CONGRESS MUST RESTORE CONSTITUTIONAL LIMITS ON SURVEILLANCE

"*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.*"

Fourth Amendment to the U.S. Constitution

The language of the Fourth Amendment forbidding warrantless surveillance provides no exemptions or exceptions. And it's clear that the "effects" covered in this amendment include our most personal information captured by digital technology. In recent decades, however, our government has become comfortable acting in ways that violate the letter and the spirit of that Amendment.

For example, the government routinely uses the powers of the Foreign Intelligence Surveillance Act, meant to catch foreign spies and their enablers, to watch Americans. It sidesteps warrant requirements through a growing practice of simply purchasing our personal data from data brokers. It deploys new modes of aerial and biometric surveillance in ways that chill the First Amendment rights of Americans to protest and political groups to organize. Relying on secret legal interpretations, it plays verbal games and exploits new technologies to open loopholes in privacy laws that Congress never envisioned.

Further, there is reason to believe the government may have secretly concluded that intelligence agencies have inherent authority, in the absence of any court order or Congressional authorization, to conduct surveillance on people in the United States.

As a result, the government has multiple ways to access Americans' communications and other highly sensitive information *without any suspicion of wrongdoing* — let alone probable cause and a warrant. Predictably, these tools for warrantless surveillance have been turned on racial, ethnic, and religious minorities, as well as political activists and opponents.

Such abuses are not necessary to protect our people from crime or our nation from spies and terrorism. However, these privacy abuses have repeatedly proven to be an escalating threat not only to those suspected of wrongdoing but to every American. Congress should act this session to make sure that our government continues to uphold the Fourth Amendment.

Pressing Surveillance Issues before Congress

It is past time for Congress to enact surveillance reforms that restore Americans' constitutional rights and create a sustainable legal framework for privacy in the digital age. Members of Congress who value privacy should pursue these current legislative opportunities to secure constituents' liberties:

- **Support The Fourth Amendment Is Not For Sale Act (H.R.2738/S.1265)**, which closes the legal loophole that the government is exploiting to purchase troves of information from private data brokers that it would otherwise need a court order or subpoena to obtain. This legislation was been introduced in the Senate by Sens. Ron Wyden, Mike Lee, Patrick Leahy, Steve Daines, Rand Paul, and others, including Majority Leader Chuck Schumer. It was introduced in the House by Reps. Jerry Nadler and Zoe Lofgren.

- **Strengthen the Foreign Intelligence Surveillance Court and remove impediments to judicial oversight** — as provided for in Sens. Patrick Leahy and Mike Lee's amendment that passed the Senate in 2020 with 77 votes.

- **Rein in warrantless surveillance under Executive Order 12333 and Section 702 of FISA**, for instance by supporting the Lofgren-Massie amendment to prohibit "backdoor" searches of Americans' communications, which has been endorsed by dozens of organizations.
    - **This is necessary to restore any EU-US Privacy Shield agreement**, which in 2020 the Court of Justice of the European Union (CJEU) struck down for the second time.

- **Update privacy laws to comply with recent Supreme Court decisions** and protect newer forms of highly personal information, such as geolocation data, web browsing and Internet search histories, DNA and other forms of biometric information, and more. Sens. Ron Wyden and Steve Daines, for instance, offered an amendment in 2020 to protect Internet browsing and search histories from warrantless surveillance under the Patriot Act, which earned 59 votes in support (it has also been incorporated in The Fourth Amendment Is Not For Sale Act).

- **Adopt reforms that ensure proper transparency when an American citizen has been subject to surveillance.** Congress should adopt legislation that requires law enforcement to notify domestic targets of electronic data surveillance in a timely manner. Currently, the government is able to avoid notification, or delay it indefinitely, with only a weak showing of need.

- **Stop the proliferation of facial recognition and biometric technology** by the federal government, which it is aggressively deploying in the absence of statutory authorization.

- **Support the Cell-Site Simulator Warrant Act (H.R.4022/S.2122)**, which would require the government obtain a warrant before deploying cell site simulators, often called "Stingrays," to identify and track all cell phones in an area.

- **Support the Open Technology Fund (OTF)**, an independent entity created, owned, and operated in partnership with the US government, in particular by empowering OTF to support secure technology domestically (fact sheet).

- **Eliminate the government's ability to engage in "bulky collection"** or otherwise collect sensitive data without any individualized suspicion of wrongdoing.

- **Update and modernize the Electronic Communications Privacy Act (ECPA)** to reflect changes in technology and the public's privacy expectations.

- **Fight secret law and get straight answers from the executive branch** about how it is using the legal authorities Congress has provided, as well as whether it believes it has "inherent authority" to conduct surveillance on the American people.

- **Join the Fourth Amendment Caucus**, co-chaired by Reps. Zoe Lofgren (contact: ryan.clough@mail.house.gov) and Thomas Massie (contact: seana.cranston@mail.house.gov).

