MILITARISM AT HOME: THE EXCESSIVE SURVEILLANCE OF OUR COMMUNITIES

A REPORT BY THE CONGRESSIONAL PROGRESSIVE CAUCUS CENTER

TABLE OF CONTENTS

INTRODUCTION

There is a long tradition of domestic surveillance in the United States. From companies spying on workers and unions to the NYPD crackdown on Muslim communities after 9/11, U.S. citizens have been the targets of spying in their homes, neighborhoods, and workplaces. As more of our lives are captured and preserved digitally and online, critical questions have emerged about the government's authority to surveil Americans and non-Americans, and the tactics that private actors can employ to monitor citizens.

In this report, we explore the current sources of spending for several intelligence programs. We also call attention to historical examples of surveillance by the state and the tactics employed. Our report draws a clear connection between the taxpayer dollars spent on intelligence programs and the militarized surveillance of our neighbors and communities.

Authors:

Mariam Malik, Senior Foreign Policy Associate
mariam@progressivecaucuscenter.org

Alan Barber, Policy Director
alan@progressivecaucuscenter.org

The CPC Center thanks Sean Vitka of Demand Progress, Jessica Katzenstein and Fatema Ahmad of Muslim Justice League for their comments, insights, and contributions to this report.

MILITARY SPENDING

To understand the U.S.'s massive surveillance state, we must first understand how much the U.S. government spends on its military. The military budget includes spending on various surveillance technologies, equipment, intelligence operations, and more. While most surveillance occurs by intelligence agencies, such as the Central Intelligence Agency (CIA), or law enforcement agencies, such as the Federal Bureau of Investigation (FBI), the funding for most surveillance practices comes from the military budget. For FY2024, Congress approved a Pentagon budget of $824 billion, an increase of $27 billion or a little more than 3 percent from FY2023. In December 2023, Congress passed and President Biden signed into law the FY2024 National Defense Authorization Act (NDAA) which authorized $886 billion in military spending for FY2024.[1]

Surveillance spending is spread across multiple government agencies, most notably the CIA, the FBI, the Department of Defense (DOD), the Department of Homeland Security (DHS), the National Security Agency (NSA), The National Counterterrorism Center (NCTC), and various programs at the Department of Justice (DOJ). Surveillance spending is difficult to pin down because no single surveillance budget function exists in the annual appropriations process. Additionally, intelligence budgets are usually legislated in secret, so the taxpayers are generally unaware of the intelligence practices they are paying for. The requested intelligence budget for FY 2025 totals $99.6 billion.

Some of the ways surveillance funds are used include:

- Intelligence agencies such as the CIA, NSA, and NCTC.
- Law enforcement agencies, such as the FBI.
- Private corporations such as Lockheed Martin.
- Third-party data-brokers that harvest data from communication and technology companies.
- Social media companies that assist the government with surveillance.

[1] For more on the difference between appropriations and authorization bills, see our explainer.

National Security Agency (NSA) headquarters in Fort Meade, Maryland.

SURVEILLANCE AND MILITARIZATION ACROSS THE U.S.

Section 215 of The USA Patriot Act

The USA Patriot Act was signed into law 45 days after 9/11. It allowed mass surveillance to support counterterrorism operations, foreign intelligence investigations, and national security. In practice, it led to the bulk collection of many Americans' private information.

Section 215 of the Patriot Act expanded the type of information the government could collect on businesses and citizens to "any tangible thing." More specifically, virtually any information on anyone was fair game for the government to target and collect. This could be phone calls, internet activity, financial details, medical information, addresses visited, and much more. Section 215 also:

- Made it easier and quicker for the government to obtain bulk information, by lowering the requirements it had to go through to get a court order to gather this information.
- No longer required government agencies to provide evidence that subjects were a "foreign agent" to conduct a search on them. This enabled mass surveillance without suspicion.

