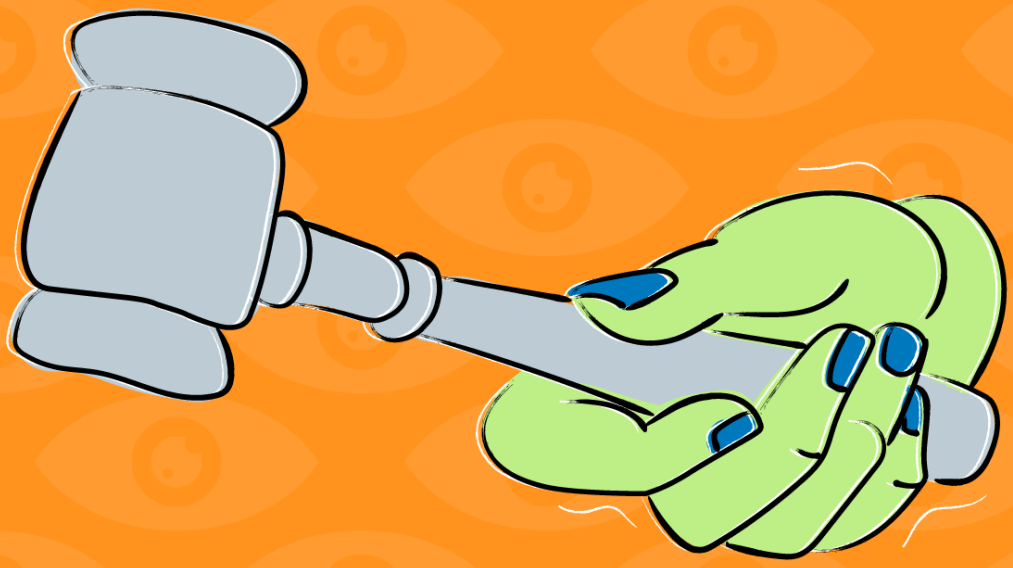

An Issue Brief on the

Foreign Intelligence Surveillance Act

RESTORE the FOURTH

What is FISA?

FISA, or the Foreign Intelligence Surveillance Act, is a federal law passed in 1978 that creates a structure for the US government to surveil and collect information, through digital or physical means, on "agents of foreign powers," without using probable cause warrants. It was originally introduced by Senator Edward Kennedy in reaction to several high-profile scandals involving executive spying, including Watergate as well as CIA, NSA and FBI spying revealed by the Church Committee. The thought was that it would bring the federal government's intrusive surveillance practices under statutory control. Sadly, it has not worked out that way.

The Foreign Intelligence Surveillance Court (FISC)

FISA deemed that foreign intelligence collection activities by the US government would not require an ordinary criminal warrant. A special court, the Foreign Intelligence Surveillance Court or FISC, had to find probable cause that the target was either a foreign power or an agent of a foreign power. The definition of "agent of a foreign power" as applied to U.S. persons necessarily involved criminal activity. So, the original FISA process looked quite similar to ordinary criminal warrants, except for the involvement of a special court.

Most FISC cases are heard by a single judge. Their decisions can be appealed to a higher court, but only by the government, because the interests of the target have historically not been represented in FISC proceedings—usually, only the state may present its case. FISC judges are appointed solely by the sitting Chief Justice, drawn from sitting Article III judges who have been Senate-confirmed. This higher court is called the Foreign Intelligence Surveillance Court of Review (FISC-R) and consists of a panel of judges.

Even during the original incarnation of FISA, before the post-9/11 expansions of the law, the communications of US persons[1] who were in contact with the intended target of surveillance could be collected without a separate warrant. And US persons could, and still can, be targeted directly under Title I of FISA, as long as the FISC finds probable cause and issues an individualized surveillance order. However, as FISA was originally designed, the court approved targets on an individual basis, so the original collection under FISA is unlikely to have affected many US persons. With changes to FISA after 9/11, the number of Americans affected has risen by an order of magnitude—but exact figures still remain unknown.

Criticisms of the FISC include that it defers too much to the intelligence community, operates in secret, doesn't publicize when it meets, generally hears no opposing viewpoints to those of the US intelligence community, and offers no opportunity to appeal a decision in the government's favor. It is incredibly rare for warrants requested for surveillance programs to be rejected.

