiss stage).

[196] *Alhathloul v. Darkmatter Group LLC, supra* note 6 (plantiff's CFAA claim survived motion to dismiss).

[197] *Id.*

[198] Joseph Cox, *NSO Group Pitched Phone-Hacking Tech to American Police*, Vice (Apr. 7, 2022), https://www.vice.com/en/article/nso-group-pitched-phone-hacking-tech-american-police/.

[199] *Virtue or Vice?, supra* note 8.

[200] *All-Out Mobilization Against the French "War-On-Drugs" Law*, La Quadrature du Net, https://www.laquadrature.net/en/warondrugslaw/ (last visited Oct. 31, 2025).

[201] Austria's government, a signatory of the Pall Mall Process, agreed to legislate a law that authorizes law enforcement use of spyware for limited purposes and under technical and organizational safeguards. *See* Barbara Steinbrenner, *Messenger-Überwachung: Worauf sich die Regierung geeinigt hat*, Die Presse (Jun. 18, 2025), https://www.diepresse.com/19807577/messenger-ueberwachung-worauf-sich-die-regierung-geeinigt-hat.

[202] *See, e.g.*, Alyasah Ali Sewell et al., *Is Atlanta's Cop City the Answer to Public Safety?*, Brookings (Jan. 31, 2023), https://www.brookings.edu/articles/is-atlantas-cop-city-the-answer-to-public-safety/.

[203] *See, e.g.*, City of L.A., *FY 2024–25 Budget Summary* 62 (2024), https://cao.lacity.gov/budget24-25/2024-25Budget_Summary.pdf; NYC Council, *FY 2025 Executive Budget: NYPD* (Mar. 2024), https://council.nyc.gov/budget/wp-content/uploads/sites/54/2024/03/056-NYPD.pdf.

[204] *See, e.g.,* Todd Feathers & Alfred Ng, *Tech Industry Groups Are Watering Down Attempts at Privacy Regulation, One State at a Time*, The Markup (May 26, 2022), https://themarkup.org/privacy/2022/05/26/tech-industry-groups-are-watering-down-attempts-at-privacy-regulation-one-state-at-a-time.

[205] *See EPIC Commends Oregon for Enacting Heightened Protections for Location, Minors' Data,* EPIC (Jun. 4, 2025), https://epic.org/epic-commends-oregon-for-enacting-heightened-protections-for-location-minors-data/; Nancy Libin et al., *Maryland Creates a New Paradigm for Data Privacy*, *Davis Wright Tremaine LLP* (May 15, 2024), https://www.dwt.com/blogs/privacy--security-law-blog/2024/05/maryland-online-data-privacy-act-signed.

[206] Letter from over 100 Civil Society Orgs. to U.S. Congress (Feb. 4, 2024), https://s3.us-east-1.amazonaws.com/demandprogress/letters/Over_100_groups_support_major_FISA_reform_oppose_sham_FISA_Reform_and_Reauth.pdf.

[207] Joe Lancaster, *New Montana Law Blocks the State From buying Private Data to Skirt the Fourth Amendment*, Reason Magazine (May 16, 2025), https://reason.com/2025/05/16/new-montana-law-blocks-the-state-from-buying-private-data-to-skirt-the-fourth-amendment/.

[208] *See, e.g.,* S.B. 20-217, 72d Gen. Assemb., Reg. Sess. (Colo. 2020).

[209] Jake Laperruque, *Status of State Laws on Facial Recognition Surveillance: Continued Progress and Smart Innovations*, Tech Policy Press (Jan. 6, 2025), https://www.techpolicy.press/status-of-state-laws-on-facial-recognition-surveillance-continued-progress-and-smart-innovations/.

[210] *See, e.g.,* 18 U.S.C. § 2511(1)(a).

[211] Ark. Code Ann. §§ 5-60-120 (2024).

[212] N.D. Cent. Code § 29-29.2-02(1) (2024).

[213] EPIC, *The Electronic Communications Privacy Act (ECPA)*, https://epic.org/ecpa/.

[214] Md. Code Ann. Cts. & Jud. Proc. § 10-403 (2024).