In 2013, former NSA contractor Edward Snowden leaked that the agency was engaging in bulk collecting Americans' phone records and used Section 215 to justify it. This exposed the government's mass spying on Americans' phone records, such as phone calls, length of calls, emails, text messages, website visits, internet activity, and other information. These leaks confirmed privacy advocates' claim that the government was using Section 215 to spy on virtually every American and collect whatever information it wanted without meaningful oversight or an approval process. Later, in 2019, a federal court ruled that the government's interpretation of Section 215 was "unprecedented and unwarranted."

President George W. Bush signing the Patriot Act on October 26, 2001.

In addition to collecting bulk data, law enforcement agencies used Section 215 to demand that banks and other financial institutions produce the financial records of many people. Doctors were ordered to hand over their patient's medical information if an intelligence agency requested it. Libraries, bookstores, universities, communication companies, and other institutions must provide information about their patrons when requested. The author of the Patriot Act, former Congressman Jim Sensenbrenner (R-WI-05), stated that the NSA abused its power and the legislation was not intended for mass, suspicionless surveillance.

Section 215 expired on June 1, 2015, and, instead, lawmakers passed the USA Freedom Act, which reigned in the government's mass surveillance practices and limited the types of private information it could collect. This latest version of Section 215 expired on March 15, 2020, and has not been re-authorized since. While surveillance practices under Section 215 ended, there are still other avenues the government uses to unjustly and illegally surveil Americans and non-Americans.

Section 702 of the Foreign Intelligence Surveillance Act

Immediately after 9/11, President George W. Bush initiated a series of massive unconstitutional surveillance efforts under a program code named Stellar Wind. In 2008, before key details of Stellar Wind came to light, Congress legalized the most flagrantly illegal part of the surveillance — compelling companies to provide access to international communications without a warrant — as Section 702 of the Foreign Intelligence Surveillance Act (FISA), which sets the rules for the collection of foreign intelligence.

Today, FISA is an uneven patchwork that includes provisions that protect and compromise Americans' privacy. It first became law in 1978, but since then, it has been amended multiple times to enable greater domestic surveillance.

Section 702 of FISA generally allows intelligence agencies, namely the CIA, NSA, and NCTC, and law enforcement agencies, namely the FBI, to search through billions of warrantlessly acquired international communications. These agencies target non-U.S. persons (meaning non-U.S. citizens or residents) outside the U.S. and compel electronic communications companies, like Google and Verizon to turn over these individuals' communications. Because we live in a globalized world, many Americans' Fourth Amendment-protected conversations are swept up "incidentally." This information includes emails, text messages, and internet data.

The CIA, FBI, NSA, and NCTC knowingly search through this staggering amount of warrantless surveillance, specifically looking for information about people in the U.S. who otherwise cannot be "targeted" under Section 702. Americans can, however, be subjected to "U.S. person queries," which critics call the "backdoor search loophole." In 2022, intelligence agencies conducted over 200,000 of these "backdoor searches." The FISA Court has revealed that the FBI has a history of "persistent and widespread" violations when conducting these backdoor searches, and the NSA has a similarly sordid history.

The Section 702 database has been used to search for the communications of:

- A sitting Member of Congress and a sitting Senator.
- 141 Black Lives Matter protesters.
- 19,000 individuals who donated to a congressional campaign.
- Journalists.
- Individuals whom eyewitnesses called "tips" on because they were of "Middle Eastern" descent.
- A state court judge who reported civil rights violations to the FBI.
- An NSA analyst's online dating matches.
- NSA analysts' prospective tenants.

Despite Section 702's stated use for foreign intelligence, it has become a tool of domestic surveillance and led to repeated violations by the intelligence community and misuse of Fourth Amendment-protected private communications.

Most recent misuses of backdoor searches of Section 702 information threaten journalists, politicians, and protesters.

