US Senate reauthorizes domestic surveillance, allows access to internet histories

Kevin Reed
16 May 2020

The US Senate voted on Thursday to approve the USA Freedom Reauthorization Act of 2020. The law authorizes government surveillance of the public, including federal law enforcement agency access to the internet browsing and search histories of American citizens.

Voting 80 to 16, the Senate approved a two-and-a-half-year extension of the Foreign Intelligence Surveillance Act (FISA) provisions that have been the basis of expanding abuses by US intelligence, which originated in the aftermath of the terror attacks of September 11, 2001 and were authorized in the USA PATRIOT Act.

According to congressional procedures, although the House of Representatives already approved a similar bill last March, the modified version adopted by the Senate must now go back to the House for final approval before it can be sent to the White House to be signed into law by President Trump.

The Senate reauthorization of the FISA provisions was supported by both Democrats and Republicans and easily surpassed the sixty-vote threshold necessary for passage.

Under the FISA rules, law enforcement is supposed to obtain approval from a special FISA court—an individual judge who reviews FBI and CIA requests in secret—before engaging in eavesdropping and surveillance operations on US citizens.

Significantly, the Senate vote restored FISA elements that have become known as the "business records," "lone wolf" and "roving wiretap" provisions in counterterrorism or espionage investigations, which were the subject of debate in recent months. All three of these rules had expired last December. They involve details about what law enforcement officers are permitted to do once the FISA court authorizes the secret surveillance of an individual.

As has been the case throughout the history of the PATRIOT Act as well as the revised USA Freedom Act (2015) adopted during the Obama era, the official political debate in the lead-up to the Senate vote on Thursday was never about halting the illegal government surveillance of the US public that has been going on for two decades, but rather how to extend it.

This fact was proven in the first of three amendments to the law that were discussed during the Senate deliberations. When Republican Senator Rand Paul from Kentucky proposed to block the use of FISA courts on US citizens because "you don't get a lawyer," his amendment was quickly rejected by 11–85.

A second amendment proposed by Republican Senator Mike Lee of Utah and Democratic Senator Patrick J. Leahy of Vermont was adopted with the support of 77 senators. The Lee-Leahy amendment lowers the threshold for the FISA court to appoint an "amicus curiae" advisor in cases that involve a "sensitive investigative matter."

Prompted by numerous abuses of FISA procedures uncovered during the 18 month-long "Russia probe" in 2018–2019, the proposal enables the court to appoint an advisor who, according to Lee, "can raise any issue with the court at any time and give both the amicus and the FISA court access to all documents and information related to the surveillance application."

According to publicly available FISA data, such amici have been used only 16 times among the thousands of surveillance applications that have been approved in the past five years. However, even this minuscule adjustment by the Senate was criticized by the US Justice Department, with national security spokesman Marc Raimondi stating, "We appreciate the Senate's reauthorization of three expired national security authorities. As amended, however [the bill] would unacceptably degrade our ability to conduct surveillance of terrorists, spies and other national security threats."

In a very significant vote, the Senate rejected a third amendment to the reauthorization bill that would have prevented federal law enforcement agencies from obtaining the internet browsing and search histories of American citizens without a warrant.

The vote on the amendment—drafted by Democratic Senator Ron Wyden of Oregon and Republican Senator Steve Daines of Montana—was 59–37, one vote shy of the

60 needed for adoption. The provision allowing the FBI and CIA access to internet browsing activity histories without court approval is contained in Section 215 of the act.

In discussing the implications of the warrantless data gathering on the Senate floor, Wyden warned, "Collecting this information is as close to reading minds as surveillance can get. It is digital mining of the personal lives of the American people … without this bipartisan amendment, it is open season on anybody's most personal information."

Wyden went on, "Under Section 215, the government can collect just about anything so long as it is relevant to an investigation. This can include the private records of innocent, law-abiding Americans. They don't have to have done anything wrong. They don't have to be suspected of anything. They don't even have to have been in contact with anyone suspected of anything."

Wyden also pointed out that tens of millions of Americans are now stuck at home during the pandemic and using the internet more than ever as their only connection to the outside world.

The corporate media was quick to point out that the amendment failed in part because four Senators did not cast a vote at all, including former Democratic presidential candidate and senator from Vermont Bernie Sanders, Republican Senator from Tennessee Lamar Alexander, Democratic Senator from Washington Patty Murray and Republican Senator from Nebraska Ben Sasse.

Concerns in the Senate were so high that the Wyden-Daines amendment might pass that Republican Majority Leader Mitch McConnell was reportedly working on his own measure to officially write into the law a provision that the government may collect records of internet search and browsing histories without a warrant.

According to *Recode*, "that amendment never came to the floor, likely because McConnell knew the Wyden-Daines amendment wouldn't get enough votes."

Privacy and civil rights groups have pointed to the dangers posed by the Senate reauthorization of the FISA domestic surveillance measures. However, they focused almost exclusively on the use of these tools in the hands of the Trump administration. Sean Vitka, senior policy counsel at Demand Progress, which led a coalition of 36 organizations including the American Civil Liberties Union (ACLU) and Freedom Works supporting privacy amendments to the legislation, said on Thursday, "[T]he loss of the warrant protection for browser history due to absences during the vote by supportive senators was a huge disappointment."

Vitka went on, "These protections are particularly critical given the Trump administration's history of abusing marginalized communities and others the president regards as enemies. Without more protections that would limit the information spy agencies can collect without a warrant, Congress will be giving the Trump administration the power to snoop on billions of data points for every single person in the United States."

However, the rejection of the Wyden-Daines amendment was bipartisan. That vote explicitly makes key aspects of the National Security Agency (NSA) data gathering operation, exposed by former intelligence contractor Edward Snowden in 2013, a legal government practice and shows that the electronic surveillance of US citizens is ongoing and has never stopped.

Snowden exposed a secret NSA program called XKeyscore that allowed intelligence analysts to search without authorization through databases containing the email messages, online chats and browsing histories of everyone. In the training materials leaked by the whistleblower, the NSA boasted that XKeyscore was the "widest-reaching" intelligence gathering system, which collects "nearly everything a typical user does on the internet" in real time.

In describing the NSA system to the *Guardian* in 2013, Snowden explained its purpose: "Because even if you're not doing anything wrong, you're being watched and recorded… You simply have to eventually fall under suspicion from somebody—even by a wrong call. And then they can use the system to go back in time and scrutinize every decision you've ever made, every friend you've ever discussed something with, and attack you on that basis, to sort of derive suspicion from an innocent life and paint anyone in the context of a wrongdoer."

Under conditions of an increase in strikes and class conflict arising from the pandemic and the deepening economic crisis, the state is bolstering its internet browser data gathering measures as part of the preparations for a major confrontation with the working class.

End-to-end encryption tools built into the mobile devices and apps are being used by tens of millions of people, blocking law enforcement's ability to monitor the content of individual communications. This means that the gathering of browsing data becomes one of the main electronic surveillance windows into the private and political activity of individuals and organizations that will be targeted for their opposition to the government and the capitalist system as a whole.