Government Surveillance Reform Act of 2023 Seeks to End Warrantless Police and FBI Spying

The Government Surveillance Reform Act of 2023 pulls from past privacy bills to overhaul how police and the feds access Americans' data and communications.

By Dell Cameron

Nov 07, 2023 03:44 PM · 7 min. read · View original

In 1763, the radical journalist and colonial sympathizer John Wilkes published issue no. 45 of *North Briton*, a periodical of anonymous essays known for its virulent anti-Scottish drivel—and for viciously satirizing a British prime minister until he quit his job. The fallout from the subsequent plan of the British king, George III, to see Wilkes put in irons for the crime of being too good at lambasting his own government reverberates today, particularly in the nation whose founders once held Wilkes up as an idol, plotting a revolt of their own.

Wilkes' arrest boiled the Americans' blood. Reportedly, the politician-cum-fugitive had invited the king's men into his home to read the warrant for his arrest aloud. He quickly tossed it aside. At trial, Wilkes explained its most insidious feature: "It named nobody," he said, "in violation of the laws of my country." This so-called general warrant, which subsequent lawsuits by Wilkes would see permanently banned, vaguely described some criminal allegations, but not a single place to be searched nor suspect to be arrested was named. This ambiguity granted the king's men near blanket authority to arrest anyone they wanted, raid their homes, and ransack and destroy their possessions and heirlooms, confiscating large bundles of private letters and correspondence. When the Americans later passed an amendment to ban vague legal warrants describing neither "the place to be searched" nor "persons or things to be seized," it was Wilkes's home, historians say, that they pictured.

This morning, a group of United States lawmakers introduced bicameral legislation aimed, once again, at reining in a government accused of arbitrarily snatching up the private messages of its own citizens—not by breaking down doors and seizing handwritten notes, but by tapping into the power of internet directly to collect an endless ocean of emails, calls, and texts. The Government Surveillance Reform Act

of 2023 (GSRA)—introduced in the US House by representatives Zoe Lofgren and Warren Davidson, and in the US Senate by Ron Wyden and Mike Lee—is a Frankenstein bill more than 200 pages long, combining the choicest parts of a stack of cannibalized privacy bills that rarely made it past committee. The patchwork effect helps form a comprehensive package, targeting various surveillance loopholes and tricks at all levels of government—from executive orders signed by the president, to contracts secured between obscure security firms and single-deputy police departments in rural areas.

5:46

“Americans know that it is possible to confront our country’s adversaries ferociously without throwing our constitutional rights in the trash can,” Wyden tells WIRED, adding that for too long surveillance laws have failed to keep up with the growing threats to people’s rights. The GSRA, he says, would not strip US intelligence agencies of their broad mandate to monitor threats at home or abroad, but rather restore warrant protections long recognized as core to democracy’s functioning.

The GSRA is a Christmas list for privacy hawks and a nightmare for authorities who rely on secrecy and circumventing judicial review to gather data on Americans without their knowledge or consent. A US Justice Department requirement that federal agents

obtain warrants before deploying cell-site simulators would be codified into law and extended to cover state and local authorities. Police in the US would need warrants to access data stored on people's vehicles, certain categories of which should already require one when the information is stored on a phone. The government could also no longer buy sensitive information about people that would require a judge's consent, had they asked for it instead.

What's more, the bill will end a grandfather clause that's keeping alive expired portions of the USA Patriot Act that's allowed the FBI to continue employing surveillance techniques that have technically been illegal for two years. Petitioners in federal court seeking relief due to privacy violations will also no longer be shown the door for having no more than a "reasonable basis" to believe they've been wrongfully searched or surveilled.

5:46

Not to be outstripped by the sheer variety of smaller pet reforms—such as yanking the security clearances of anyone caught abusing a classified database (a crime that's commonly punished with a slap on the wrist), or ensuring that the government can't simply store people's data for the rest of their lives because it hasn't been decrypted—the GSRA principally takes aim at Section 702 of the Foreign Intelligence Surveillance Act, the government's most promiscuous surveillance program through

which it captures a large but *indeterminate* amount of messages en route to and from Americans' phones each day.

After 9/11, the US government commenced with some of the most extensive domestic surveillance in modern history, a monument achieved on the back of the internet's technological revolution that redefined what it meant for people to communicate. Exposed by journalists and leakers at the height of America's recent wars in the Middle East, the extent of the surveillance, once publicly acknowledged, unleashed bad memories of corrupt intelligence agencies relentlessly bugging anyone with a phone—actors, comedians, civil rights leaders, and even one another.

