From Writs to Wires: The Surveillance State's Long War on Privacy

By Patrick G. Eddington, Nicholas Anthony, Jeffrey A. Singer, and Jennifer Huddleston

ILLUSTRATIONS BY MARK WEAVER

In the lead-up to the American Revolution, British customs officers wielded general warrants and physical force to search colonists' homes, stores, desks, ships, and other private property. Anger over these intrusions reached a boiling point with the writs of assistance, which Massachusetts lawyer James Otis Jr. argued in court were the "worst instrument of arbitrary power" and destructive to fundamental principles of law and liberty.

A 25-year-old John Adams watched Otis's five-hour oration in 1761 and later recalled it as a "flame of fire" that left those in attendance "ready to take arms." "Then and there," Adams reflected decades later, "the child Independence was born." Otis's defense of liberty helped lay the groundwork for the Fourth Amendment, which guaranteed the right of the people to be secure against unreasonable searches and seizures.

Two and a half centuries later, the surveillance state is quieter, more pervasive, and largely invisible. Under the banner of security, government has constructed a digital panopticon that allows it to peer into citizens' finances, health records, and personal data on a scale the Founders scarcely could have imagined. This feature examines how that system grew, and how it might yet be restrained.

American Dystopia: Surveillance-Enabled Political Repression and How to End It

By Patrick G. Eddington

A quarter of the way through the 21st century, the scale and ubiquity of America's surveillance architecture has become as mind-boggling as it is terrifying.

Facial recognition (including the mobile variety), iris-scanning apps, finger- and palm-print readers, voiceprint analyzers, GPS-enabled tracking, automated license plate readers, cell-site simulators, spyware, and online ad tracking software . . . these are just some of the technologies that day by day are making it harder for any of us to maintain our privacy and anonymity.

Corporate actors frequently sell information they collect on you—including demographic and identifier data, health information, financial and biometric data, online activity, communications metadata, and more—to those willing to pay for it. While this is acceptable to many Americans when they are properly notified and given the ability to consent or opt out, a much more serious problem arises when the state

sidesteps the warrant requirement by simply purchasing information on the open market. Law enforcement agencies at the local, state, and federal levels, including the FBI, the IRS, the Drug Enforcement Administration, the Department of War, and the Department of Homeland Security, have been customers of this data, according to a major report by the Brennan Center for Justice.

The evolution of surveillance technologies and techniques is creating new points of vulnerability from a constitutional rights standpoint.

Take the home security business, for instance. In July 2025, Ring announced that, in partnership with security services contractor Axon, it was resuming its Request for Assistance program, whereby law enforcement personnel will have warrantless access to Ring users' videos. Accordingly, the Ring camera your next-door neighbor installed can now be used by police to monitor when you leave or arrive, when you have guests, when a repairman arrives to fix your stove . . . the list goes on.

Police in California have also been creative in seeking video from another platform: Tesla.

As the *San Francisco Chronicle* reported in 2024, Bay Area police have gone so far as to tow Teslas from crime scenes to get access to data from a given vehicle's external-facing video camera, though they

"It is unsurprising, then, that a key objective of modern government surveillance state apparatchiks has been a quest to undermine publicly available encryption options."

have been forced in several cases to get warrants to do so.

In the case of the FBI, the access that agents have to both commercially available data and classified information, when combined with an internal Department of Justice (DOJ) authority known as an "assessment," gives them the ability to open an investigation on a person or organization and collect and collate a vast amount of data on the target—all without having to get a warrant.

Under the current administration, President Trump isn't simply issuing executive orders that have no statutory or constitutional basis to harm individuals, classes of persons, or civil society organizations; he's personally directed his attorney general to open baseless criminal investigations and has twisted an already broken federal grand jury process into a vehicle for securing indictments against his political enemies—real or imagined. The Founders launched a revolution to free themselves from these kinds of tyrannical acts.

George Washington, Thomas Jefferson, Patrick Henry, John Hancock, Benjamin Franklin, and other early Americans launched and led a revolution against a British monarchy that routinely intercepted their mail and (in Hancock's case) seized their property because of their opposition to the Crown's repressive policies, such as warrantless searches and taxation without representation.

Indeed, Jefferson, John Adams, James Monroe, and other Founders used encryption in their personal and professional communications because of British political repression—before, during, and after the Revolutionary War. It is unsurprising, then, that a key objective of modern government surveillance state apparatchiks has been a quest to undermine publicly available encryption options.

Can this part of the slide toward an American autocracy be reversed?