[215] In most states, only one party to the communication needs to consent; however, 11 states are known as all party or two-party consent states where all parties to the communication need to consent to the recording of a communication.

[216] *But see* Jennifer S. Granick et al., *Mission Creep and Wiretap Act 'Super Warrants': A Cautionary Tale*, 52 Loyola of Los Angeles L. Rev. 4, 431(2019) (noting that strong oversight and enforcement of super warrant requirements is necessary for these provisions to protect civil rights as intended).

[217] *But see,* Fed. R. Crim. P. 41(b)(6) (allowing magistrate judges to issue warrants "to use remote access to search electronic storage media and to seize or copy electronically stored information" in certain circumstances).

[218] Mass. Gen. Laws. Ch. 272 § 99(I)(2) (2024) (15 days for the initial interception period unless physical installation if a device is required, in which case a 30 day interception period is allowed).

[219] N.J. Stat. Ann. § 2A:156A-12(f) (2024) (20 days for the initial period and a limit of 2 extensions each lasting 10 days).

[220] Wash. Rev. Code § 9.73.040(7)(2024) (15 Days for the initial interception and 15 days for extensions).

[221] 18 U.S.C. § 2518(5).

[222] Md. Code Ann. Cts. & Jud. Proc. § 10-408(c)(5)(ii) (2024); Mass. Gen. Laws ch. 272 § 99.

[223] 18 Pa. Cons. Stat. §§ 5725-5728.

[224] Ga. Code Ann. §§ 16-11-60 - 16-11-70.

[225] Mont. Code Ann. §§ 46-5-601 - 46-5-614.

[226] *Id.*

[227] Va. Code Ann. §§ 18.2-152.1 – 18.2-152.16.

[228] Restatement (Second) of Torts § 652 (Am. L. Inst. 1977).

[229] *See, e.g.,* Virginia, *supra* note 227.

[230] *Riley*, *supra* note 3.

[231] *Nader v. General Motors Corp.*, 255 N.E.2d 765 (N.Y. 1970) (while the case was adjudicated in New York, the case pertains to District of Columbia law).

[232] Computer Spyware Protection Act, ALEC (last updated Jan. 20, 2018), https://alec.org/model-policy/computer-spyware-protection-act-2/. *See* Appendix 3 for list of states that have adopted this law.

[233] Alaska Stat. § 45.45.798.

[234] Spyware Executive Order, *supra* note 4.

[235] Modeled off of the language from 18 Pa. Cons. Stat. § 5716.

[236] 18 U.S.C. § 1030(e)(1) (2022), "the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device."

[237] Modeled after D.C. Code § 28-3905(k)(1)(C).

[238] Modeled after D.C. Code § 28-3905(k)(1)(D).

[239] EPIC opposed the proposed amendment to Rule 41 that explicitly allows remote warrants and believes a stronger safeguard is needed. Alan Butler, *Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure before the Judicial Conference Advisory Committee on Criminal Rules* (Nov. 5, 2014), https://archive.epic.org/privacy/surveillance/remote-access/EPIC-FRCP-Rule-41-Amendments-Testimony.pdf.

[240] Spyware Executive Order, *supra* note 4.

[241] *See, e.g.,* Cal. Pen. Code § 502(c)(8).

[242] Iowa Code § 716.6B.

[243] Verdict, *Whatsapp v. NSO Group Technologies* Case No. 19-cv-07123-PJH (May 6, 2025).

[244] *See, e.g.,* Cal. Pen. Code § 502(c)(8).

[245] D.C. Code § 28-3901 et seq.

[246] D.C. Code § 28-3905(k)(1)(C).

[247] *Id.* (noting broader standing requirements than under Article III.)

[248] *Id.*

[249] Cal. Pen. Code § 502; Verdict, *supra* note 243.

[250] Verdict, *supra* note 243; Alhathloul, *supra* note 6.

[251] *See generally Financial Investigations for Good*, FIND, https://find.ngo/ (last visited Oct. 31, 2025); *Advancing Human Rights in Investment*, Heartland Initiative, https://heartland-initiative.org (last visited Oct. 31, 2025); Surveillance Watch, *supra* note 47.