The House and Senate Intelligence Committees

In 1976, in the immediate wake of the Church Committee and two years before FISA was passed, the House and Senate Intelligence Committees were established to provide oversight of an intelligence community that had clearly overstepped its bounds. In practice, these committees are limited in how much oversight they provide. Leadership usually chooses for these coveted committee positions, with a few honorable exceptions, legislators whose sympathies already lie with the intelligence community. Even worse, when so-called "Gang of Eight" provisions are invoked, as they were after 9/11 for the President's illegal mass surveillance, the executive is permitted to consult

1 This term of art, as defined in FISA, covers "a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power." Constitutionally, under United States v. Verdugo-Urquidez, 494 U.S. 259 (1990), it is possible that others with "substantial voluntary connections" to the United States could qualify as having Fourth Amendment protections.

only with the Chair and Vice-Chair or ranking minority member of each Intelligence Committee, deciding how much or how little is to be disclosed to the other 527 members of Congress. A further problem is that staffers for members of Congress not on the Intelligence Committee often lack the security clearances necessary to be allowed to see the materials on which the Intelligence Committee has passed judgment, so, unlike for other areas of government, they cannot evaluate the Committee's judgments independently.

The consequence of this is that back in 2013, the NSA was able to claim that what it was doing had been reviewed and approved by Congress (meaning, this small subset of Congress), and simultaneously, most Congressmembers were able to plausibly claim unawareness that such surveillance was happening.

Surveillance Outside FISA

Congress intended FISA to be the exclusive means by which foreign intelligence surveillance would be legally conducted. But it's worth noting that even after the passage of FISA, some illegal foreign surveillance continued under other authorities. Starting in the 1990s, for example, the Drug Enforcement Administration (DEA) collected phone metadata on a mass basis for several whole Caribbean countries, abusing a statutory subpoena authority to "permit" bulk collection. Similarly, in February 2001—almost immediately after assuming office—the Bush administration proposed agreements with telecommunications companies, outside FISA, that would collect phone billing data on a mass basis.

The September 11 Attacks

After the attacks of September 11, 2001, a frightened Congress weakened FISA and passed the USA PATRIOT Act. This allowed surveillance applications to be submitted for approval even when the primary purpose was not to gather foreign intelligence, meaning that FISA surveillance could theoretically be used for domestic law enforcement purposes just so long as intelligence gathering was still a "significant purpose." Going beyond this, based on secret opinions from the Office of Legal Counsel, the administration asserted inherent authority under Article II to skirt procedures laid out in FISA, and create the illegal mass surveillance program Stellar Wind. Stellar Wind intercepted metadata on virtually all cell phone calls in the United States.

According to the testimony of whistleblower Russ Tice, elements within the Bush administration went even farther, conducting political surveillance on presidential candidates and, more broadly, those with the ability to constrain the operations and budget of the intelligence services.

The FISA Amendments Act of 2008

Press reports began informing the public about some of the administration's illegal surveillance practices, starting in 2005, after the New York Times sat on the story for a year at the President's request. The administration's short-term response was to give their practices a veneer of legality, by declaring that the USA PATRIOT Act's infamous Section 215 could be used to provide legal cover. In secret, the Gang of Eight also allowed the Bush administration to expand the scope of the illegal surveillance it was conducting outside FISA.

Congress eventually responded to the scandal by passing the FISA Amendments Act of 2008. Rather than implementing reforms, it granted telecommunications companies legal immunity for their involvement in warrantless mass surveillance, and legalized Stellar Wind after the fact. Senator Kennedy argued passionately against it, and then did not vote on it. Then-Senator Obama voted for it; Senator Biden voted against it.

With the FISA Amendments Act, FISA had now pivoted from being focused on surveilling individuals to being focused primarily on mass surveillance. The amended FISA allowed for the use of "programmatic warrants"—not properly warrants at all, but court orders—which make a mockery of Fourth Amendment protections. The Fourth Amendment requires particularity; these court orders authorized surveillance on thousands of foreigners overseas at a time, including "incidental" collection on their contacts whether

American or not, without any individualized FISC review of who the targets were. In 2019, and again in 2020, there were over 200,000 "targets." In a digital environment where mail and texts are free to send and receive, the number of 'contacts' per person has exploded, as has the number of their international contacts. Consequently, the same law that authorized the warrantless collection of some Americans' communications in the 1970s, now authorizes the warrantless collection of (at least) millions of communications to or from Americans today. The exact number of such persons whose communications are captured every year remains secret, despite strenuous efforts by some members of Congress to force disclosure.

The FBI has also been steadily granted easier and easier access to the databases NSA collects under section 702 of the FISA Amendments Act, which covers US-to-foreign communications.[2] The latest estimate is that they conduct more than three million such searches per year. Restore the Fourth, as a Fourth Amendment oriented organization, believes that the FBI should need a warrant before accessing databases for domestic law enforcement purposes.

The Snowden revelations and the USA FREEDOM Act

In 2013, Edward Snowden came out of the NSA, providing documents to journalists that proved the extent of mass surveillance, and the failure of the Foreign Intelligence Surveillance Court to restrain it. As one example, the Snowden archive included a classified FISC ruling approving the ongoing collection of all cellphone metadata from Verizon Wireless subscribers, on the basis that any cellphone metadata record could be potentially relevant for foreign intelligence purposes. It would be hard to envision a more comprehensive violation of US persons' privacy rights.