How We Got Here

In the 1970s, the Church Committee revealed that intelligence agencies, including the CIA, the FBI, and the NSA, had been spying on Americans for decades. Congress and the executive branch responded by enacting laws and policies designed to limit government surveillance and protect Americans' constitutional rights. Congress also acted to protect consumer privacy in areas like financial transactions and telecommunications.

Unfortunately, these laws have failed to keep up with technology. The Electronic Communications Privacy Act, for instance, was enacted before the advent of the modern Internet and hasn't been meaningfully updated since. Some surveillance laws in place today would likely be unconstitutional under recent Supreme Court case law. None addresses the modern phenomenon of data brokers — a gap the government now routinely exploits to purchase data that it would otherwise need a court order to obtain. Likewise, most of the electronic communications surveillance the U.S. government conducts overseas is unregulated by Congress, based on the long-outdated assumption that overseas surveillance has little impact on Americans' privacy.

Compounding this problem, surveillance laws were dramatically expanded — and privacy protections weakened — in the aftermath of 9/11. We have now had twenty years of experience with these laws, and it's clear that a reset is needed. Surveillance authorities that were meant to target foreigners in international terrorism cases have morphed into tools for warrantless access to Americans' communications in purely domestic criminal matters. Court decisions have revealed systemic failure to comply with of privacy safeguards established by Congress and the courts. And reviews by independent government bodies have concluded that some of the most intrusive post-9/11 surveillance programs have yielded little value in protecting America.

The Fallout: Surveillance Abuses and Economic Risks

When government is free to conduct warrantless surveillance, the result has always been the same: targeting of marginalized communities, including racial and religious minorities, as well as political opponents and many who exercise their constitutional right to express dissent. In the era examined by the Church Committee, the FBI set its sights on Martin Luther King, Jr. and other civil rights and anti-war activists. In recent years, we have seen troubling echoes of those practices from administrations of both parties.

Although the government's actual surveillance practices are highly secretive — and officials have sometimes provided false or misleading statements to Congress about those practices — investigative reporting and public scandals have uncovered some disturbing activities. A small sample:

- The Department of Defense buys detailed geolocation information generated by popular prayer and dating apps used by Muslims around the world, including the United States — despite the fact that the Supreme Court held in 2018 that such information is protected by the Fourth Amendment.

- The Department of Justice (DOJ) Inspector General found that applications to conduct surveillance of a Trump campaign aide — a highly sensitive investigation that demanded scrupulous accuracy — were riddled with errors and omissions. The inspector general also conducted a random survey of 29 FISA surveillance requests regarding other individuals and found numerous errors in all of them.

- In June, as thousands of people took to the streets to protest police killings of Black Americans, the Department of Homeland Security (DHS) collected and analyzed protesters' text messages — then denied the practice in a congressional hearing. DHS also deployed helicopters, airplanes, and drones over 15 cities to monitor the protests, logging at least 270 hours of surveillance.

- To assist in identifying undocumented immigrants, DHS has bought access to a private database that tracks millions of cell phones using geolocation information generated by games and weather apps.

These examples are likely the tip of the iceberg, given the other ways in which racial, religious, and ethnic minorities and political activists and opponents have been singled out by law enforcement and intelligence agencies. For instance, as far back as 2015, DHS monitored the social media posts of civil rights leaders protesting racial issues in policing. More recently, Immigration and Customs Enforcement (ICE) kept careful track of "anti-Trump" protests in New York City. And DHS compiled intelligence files on journalists who covered the George Floyd protests. Regardless of one's position on the intelligence collection techniques used in each of these cases, they all illustrate the problem of discriminatory use of police surveillance power.

Furthermore, U.S. surveillance practices increasingly violate international laws and norms, creating tensions with allies and making it more difficult for U.S. companies to do business with overseas partners. Lax privacy protections in the United States recently led CJEU to invalidate the agreement that allows data transfers between European Union and U.S. companies. If the situation isn't remedied, it could have a profound effect on the ability of U.S. businesses to do business in Europe.

In short, the need to rethink our surveillance practices is abundantly clear. As opportunities for meaningful reforms arise, we will provide additional materials to give members the information they need to stand up for Americans' constitutional rights. In the meantime, feel free to contact any of us with thoughts or questions:

American Civil Liberties Union
Kate Ruane, kruane@aclu.org

Americans for Prosperity
Jeremiah Mosteller, jmosteller@afphq.org

Brennan Center for Justice
Elizabeth Goitein, elizabeth.goitein@nyu.edu

Demand Progress
Sean Vitka, sean@demandprogress.org

Free Press Action
Sandy Fulton, sfulton@freepress.net

FreedomWorks
Cesar Ybarra, cybarra@freedomworks.org

Project for Privacy & Surveillance Accountability
Gene Schaerr, gschaerr@protectprivacynow.org

Additional Resources

We encourage offices to sign up for these resources that will help keep them up to date:

Secure Liberties Newsletter, by Demand Progress Education Fund: www.secureliberties.org

Project for Privacy & Surveillance Accountability Newsletter: www.protectprivacynow.org