5:46

The US Congress, fearful of foreign threats, enacted only piecemeal reforms in response to these revelations, which kicked off in the early aughts and crescendoed in 2013 with Edward Snowden's polemic leaks. The government's sporadic but incessant updating of agency rules and procedures have done little to stymie routine abuses of the 702 data—which is currently fathomless. The first thing to know about the program, and how many Americans it ensnares each year, is that the government doesn't know the number and has little interest in learning it. A key defense, in fact, of the government's lack of transparency in this area

is that examining the data to determine who is and is not an American would technically commit the very violation its procedures are designed to prevent.

While the program is strictly authorized for the surveillance of foreigners on foreign soil, wiretapping internet communications is neither accurate nor precise. In 2008, Congress was forced to effectively recognize that the collateral surveillance of Americans was the inevitable byproduct of operating an intelligence program with Big Brother–like proportions. Faced with growing privacy fears at home and emerging national security threats abroad, Congress took stock of the situation and then resigned to split the baby.

Nearly 60 years ago, in the face of overwhelming evidence that police interrogations are inherently coercive, the US Supreme Court did not ban the practice in *Miranda v. Arizona* but rather ruled that the threat to people's rights could be reasonably mitigated by cops reading “collared” suspects a brief statement of rights—a “warning” that has much the same purpose as legal disclaimers read aloud on customer care calls. Similarly, Congress chose not to put an end to the surveillance of Americans' communication despite the enormous scale of rights violations accumulating steadily each day. Instead, it ordered the creation of many byzantine rules

and procedures designed to ameliorate constitutional risks to some reasonable degree —by merely lessening the odds of a federal employee laying eyes on any illicitly gained information.

“Incidental” is a surveillance term of art referring to communications of Americans not *accidentally* intercepted by their own government, but *unavoidably*. In a report last month, a federal privacy watchdog stressed that while the word “incidental” made the collection sound small, “it should not be understood as occurring infrequently.”

5:46

The GSRA takes aim at the use of incidental data by federal law enforcement agents, who are not bound by the same rules against spying on Americans as are analysts at the Pentagon, whose purview lies strictly overseas. While it is illegal to target US persons under 702, once they have been surveilled, the communications become accessible nevertheless to the Federal Bureau of Investigation, which has its own procedures for “querying” the nebulous database—rules that can permit, for example, the reading of emails marked “attorney-client privilege” so long as the subject isn’t wanted for a crime.

An inspector general’s investigation last year found the FBI’s own legal experts at variance over “key legal principles” tied to rules

governing 702's use. Findings like these have served only to repeatedly injure the FBI, nurturing a cycle of disappointment and distrust in its capacity to behave as a competent surveillant.

The GSRA could work positively to solve many problems at the FBI. Trust in the bureau among lawmakers is only likely to grow, for instance, once its unfettered access to a digital black box of everyone's secrets becomes subject to regular judicial review. The GSRA removes the ability entirely for the FBI to run queries on US persons without probable cause, that is, “a reasonable amount of suspicion, supported by circumstances sufficiently strong to justify a proven and cautious person's belief that certain facts are probably true.” (In contrast, the current standard is this: Be looking for evidence of a crime, don't go fishing, and be “reasonably” confident the information you're after is “likely” to be found.)

5:46

“For too long, intelligence and law enforcement agencies have had unchecked access to Americans’ personal data,” says Lofgren, the representative from California who issued a warning to colleagues on Tuesday against the “unwise” move of reauthorizing the 702 program without “carefully considering and enacting surveillance reforms.”

The GSRA is currently the only bill in Congress that could reauthorize the 702 statute that's set to expire by the end of the year. The statute is what allows the government to apply for "certifications" issued by the secret Foreign Intelligence Surveillance Court (FISC). These certifications, which all last for one year, allow the government to compel the cooperation of communications services providers for three purposes: foreign intelligence, counterterrorism, and the tracking of nuclear proliferation—with an array of threats, from cybercrime to narco-trafficking, all couched within those categories.

5:46

Whether or not Congress reauthorizes 702 before it expires, the collection will continue unabated until at least April, when the certifications expire. Hypothetically, the government could reapply for new certifications, which the FISC could grant before April, thereby extending the program's life into 2025 without Congress lifting a finger. That is unlikely, however, says Bob Goodlatte, former chairman of the House Judiciary Committee, who says any attempt to wrest control away from Congress will be viewed as a "hostile gesture," further imperiling Section 702's survivability.

"The FISA Court and the Director of National Intelligence have confirmed that our government conducted warrantless surveillance of millions of Americans' private communications," says Senator Mike Lee.

In remarks to WIRED, Lee pointed to high-level confirmations that the US government is conducting “warrantless surveillance of millions of Americans” each day. “It is imperative that Congress enact real reforms to protect our civil liberties,” he says, including “statutory penalties for privacy violations,” a precondition of his support for “reauthorizing Section 702.”