Yes.

In April 2024, the House passed the Fourth Amendment Is Not for Sale Act, which would require government agents to obtain a court order before acquiring certain customer and subscriber records or any illegitimately obtained information from a third party. The Senate failed to act on the bill, which is all the more reason it should be reintroduced.

Full repeal of the PATRIOT Act and FISA Amendments Act would also help turn back the surveillance tide, as both authorities have been serially abused.

A single federal law enforcement agency charter that prohibits surveillance of persons or infiltration of groups engaged in activity protected by the First Amendment, absent probable cause that a federal crime has been or is being committed, should also be created.

The most difficult but necessary reform would be moving the DOJ out of the executive branch and placing it under the federal judiciary.

Congress created the DOJ via statute and has direct constitutional power over both the structure of the federal judiciary and the scope of the Supreme Court's appellate review authority. These are powers clearly within Congress's Article I authority. Accordingly, Congress could statutorily move the DOJ out of the executive branch and include a provision stating that no federal court has jurisdiction to review a congressional act designed to restructure the government to reduce the potential for executive branch tyranny.

A heavy political lift? Almost surely. But perhaps less so in a post-Trump political environment, and absolutely necessary if the republic is to survive for another 250 years.

ABOUT THE AUTHOR

Patrick G. Eddington is a senior fellow in homeland security and civil liberties at the Cato Institute and the author of *The Triumph of Fear: Domestic Surveillance and Political Repression from McKinley to Eisenhower.*

How the State Keeps Watch on Your Wallet

By Nicholas Anthony

There are few places where privacy is more misunderstood than in our finances. Think of all the steps you take to keep your financial information under lock and key. You might post vacation photos on social media, but you probably don't post your credit card history. You might throw away your mail, but you probably take a moment first to rip up bank statements. Yet strangely, none of that matters to the government.

Put simply, you might think you have financial privacy, but what you really have is the illusion of financial privacy.

This illusion is maintained by a series of laws passed over the last 55 years, including the Bank Secrecy Act, the Money Laundering Control Act, the Annunzio–Wylie Anti–Money Laundering Act, the Money Laundering Suppression Act, the PATRIOT Act, and more. With each new law, Congress steadily expanded what types of transactions must be reported to the government, leading to the opaque financial surveillance web we have today.

If you are thinking this invasion of your privacy sounds unconstitutional, you're not

alone. When the Cato Institute surveyed the American public, 83 percent of respondents thought the government should need a warrant to access personal financial records. After all, isn't that what the Fourth Amendment is supposed to require?

Unfortunately, that's not how the system works today. The Supreme Court weighed in on this question in the 1970s, ultimately siding with Congress and creating what has come to be known as the third-party doctrine. In short, the idea is that you lose all protections because you shared information with someone else. Yet you can't have an account with a bank (or any traditional financial service) without sharing your information. So, in effect, all those records held by your bank, financial planner, and similar entities are fair game for prying eyes—as long as those eyes belong to the government.

The groundwork for financial surveillance began five decades ago, but the government is still expanding those powers today. Under the Biden administration, a proposal to further surveil bank accounts with at least $600 in annual activity was stopped, but a similar proposal to surveil payment apps like PayPal and Cash App took effect. Now under the Trump administration, the government set up a new system for surveilling transactions of $200 or more sent through money service businesses like Western Union.

Congress has been busy, too. The recently enacted stablecoin legislation, which covers cryptocurrencies pegged to the dollar or another asset, put parts of this new

ecosystem within the confines of the Bank Secrecy Act regime. And there has been a steady stream of attempts to apply these requirements to all cryptocurrency activity.

Now more than ever, it is time to reclaim financial privacy. It's time to turn back the tide on ever-increasing financial surveillance. There are a few options on the table for getting this done.

Taking it to the courts is one route. The Supreme Court has slowly started to recognize that past laws were not crafted with a full appreciation of the digital age. Cases like *United States v. Jones*, *Riley v. California*, and *Carpenter v. United States* have steadily refined the limits on government access to our private lives. Much more is needed, but these have been positive developments.

Yet, even then, the judicial process can be uncertain. Will a case be heard? If it is, what if the Court rules in an unexpected direction? The Court might even weigh in your favor, but base its decision on a narrower or unrelated legal question.

That's why Congress must act. Legislators got us into this web of financial surveillance and they now have three main options to help get us out.