APPENDICES

APPENDIX 1: WIRETAPPING LAWS

State	Citation	Time Limitation (Initial Interception)	Time Limitations (Extensions, if any)	Notification Requirement	Private Right of Action
Federal	18 U.S.C. §§ 2510-2523	30 days	30 days (no limit on number)	☑	☑
Alabama	Ala. Code §§ 20-2b-1 - 20-2b-16	30 Days	30 days (no limit on number)	☑	☑
Alaska	Alaska Stat. §§ 12.37.010 - 12.37.130	30 days	30 days (no limit on number)	☑	☒
Arizona	Ariz. Rev. Stat. Ann. §§ 13-3001 - 13-3019	30 days	30 days (Limit based on judge's discretion)	☑	☒*
Arkansas	N/A	N/A	N/A	N/A	N/A
California	Cal. Pen. Code §§ 629.50 - 629.98	30 days	30 days (no limit on number)	☑	☑
Colorado	Colo. Rev. Stat. §§ 16-15-101 - 16-15-104	30 days	30 days (3 extensions max)	☑	☒
Connecticut	Conn. Gen. Stat. §§ 54-41a - 54-41u	15 Days	15 days (3 extensions max)	☑	☑
District of Columbia	D.C. Code §§ 23-541- 23-556	30 days	30 days (no limit on number)	☑	☑
Delaware	Del. Code Ann. tit. 11 §§ 2401- 2434	30 days	30 days (no limit on number)	☑	☑
Florida	Fla. Stat. §§ 934.01 - 934.50	30 days	30 days (no limit on number)	☑	☑
Georgia	Ga. Code Ann. §§ 16-11-60 - 16-11-70	No limits	No limits	☒	☒
Hawaii	Haw. Rev. Stat. §§ 803-41 - 803-49	30 days	30 days (no limit on number)	☑	☑
Idaho	Idaho Code §§ 18-6701- 18-6726	30 days	30 days (no limit on number)	☑	☑
Illinois	725 Ill. Comp. Stat. 5/108A/1 - 5/108B-14	30 days	30 days (no limit on number)	☑	☑
Indiana	Ind. Code §§ 35-33.5-2-1 - 35-33.5-2-5	30 days	30 days (3 extensions max)	☑	☑
Iowa	Iowa Code §§ 808B.1 - 808B.14	30 days	30 days (no limit on number)	☑	☑

State	Citation	Time Limitation (Initial Interception)	Time Limitations (Extensions, if any)	Notification Requirement	Private Right of Action
Kansas	Kan. Stat. Ann. §§ 22-2514 -222519	30 days	30 days (no limit on number)	☑	☑
Kentucky	N/A	N/A	N/A	N/A	N/A
Louisiana	La. Stat. Ann. §§ 15.1302 - 15.1318	30 days	30 days (no limit on number)	☑	☑
Maine	N/A	N/A	N/A	N/A	N/A
Maryland	Md. Code Ann. Cts. Jud. Proc. §§ 10-401 - 10-414	30 days	30 days (no limit on number)	☑	☑
Massachusetts	Mass. Gen. Laws ch. 272 § 99	15 days	15 days (no limit on number, but must be within 2 years of date of effect of original warrant)	☑#	☑
Michigan	N/A	N/A	N/A	N/A	N/A
Minnesota	Minn. Stat. §§ 626A.01 - 626A.42	30 days	30 days (no limit on number)	☑	☑
Mississippi	Miss. Code Ann. §§ 41-29-501 - 41-29-536	30 days	30 days (no limit on number)	☑	☑
Missouri	Mo. Rev. Stat. §§ 542.400 - 542.422	30 days	30 days (no limit on number)	☑	☑
Montana	Mont. Code Ann. §§ 46-5-601 - 46-5-614	No limits	No limits	☑#	☒**
Nebraska	Neb. Rev. Stat. §§ 86.271 - 86.2,117	30 days	30 days (no limit on number)	☑	☑***
Nevada	Nev. Rev. Stat. §§ 179.410 - 179.515	30 days	30 days (no limit on number)	☑	☒****
New Hampshire	N.H. Rev. Stat. Ann. §§ 570-A:1 - 570-A:11	10 days	10 days	☒	☑
New Jersey	N.J. Stat. Ann. §§ 2A:156A-1 - 2A:156-37	20 days	10 day extension (2 extensions max)	☑	☑
New Mexico	N.M. Stat. Stat. Ann. §§ 30-12-1 - 30-12-14	30 days	30 days (no limit on number)	☑	☑
New York	N.Y. Crim. Proc. Law §§ 700.05 - 710.70	30 days	30 days (no limit on number)	☑	☒
North Carolina	N.C. Gen. Stat. §§ 15A-286 - 15A-298	30 days	30 days (no limit on number)	☑	☑