- Tens of thousands of FBI searches on "civil unrest."
- 141 communications of racial justice protestors.
- Searches on 1600 Americans whose travel, flights, and time at the airport during specific date ranges, as well as the countries they visited.
- Individuals listed in police homicide reports, including victims, next-of-kin, witnesses, and suspects.
- 19,000 donors to a congressional campaign.

While FISA is used to justify gathering foreign intelligence and combating threats from abroad, these examples show that many of the backdoor searches conducted under Section 702 of FISA are not related to international intelligence or matters abroad.

However, the U.S. has a history of spying on social movements, its citizens, and people of color.

Executive Order 12333

Executive Order (EO) 12333, signed on December 4, 1981, allows the government to spy on foreign individuals, organizations, and other entities abroad. Like Section 702, this inevitably collects private information on Americans, given our interconnected world. This means there are similar backdoor searches conducted under EO 12333 as under Section 702. The CIA operates bulk collection programs under EO 12333, which includes gathering Americans' financial transactions and other private information. The Government Surveillance Reform Act (GSRA) – introduced on November 7, 2023, by Rep. Warren Davidson (R-OH-08), Rep. Zoe Lofgren (D-CA-18), Sen. Ron Wyden (D-OR), and Sen. Mike Lee (R-UT) – would rein in such searches of EO 12333 data for Americans' private information. More information on the GSRA is below.

THE SURVEILLANCE OF PEOPLE AND MOVEMENTS

Surveillance of Civil Rights Groups

The surveillance of social movements and communities of color by the U.S. government is not a new phenomenon. Civil rights groups, peace activists, and climate activists, along with Black, brown, and indigenous citizens, have long been the subject of domestic intelligence efforts.

J. Edgard Hoover in the Oval Office, 1967.

The FBI surveillance of the civil rights movement and its leaders is widely known. J. Edgar Hoover, the head of the FBI from 1924 to 1972, was personally vested in these efforts. Hoover and others in the agency believed that civil rights organizing by Dr. Martin Luther King Jr. and other leaders were heavily influenced by communism despite little to no evidence to support this assertion.

At the same time, the FBI was surveilling the movement for Black civil rights; the National Security Agency or NSA spied not only on King but other anti-war activists, including Jane Fonda, Muhammed Ali, U.S. Senators, and others. Along with funds appropriated for intelligence work for the FBI, the CIA, and the military, the budget for domestic surveillance of anti-war activists was in excess of $80 million in 1975 dollars, with a large share of this coming from the military budget.[2]

Surveillance of Climate Activists

Militaristic or military-funded surveillance has also been employed against climate activists. The Water Protectors' fight against the Dakota Access Pipeline (DAPL) is one of the better-known examples. When the Standing Rock Sioux rallied against the DAPL in 2016, they were joined by groups, including the Movement for Black Lives, Veterans for Peace, and others. The Movement for Black Lives alignment with the DAPL protests was natural, as racial justice is a key element of environmental justice.

[2] The CIA, NSA, and the military are all funded through the military budget.

Despite a large outpouring of public support for the protest and the protestors, pipeline construction continued. Energy Transfer Partners, the company building the DAPL, eventually brought a private security company to confront the protestors. The security company TigerSwan is a group with extensive paramilitary training founded by a retired U.S. Army lieutenant colonel. In an example of how military training to protect civilians is turned on its head and used against U.S. citizens, TigerSwan used militaristic surveillance and counter-intelligence tactics on the protestors and worked with police agencies across several states to help disrupt the protests.

Surveillance of Muslim Communities after 9/11

The U.S. has illegally and unjustly surveilled Muslims for at least a century. Examples include the Moorish Science Temple in the 1930s, surveillance of the Nation of Islam during the civil rights era, and monitoring Muslims because of U.S. foreign policy towards Palestine.

The U.S. surveillance state as we know it today, took its shape after 9/11. Heightened bigotry, Islamophobia, and the national feeling to "do something" after 9/11 led to the establishment of multiple surveillance practices that overwhelmingly targeted Muslim Americans, or anyone who could be perceived to be Muslim, including U.S. citizens, U.S. residents, or non-Americans. This increased support for surveillance, again driven by racism and Islamophobia, led to the erosion of safeguards that protected Americans' privacy and data rights.