At a minimum, all the thresholds for reports required under the Bank Secrecy Act should be adjusted for inflation. Congress could go further and eliminate the reporting requirements. Even better, Congress could also do away with the Bank Secrecy Act regime entirely. This last route would let banks decide what information they need, whom they do business with, and what risks they take on. It would still be illegal to knowingly assist criminal activity, and law enforcement would still be able to get a warrant should an investigation justify it. The only change would be the absence of this multibillion-dollar surveillance system.

Whichever path Congress chooses, reform is long overdue.

ABOUT THE AUTHOR

Nicholas Anthony is a policy analyst at the Cato Institute's Center for Monetary and Financial Alternatives, and the author of *Digital Currency or Digital Control? Decoding CBDC and the Future of Money*.

"All those records held by your bank, financial planner, and similar entities are fair game for prying eyes—as long as those eyes belong to the government."

How the War on Drugs Undermines Adult Autonomy— and Invades Our Privacy

By Jeffrey A. Singer

Every time an American fills a prescription for medication classified as a controlled substance, they now leave a digital trail available to law enforcement known as a Prescription Drug Monitoring Program (PDMP).

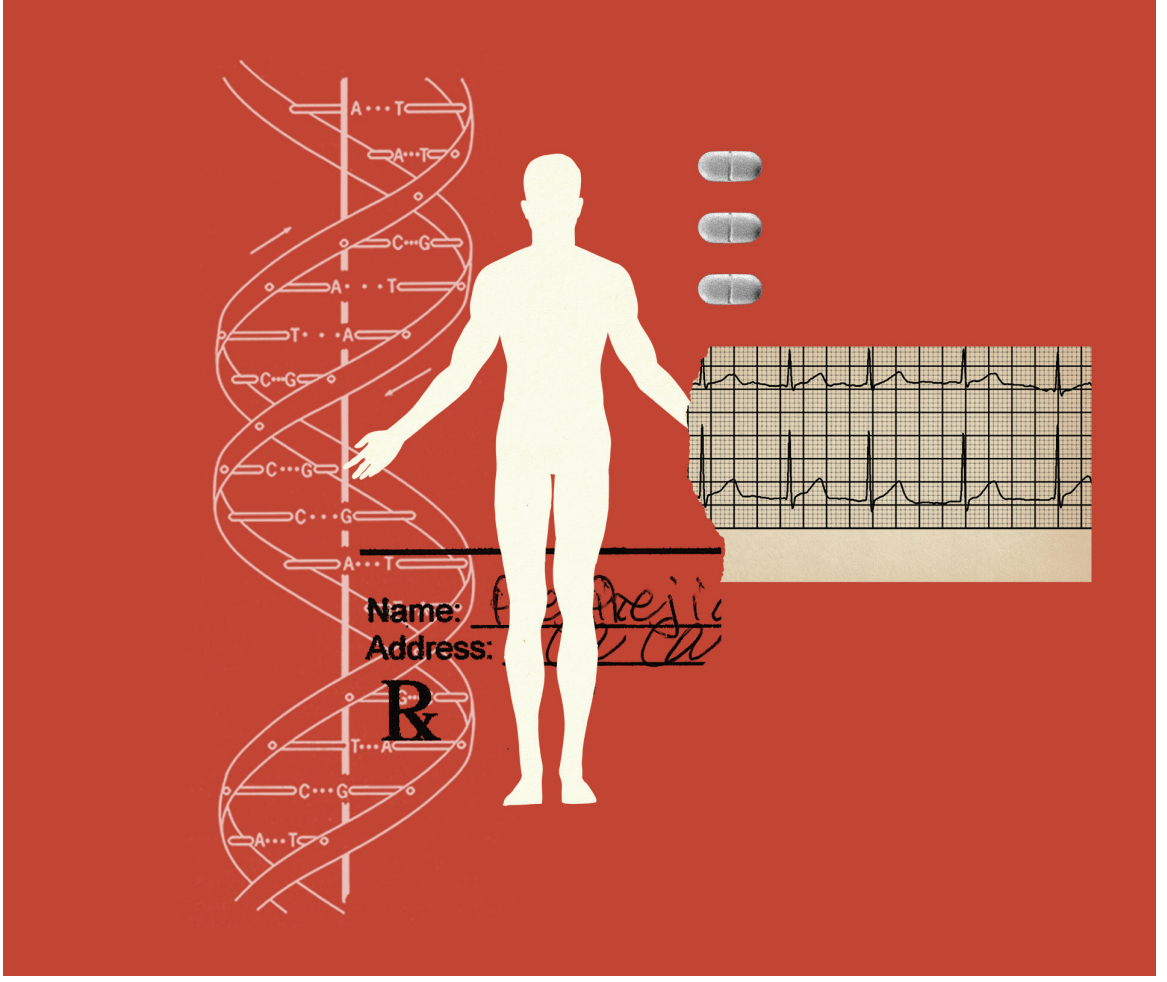
This is the latest iteration of the US government's century-long assault on personal autonomy and privacy through the war on drugs. What began as a moral crusade by policymakers to dictate what an individual can or cannot put in their body has morphed into warrantless surveillance of the once-private space between a patient and their doctor.