State	Citation	Time Limitation (Initial Interception)	Time Limitations (Extensions, if any)	Notification Requirement	Private Right of Action
North Dakota	N.D. Cent. Code §§ 29-29.2-01 - 29-29.2-05	30 days	30 days (no limit on number)	☑	☒
Ohio	Ohio Rev. Code Ann. §§ 2933.51-2933.65	30 days	30 days (no limit on number)	☑	☑
Oklahoma	Okla. Stat. tit. 13 §§ 176 - 177	30 days	30 days (no limit on number)	☑	☒
Oregon	Or. Rev. Stat. §§ 133.721 - 133.740	30 days	30 days (no limit on number)	☑	☑
Pennsylvania	18 Pa. Stat. and Cons. Stat. Ann. §§ 5701 - 5782	30 days	30 days (no limit on number)	☑	☑*****
Rhode Island	12 R.I. Gen. Laws §§ 12-5.1 - 12-5.2	30 days	30 days (no limit on number)	☑	☑
South Carolina	S.C. Code Ann. §§ 17-29-10 - 17-30-145	30 days	30 days (no limit on number)	☑	☑
South Dakota	S. D. Codified Laws §§ 23A-35A-1 - 23A-35A-34	30 days	30 days (no limit on number)	☑	☒
Tennessee	Tenn. Code Ann. §§ 40-6-301 - 40-6-311	30 days	30 days (no limit on number)	☑	☒
Texas	Tex. Code Crim. Proc. Ann. art. 18A-001 - 18A.553	30 days	30 days (no limit on number)	☑	☑
Utah	Utah Code Ann. §§ 77-23a-1 - 77-23a-16	30 days	30 days (no limit on number)	☑	☑***
Vermont	Vt. Stat. Ann. tit. 13, §§ 8101 - 8108	Fully prohibits real time interception	Fully prohibits real time interception	N/A	☒
Virginia	Va. Code Ann. §§ 19.2-61 - 19.2-70.3	30 days	30 days (no limit on number)	☑	☑
Washington	Wash. Rev. Code §§ 9.73.040 - 09.73.060	15 Days	15 days	☑	☑
West Virginia	W. Va. Code §§ 62-1D-1 - 62-1D-16	20 days	20 days, but if there is a communication captured where a party to the communication is not identified in the warrant, then the extension period will automatically terminate	☑	☑

State	Citation	Time Limitation (Initial Interception)	Time Limitations (Extensions, if any)	Notification Requirement	Private Right of Action
Wisconsin	Wis. Stat. §§ 968.27 - 968.375	30 days	30 days (no limit on number)	☑	☑****
Wyoming	Wyo. Stat. Stat. Ann. §§ 7-3-701 - 7-3-806	30 days	30 days (no limit on number)	☑	☑

* includes criminal penalties for non-compliance (AZ)