Surveillance of Muslim Communities after 9/11 in New York City

The New York Police Department's (NYPD) Intelligence Division is notorious for targeting Muslims in New York without suspicion. In the years following 9/11, the NYPD significantly increased its searches on mosques, student organizations, Muslim-owned businesses, and other targets.

The NYPD Intelligence Division spied on Muslims in New York City by:

- Mapping neighborhoods based on "ancestries of interest." This generally meant people with ties to Muslim countries.
- Taking pictures and videos of individuals going to mosques.
- Recording the license plate number of Muslims.
- Hiring informants, which the NYPD called "mosque crawlers," to attend services and gather names, addresses, and other personal information of worshippers. These informants engaged in a tactic referred to as "create and capture," where they would "create" conversations about jihad or Islamic terrorism and "capture" the responses and use them to prosecute or arrest innocent people.
- Gathering information on the daily lives of Muslims, such as restaurants, community centers, or shops Muslims would frequent. This information was gathered by "police rakers"—plainclothes officers who would "blend in" and gain the trust of everyday people and then gather information about Muslims' daily lives for law enforcement.

This hyper-surveillance led to a rise in Islamophobic and racist attacks against Muslims and non-Muslims, specifically Sikhs, South Asians, and Arabs. It also created an atmosphere of fear and mistrust. Newcomers at mosques were met with suspension by regular worshippers who were unsure if they were a spy. Imams would censor their sermons and even record them out of fear their words could be used to prosecute or arrest them. Muslims began to mistrust the police, and some changed their dress to "appear" less Muslim.

Fusion Centers

Fusion centers funded by DHS are state-operated physical sites that oversee information sharing between local, state, tribal, and federal governments. These centers work with the FBI and other federal agencies to collect and analyze massive amounts of data, such as phone calls, texts, facial recognition, and more. Fusion centers also work with private companies to gather data on people through camera surveillance, telecommunications, facial recognition, policing software, and government databases.

Fusion centers were founded after 9/11 as a "counterterrorism response." Today, fusion centers enable the police state, mass surveillance, immigration detention and deportation, and government spying on social movements and activists. A fusion center in Boston, the Boston Regional Intelligence Center (BRIC), created a "gang database," in which 97.7% of the people were people of color and more than 75% were Black men or teens. However, many of the people in the database were not and had never been affiliated with gangs. Fusion centers also collaborate with DHS, ICE, and CBP to bypass privacy and sanctuary laws that protect immigrants.

"It is important to understand that Islamophobia has justified the expansion of the surveillance state in ways that impact all communities - like with fusion centers. The militarism at home is not just that these agencies share surveillance practices and technology, but that our foreign policy necessitates domestic surveillance of communities impacted by wars abroad. It suppresses community organizing and political dissent, which we can see quite sharply in this moment regarding Palestine."
-Fatema Ahmed, Executive Director of Muslim Justice League

Joint Terrorism Task Force

Joint Terrorism Task Forces (JTTFs) are managed by the FBI and, theoretically, oversee cooperation between federal, state, and local law enforcement on counterterrorism investigations. This can include gathering evidence, arrests, intelligence gathering and sharing, and training for federal, state, and local law enforcement agencies. There are 200 JTTFs nationwide, including at least one in the FBI's 56 field offices. Additionally, JTTFs collaborate with other agencies, such as DHS.

In practice, JTTFs exacerbate racism in policing practices through mass surveillance and targeting Black, Brown, and other marginalized communities who are typically the targets of "counterterrorism" investigations. JTTFs have previously investigated names the FBI listed as "Black Identity Extremists." JTTFs also often knock on doors of Arab and Muslim families. Sometimes two FBI agents show up or an FBI agent and a JTTF member, i.e. a local cop. Additionally, JTTFs have conducted inquiries into Muslim communities that are illegal. The surveillance laws and practices implemented after 9/11 allowed for JTTFs to conduct these racist surveillance practices.