The push for PDMPs began in the early 2000s, when a rise in overdose deaths caught the attention of lawmakers and public health officials. Instead of rethinking prohibition, they found a convenient scapegoat: doctors. The false narrative took hold that physicians were "overprescribing" opioids and turning their pain patients into zombie-like addicts who eventually sought stronger drugs on the street. A flurry of new regulatory and legislative restrictions reduced opioid prescribing roughly 60 percent between 2011 and 2020—and today, it's back to where it was in 1992. But this failed to slow the rise in overdose deaths, which surpassed 110,000 deaths annually in the years following the COVID-19 pandemic and are currently at record levels. And during the process, law enforcement invaded patients' privacy.

The Department of Justice and the Drug Enforcement Administration first made funds available to states to establish their own PDMPs in 2003. Today, every state, along with the District of Columbia and Guam, has a PDMP. These databases track every transaction involving the prescription and dispensing of controlled substances. They record how often and how much each patient receives, as well as how frequently each clinician prescribes. In effect, PDMPs turn the private act of seeking medical care into a government surveillance effort—an unsettling invasion of the confidential relationship between doctors and their patients.

Federal and state law enforcement routinely mine PDMPs for data to identify clinicians they suspect of "overprescribing" or running so-called pill mills—a term used for clinics allegedly dispensing drugs with little or no medical justification. In practice, narcotics task forces in tactical gear have raided physicians' offices, paraded physicians before TV cameras in "perp walks," and sent a chilling message to other doctors: Prescribe opioids and risk your career—and your freedom.

PDMPs also flag patients accused of "doctor shopping," or obtaining pain prescriptions from multiple providers within a short time frame. Yet many of these individuals are not criminals at all—they're pain patients who have been abandoned or



inadequately treated by their physicians, desperately seeking relief wherever they can find it.

PDMPs also intimidate pharmacists, causing many to refuse to fill doctors' opioid prescriptions.

However, the evidence shows that, while PDMPs may be an effective law enforcement surveillance tool in reducing opioid prescribing, they have not affected the drug overdose rate. In fact, by reducing the amount of prescription pain pills that can be diverted to the underground market, evidence suggests that PDMPs may have contributed to the rise in overdose deaths, as nonmedical drug users have resorted to heroin, fentanyl, and other more readily available products. Patients in desperate pain and shunned by prescribers have turned to the dangerous underground market to find relief, often overdosing.

A growing body of research examines how clinicians can remotely monitor patients being treated for opioid use disorder, including the gradual tapering of methadone under a specialist's supervision to prevent withdrawal. The broader goal, enabled by telemedicine, is to let physicians

"What began as a moral crusade by policymakers to dictate what an individual can or cannot put in their body has morphed into warrantless surveillance of the once-private space between a patient and their doctor."

manage a wide range of conditions through connected monitoring devices, reducing the need for patients to visit the doctor's office in person. But this new technology can also be used by law enforcement as a surveillance tool.

Congress introduced legislation in 2023 and again in March 2025 requiring the Government Accountability Office to conduct a comprehensive study of remote monitoring for individuals prescribed opioids, and to submit a report to Congress with recommendations. The bill has not moved forward as of this article's writing. If enacted, such a program would take the surveillance of pain patients to a new level, extending government oversight from the pharmacy counter directly into people's homes.

The US drug war has destabilized governments in Latin America and elsewhere and filled America's prisons disproportionately with black Americans and other minorities. In the process, the iron law of prohibition—"the harder the enforcement, the harder the drugs"—has encouraged the development of more potent and deadly substances entering the illicit drug market.

The war on drugs has not only failed to save lives, it has also steadily eroded the privacy and autonomy that define a free society. Every new layer of surveillance, from prescription databases to remote monitoring, treats patients as suspects and physicians as potential criminals. Adults deserve the dignity of making their own choices about what to put in their bodies and how to manage their pain without government intrusion. Reclaiming that freedom begins with recognizing that health care decisions belong to patients and their doctors—not to law enforcement.