** AG can enforce compliance (MT)

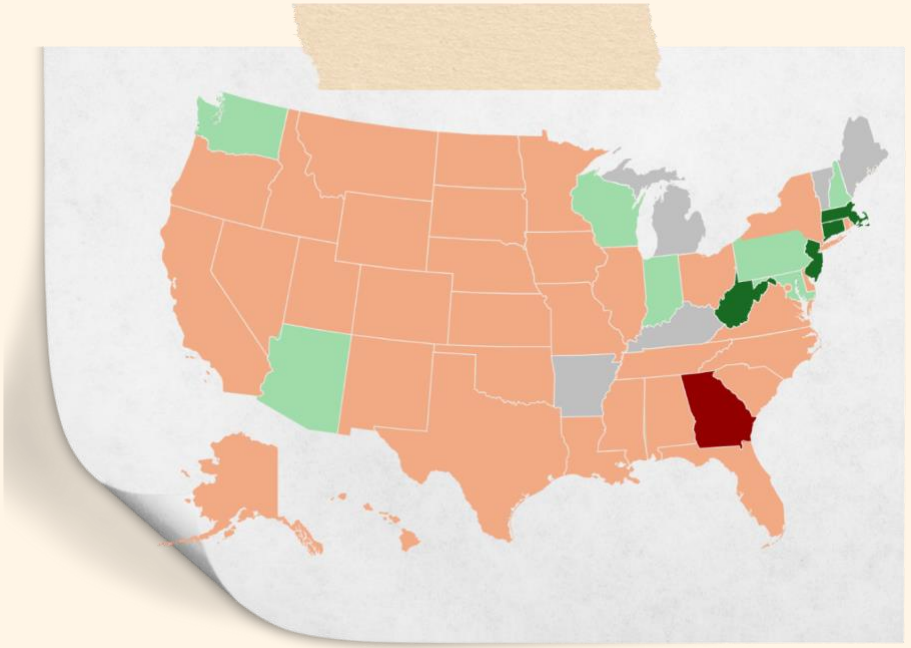
*** 2-year statute of limitations (NE, UT)

**** Gov't official engaging in wiretapping can be held in contempt of court for noncompliance w/ law (WI, NV)

***** can remove officials from office for noncompliance with the law (PA)

notification required before or contemporaneous to the warrant's execution period (MA, MT)

The map was created by assessing the states on the four factors outlined in the table above. Each element was given a weight of 1. Georgia, with 0 points, is dark red. States with 1-2 points (typically with the same time limits as ECPA, but may have a notification requirement and private right of action) are light red. States with 3 points are light green. States with 4 points are dark green. The gray states do not have a state statute regulating law enforcement wiretapping procedure.



APPENDIX 2: COMPUTER CRIME LAWS

State	Citation	Access Without Authorization	Access That Exceeds Authorization	Installation of Malware and/or Contaminant	Attorney General Enforcement	Manufacturing and/or Possession of an Access Device Criminalized	Law Enforcement Liability Carveout	Private Right of Action
Federal	18 U.S.C. § 1030	☑	☑	☒	☒	☑	☑	☑
Alabama	Ala. Code §§ 13A-8-100 -- 13A-8-119	☑	☑	☑	☒	☒	☑	☒
Alaska	Alaska Stat. ch 46 § 740	☑	☑	☑	☒	☒	☒	☒
Arizona	Ariz. Rev. Stat. Ann. §§ 13-2301, 13-2316 - 13-2316.02	☑	☑	☑	☒	☑	☒	☒
Arkansas	Ark. Code Ann. §§ 5-41-101 - 5-41-109	☑	☑	☒	☑	☒	☑	☑
California	Cal. Pen. Code § 502	☑	☑	☑	☒	☒	☑	☑
Colorado	Colo. Rev. Stat. §§ 18-5.5-101 - 18-5.5-102	☑	☑	☑	☒	☒	☒	☒
Connecticut	Conn. Gen. Stat. §§ 53a-250 - 53a-262	☑	☒	☒	☒	☒	☒	☒
Delaware	Del. Code. Ann. tit. 11 §§ 931 - 941	☑	☑	☒	☒	☒	☒	☑
DC	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