REFORMS NEEDED

Congress has proposed multiple reforms to the various surveillance practices used.

The Fourth Amendment Is Not For Sale Act

The Data-Broker Loophole allows the U.S. government to purchase Fourth Amendment-protected data, such as phone call records, internet activity, location information, and other electronic data, directly from data brokers, which are third parties that harvest data from communications and technology companies such as Verizon, AT&T, and Meta. Congress prohibited these companies from directly selling this sensitive data to the government in the Electronic Communications Privacy Act. Additionally, the Supreme Court ruled in *Carpenter v. United States* that a warrant protects some of this data. However, no court is involved in authorizing or overseeing these purchases. Agencies such as the FBI, DHS (including CBP and ICE), and DOD are purchasing this data on an enormous scale.

Congress took a meaningful step to address the warrantless purchase of Americans' data by closing the data-broker loophole in the Fourth Amendment Is Not For Sale Act – introduced by Rep. Warren Davidson (R-OH-08) and co-sponsored by Rep. Zoe Lofgren (D-CA-18), Jerry Nadler (D-NY-12), Andy Biggs (R-AZ-05), Ken Buck (R-CO-04), Pramila Jayapal (D-WA-07), Thomas Massie (R-KY-04), and Sara Jacobs (D-CA-51). This bill would prevent government agencies from purchasing Americans' data from communications and technology companies. It unanimously passed the House Judiciary Committee on July 19, 2023. House Floor consideration is pending. A companion bill has been introduced in the Senate.

Reforms to Section 702

The Government Surveillance Reform Act (GSRA) would address massive, warrantless surveillance. However, the Protect Liberty and End Warrantless Surveillance Act (PLEWSA) currently has bipartisan support in the House Judiciary Committee. The PLEWSA would:

- Address backdoor searches under Section 702 by requiring a warrant to search through 702 data.
- Reforms the FISA courts.
- Includes the Fourth Amendment Is Not For Sale Act, which would close the data-broker loophole.

Over 100 groups are focused on securing a vote on the PLEWSA ahead of Section 702's expiration on April 19, 2024. PLEWSA passed the House Judiciary Committee on December 6, 2023, with a bipartisan vote of 35-2. It may have enough votes to pass under suspension of the Rules. House Leadership removed it from floor consideration in December 2023. Further consideration is pending.

Meanwhile, the House Permanent Select Committee on Intelligence (HPSCI) is trying to advance a bill that does not address back door searches or the data-broker loophole. House leadership has not yet made clear which bill, or what amendments to that bill, will be brought to the Floor. In February 2024, there was an agreement to allow votes on these loopholes. HPSCI threatened to bring the rule down on the Floor and boycotted the Rules Committee hearing that would have finalized that agreement.

Reforms to Section 215

As noted above, when Section 215 of the Patriot Act expired in 2015, the bulk collection of Americans' phone data also ceased. It was replaced by the USA Freedom Act, which prohibited this mass collection. While ending bulk surveillance is a welcome protection of Americans' privacy, additional reforms are needed. Intelligence agencies should no longer have the authority to request and gather call data records, especially when there is no reason, evidence, or proof that this data on a particular individual is necessary for national security matters.

Additionally, the government should no longer be allowed to gather "business records" by obtaining a secret court order to require doctors, universities, banks, telecom companies, and others to hand over information on their customers, patients, students, etc.

Conclusion

While there are instances where spying and surveillance are needed to save lives and prevent violent attacks, too often, "national security" is used to justify illegal and warrantless surveillance of marginalized communities and social movements. Rather than making our communities safer, the needless surveillance of innocent people creates mistrust between communities and law enforcement, fuels racism and Xenophobia, and abrogates the civil rights of innocents.