Congress again responded in 2015, by passing the USA FREEDOM Act. This Act mandated greater transparency into programmatic court orders. It would not disclose the actual "selectors" used, but it required the FISC to regularly declassify and publish some of its rulings, review a sample of the selectors, and to invite the assistance of amici in situations requiring a novel interpretation of law. It prohibited bulk collection of all call detail records under a single court order, in exchange for statutory authorization for the government to programmatically collect records within two degrees of a target on an ongoing basis under Section 215. In the ensuing years, the NSA shut down its call detail records program because it failed to conform with the requirements of the USA FREEDOM Act, and also shut down the so-called "abouts" collection.

However, at the same time, the FBI deepened its exploitation of NSA records. The most recent compliance report from DNI illustrates the nature of the problem. It reports that in 2018, a single FBI "batch query" generated over 100,000 violations, which means that a single query can include requests for a vast amount of data on persons. It also reported that the number of 'facilities' (also known as selectors—e.g. telephone numbers and electronic communications accounts) by the NSA increased from 2017 to 2018 by nearly 25%, deepening the pool of foreign intelligence records from which the FBI draws.

In 2014 and 2015, the House passed a reform requiring warrants for this kind of "backdoor search," which was then stripped in conference with the Senate. In 2016, the aftermath of the Pulse shooting led the House to vote against requiring warrants. In 2021, the same reform was reintroduced as an amendment to the Commerce appropriations bill, but has not yet received a vote.

Trump Scrambles The Discourse

The unexpected election of President Donald Trump brought into the White House someone with no background in the surveillance state or government as a whole. He was convinced that President Obama had spied on his campaign operatives. Some of his campaign operatives,

2 This term should be treated with care. In this context, "US" more accurately means "with a probability greater than 50%, based on affirmative indicators available to NSA, the target is a US person within the meaning of FISA." If there is no information on the location or US person status of a target, NSA assumes the target to be a non-US person, and takes advantage of Section 702's looser rules relative to the rules governing "US to US" collection. So, for example, traffic on the encrypted browser Tor is automatically declared foreign, because the IP addresses of all users are routed via proxies and cannot be associated firmly with a country of origin, but in reality, a substantial proportion of Tor traffic is in fact between US persons.

such as Carter Page, were indeed under FISA surveillance as suspected agents of a foreign power.

US systems were, and are, poorly equipped to deal with situations where the executive branch's massive foreign intelligence collection butts up against the harm to democracy of the executive branch conducting surveillance on a presidential campaign from the opposing party. Political surveillance matters, and Trump's anger at FBI surveillance of his associates created political space for Republicans. They convened hearings on the "Crossfire Hurricane" scandal and, after 19 years of it abusive operation, allowed section 215 of the USA PATRIOT Act to lapse. In the course of that scandal, for the first time, FISA warrant applications were made public relating to Carter Page, which the Department of Justice's Inspector General found to have contained no fewer than 17 errors. Two applications were later invalidated, and the DHS Inspector General found that the internal FBI procedures requiring verification of each fact contained in warrant applications – the so-called "Woods Procedures" – are being continuously breached.

Conclusion

The only possible conclusion from all this is that FISA and its special courts are broken. What was intended in the beginning as a small workaround to the Fourth Amendment, to permit closely supervised approval of warrantless surveillance of individual agents of foreign powers and their contacts, has become an engine for mass surveillance.

Instead of close supervision, the surveillance state endures light guidance from an apparatus of courts and committees that regards transparency, rather than change, as the outer limit of the regulation they can impose. Neither the FISC court nor the Intelligence Committees dare to actually stop mass surveillance programs, even when there is plain and repeated evidence of abuses. There's more transparency than there was before the Snowden revelations, but that transparency is carefully structured so as to hide from the public key metrics that would enable us to judge how thoroughly we are surveilled, and how deeply embedded FISA surveillance is in the criminal justice system.

What does Restore the Fourth recommend?

(1) A warrant requirement on FBI backdoor searches;

(2) Requiring a reasonably accurate annual estimate of the median number of US persons whose communications are "incidentally" collected when targeting a non-US person;

(3) Annual disclosure of how many US person queries the FBI performs;

(4) Disclosure of the circumstances under which the government conducts foreign intelligence surveillance outside the FISA framework, inside the United States;

(5) Requiring the use by default of a civil liberties amicus to represent the interests of those whose communications would be intercepted were a FISC order to be approved;

(6) A ban on "programmatic" court orders and a return to individualized review by FISC of the targets for which FISA surveillance is to be approved;

(7) Prohibiting either wiretapping or collection of the communications of any candidate for public office in the United States, or paid employee of their campaigns, by any agency in the intelligence community, via the current system of FISA courts. Instead, such surveillance should be conducted only via an individualized probable cause warrant, brought for approval to an independent Article III judge.