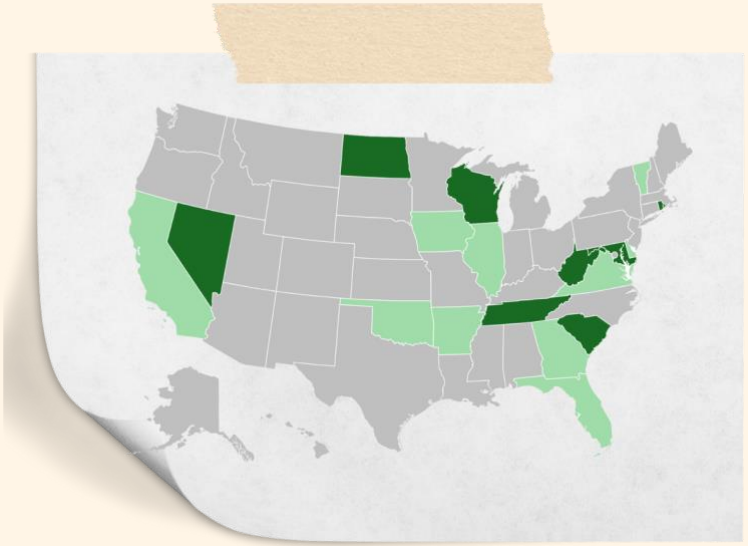
State	Citation	Access Without Authorization	Access That Exceeds Authorization	Installation of Malware and/or Contaminant	Attorney General Enforcement	Manufacturing and/or Possession of an Access Device Criminalized	Law Enforcement Liability Carveout	Private Right of Action
Florida	Fla. Stat. §§ 815.01 - 815.07	☑	☑	☑	☒	☒	☑	☑
Georgia	Ga. Code Ann. §§ 16-9-90 - 16-9-94	☑	☒	☒	☒	☒	☒	☑
Hawaii	Haw. Rev. Stat. §§ 708-890 - 708-895.7	☑	☒	☒	☒	☒	☒	☒
Idaho	Idaho Code §§ 18-2201 - 18-2202	☑	☒	☒	☒	☒	☒	☒
Illinois	720 Ill. Comp. stat. 5/17-50 - 5/17-54	☑	☑	☑	☒	☒	☒	☑
Indiana	Ind. Code § 35-43-2-3	☑	☒	☒	☒	☒	☒	☒
Iowa	Iowa Code § 716.6B	☑	☒	☒	☒	☒	☒	☑
Kansas	Kan. Stat. Ann. §§ 21-5839	☑	☑	☒	☒	☒	☒	☒
Kentucky	Ky. Rev. Stat. Ann. §§ 434.840 - 434.860	☑	☒	☒	☒	☒	☒	☒
Louisiana	La. Stat. Ann. §§ 14.73.1 - 14.73.14	☑	☑	☑	☒	☒	☒	☒
Maine	Me. Stat. tit. 17 §§ 431 - 437	☑	☑	☑	☒	☒	☒	☒
Maryland	Md. Code Ann. Crim. Law §§ 7-301 - 7-304	☑	☒	☒	☒	☒	☒	☑
Massachusetts	Mass. Gen. Laws ch. 266 § 120f	☑	☒	☒	☒	☒	☒	☒

State	Citation	Access Without Authorization	Access That Exceeds Authorization	Installation of Malware and/or Contaminant	Attorney General Enforcement	Manufacturing and/or Possession of an Access Device Criminalized	Law Enforcement Liability Carveout	Private Right of Action
Michigan	Mich. Comp. Laws §§ 752.791 752.797	☑	☑	☑	☒	☒	☒	☒
Minnesota	Min. Stat. §§ 609.87 - 609.8913	☑	☒	☒	☒	☒	☒	☒
Mississippi	Miss. Code Ann. §§ 97-45-1 - 97-45-33	☑	☒	☑	☒	☒	☒	☒
Missouri	Mo. Rev. Stat. §§ 569.095 569.099	☑	☒	☒	☒	☒	☒	☒
Montana	Mont. Code Ann. § 45-6-311	☑	☒	☑	☒	☒	☑	☒
Nebraska	Neb. Rev. Stat. §§ 28-1341 - 28-1347	☑	☑	☒	☒	☒	☒	☒
Nevada	Nev. Rev. Stat. §§ 205.473 - 205.513	☑	☒	☑	☑	☒	☒	☑
New Hampshire	N.H. Rev. Stat. Ann. §§ 638.16 - 638.19	☑	☒	☑	☒	☒	☒	☒
New Jersey	N.J. Stat. Ann. §§ 2C:20-23 - 2C:20-34	☑	☑	☑	☒	☒	☒	☒
New Mexico	N.M. Stat. Ann. §§ 30-45-1 - 30-45-7	☑	☑	☒	☒	☒	☒	☒
New York	N. Y. Pen Law §§ 156.00 - 156.50	☑	☒	☒	☒	☒	☒	☒
North Carolina	N.C. Gen. Stat. §§ 14-453 - 14-458.2	☑	☑	☑	☒	☒	☒	☒