ABOUT THE AUTHOR

Jeffrey A. Singer practices general surgery in Phoenix. He is a senior fellow at the Cato Institute in the department of health policy studies and the author of *Your Body, Your Health Care*.

Permission to Speak: How Age-Verification Laws Threaten Privacy and Safety

By Jennifer Huddleston

A wave of age-verification laws is sweeping through state legislatures and countries around the world. While aimed at keeping young people safe, this approach is threatening to normalize identity checks, personal data collection, and surveillance as a prerequisite for online speech and access to information. The privacy rights and data of both children and adults are at risk as a result.

Since 2023, about two dozen states have passed some version of an online age-verification law, but many of these laws have been enjoined when challenged in court due to their impact on adult users' First Amendment rights. Those that have been upheld, such as the requirements at issue in *Free Speech Coalition v. Paxton*, have been more limited in applying only to pornography or other adult sexual content deemed inappropriate for minors. At the federal level, multiple bills have been introduced that aim to make age verification a common form of compliance nationwide.

In countries where broader age-verification requirements have taken effect, it's already becoming clear that they affect the rights of all users, limit parental choice, and fail to protect kids and teens. The United Kingdom's Online Safety Act, for instance, implemented age verification for content deemed "harmful to minors," including not only pornography but also an array of content believed to promote violence, eating disorders, and a long list of other sensitive subjects. This affects far more than the content that might immediately come to mind. In its aftermath, the act has also required facial scans for the music streaming platform Spotify, limited access to information on the wars in Gaza and Ukraine on certain platforms, and restricted art by acclaimed Spanish painter Francisco Goya. Even accessing a *Free Press* newsletter could require UK readers to verify their age.

Australia, meanwhile, recently became the first country to implement a nationwide ban on social media for people younger than 16. Early reports make the enforcement difficulties of such laws clear, as teens are easily able to circumvent the ban through a virtual private network (VPN), which masks a user's location. For the teens who do find themselves barred from major platforms like Facebook, Instagram, and Reddit, the new law appears to be pushing them toward lesser-known, less moderated corners of the internet, perhaps creating even more risks.

Without undergoing such verification, platforms may deny access or limit the user to a "kid-safe" mode regardless of the user's actual age. The result limits the ability of individuals who are unwilling to submit information about their identity to both speak and receive information. Users have good reason to be cautious about

offering their government IDs online, as there have already been significant leaks of IDs that were collected to verify a user's age. For the young people these laws claim to protect, platforms are effectively being forced to build a database of their teen users' full names and government IDs, creating a honeypot for malicious actors and predators. For other users, such as political dissidents, whistleblowers, or those escaping abuse, the reality of potential disclosure could significantly compromise their physical safety. There are also those without IDs who could find themselves locked out of being able to express themselves or access information on important sensitive topics such as sexual health.

Some advocates for age-verification laws point out that they do not require IDs, but alternatives are invasive to privacy in other ways. For example, biometric scans are sometimes used to estimate age, but these scans are not accurate for all groups equally and are less accurate when right at the cusp of an age requirement. No facial scan can tell when it's midnight on a teen's birthday, making them suddenly eligible for full access to information. Other methods require an app to examine potentially revealing information such as credit card transactions or internet history, introducing other mechanisms that could make an individual vulnerable.

Age-verification laws also threaten anonymous speech, which the Supreme

"In countries where broader age-verification requirements have taken effect, it's already becoming clear that they affect the rights of all users, limit parental choice, and fail to protect kids and teens."

Court described as a "shield against the tyranny of the majority" in *McIntyre v. Ohio Elections Commission* and has repeatedly ruled is protected by the First Amendment. Anonymous speech has a long tradition dating back to America's Founding and beyond. Alexander Hamilton, John Jay, and James Madison published *The Federalist Papers* under the pen name "Publius" as the Founders drafted the Constitution. This magazine's publisher, the Cato Institute, took its name from *Cato's Letters*, a series of essays published anonymously by British writers John Trenchard and Thomas Gordon in the early 18th century.

Most of us want young people to be able to have positive and safe experiences, whether online or in real life. While the reasons for age-verification proposals may be well intentioned, the reality is that they make all internet users, including children and teens, less safe. ✦

ABOUT THE AUTHOR

Jennifer Huddleston is a senior fellow in technology policy at the Cato Institute, where her research focuses on the intersection of emerging technology and law.