State	Citation	Access Without Authorization	Access That Exceeds Authorization	Installation of Malware and/or Contaminant	Attorney General Enforcement	Manufacturing and/or Possession of an Access Device Criminalized	Law Enforcement Liability Carveout	Private Right of Action
North Dakota	N. D. Cent. Code §§ 12.1-06.1-08	☑	☑	☒	☒	☒	☒	☑
Ohio	Ohio Rev. Code Ann. § 2913.04	☑	☑	☒	☒	☒	☒	☒
Oklahoma	Okla. Stat. tit. 21 §§ 1952	☑	☑	☒	☑	☒	☒	☑
Oregon	Or. Rev. Stat. § 164.377	☑	☒	☒	☒	☒	☒	☒
Pennsylvania	18 Pa. Stat. and Cons. Stat. Ann. §§ 7601 - 7661	☑	☑	☑	☑	☒	☑	☒
Rhode Island	11 R.I. §§ 11-52-1 - 11-52-8	☑	☑	☒	☒	☒	☒	☑
South Carolina	S.C. Code Ann. §§ 16-16-10 - 16-16-40	☑	☑	☑	☒	☒	☒	☑
South Dakota	S.D. Codified Laws §§ 43-43B-1 - 43-43B-8	☑	☑	☒	☒	☒	☒	☒
Tennessee	Tenn. Code Ann. §§ 39-14-601 - 39-14-606	☑	☒	☑	☒	☒	☒	☑
Texas	Tex. Penal Code Ann. §§ 33.01 - 33.07	☑	☑	☒	☑	☒	☑	☒
Utah	Utah Code Ann. § 76-6-703	☑	☑	☒	☑	☒	☑	☒
Vermont	Vt. Stat. Ann. tit. 13, §§ 4101 - 4107	☑	☒	☒	☒	☒	☒	☑

State	Citation	Access Without Authorization	Access That Exceeds Authorization	Installation of Malware and/or Contaminant	Attorney General Enforcement	Manufacturing and/or Possession of an Access Device Criminalized	Law Enforcement Liability Carveout	Private Right of Action
Virginia	Va. Code Ann. §§ 18.2-152.1 - 18.2-152.15	☑	☑	☒	☒	☒	☒	☑
Washington	Wash. Rev. Code §§ 9A.90.010 - 9A.90.120	☑	☒	☑	☒	☒	☒	☒
West Virginia	W. Va. Code §§ 61-3C-1 - 61-3C-21	☑	☒	☑	☒	☒	☒	☑
Wisconsin	Wis. Stat. § 943.70	☑	☒	☒	☒	☒	☒	☑
Wyoming	Wyo. Stat. Ann. §§ 6-3-501 - 6-3-507	☑	☒	☑	☒	☒	☒	☒

The states highlighted in dark green are states with a private right of action and no law enforcement carveout. The states highlighted in light green are states with a private right of action and also a law enforcement carveout. The gray states do not have a private right of action and may or may not have a law enforcement carveout.



APPENDIX 3: ALEC MODEL LAW

State	ALEC Spyware Law citation
Arizona	Ariz. Rev. Stat. Ann. §§ 18-501 - 18-504
Arkansas	Ark. Code Ann. §§ 4-111-101 - 4-111-105
California	Cal. Bus. & Prof. Code §§ 22947 - 22947.6
Iowa	Iowa Code §§ 715.1 - 715.11
Pennsylvania	73 Pa. Const. Stat. §§ 2330.1 - 2330.20
Texas	Tex. Bus. & Com. Code Ann. §§ 324.001 - 324.102

epic.org

ELECTRONIC
PRIVACY
INFORMATION
CENTER