Comments About FISA Courts

This article is from the "Edifying the Body" section of the Church of God Big Sandy's website, churchofgodbigsandy.com. It was posted for the weekend of Feb. 17, 2018.

By Dave Havir

BIG SANDY, Texas—While most of the articles in this space ("Edifying the Body") involve biblical or religious topics, our congregation occasionally provides articles with some historical information—involving information about the civil matters concerning our life in this world. Such is the case this week.

I will provide some information about the FISA courts by including various articles about the subject.

Supporters of this system express the need to have adequate security to protect the citizens of our republic against threats—especially terrorism. Critics of this system express their concern that this system can work against the Fourth Amendment of the U.S. Constitution.

The Fourth Amendment states: "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."

A government website described the benefit of this amendment as follows: "The Fourth Amendment originally enforced the notion that 'each man's home is his castle,' secure from unreasonable searches and seizures of property by the government. It protects against arbitrary arrests, and is the basis of the law regarding search warrants, stop-and-frisk, safety inspections, wiretaps, and other forms of surveillance, as well as being central to many other criminal law topics and to privacy law."

Let's take a look at some articles that provide information about this subject.

★ ★ ★ ★ ★

Looking back to 2017, here are excerpts from an article by Holly Yan titled "What is the FISA Court, and Why is It So Secretive?" that was posted at cnn.com on March 8, 2017.

It's a highly fortified courtroom where some of the most secretive government decisions get made. And you've probably never heard of it.

But in the coming days, the Foreign Intelligence Surveillance Court—known as the FISA court or FISC—will get more attention after President Donald Trump claimed he was wiretapped during the Obama administration. (Trump has not offered any evidence supporting his claim.)

So how exactly does the court work? And why does it have a controversial reputation? Here's what you need to know.

■ What is the FISA court?

The FISA court is a tribunal established in 1978 that decides whether to approve wiretaps, data collection and government requests to monitor suspected terrorists and spies.

It's just blocks away from the White House and Capitol, inside a secure area of the US District Court on Constitution Avenue. But it's completely out of the public eye.

Officials won't say exactly where the FISA courtroom is located inside the bunker-like complex. It's so secretive, the room is tightly sealed to prevent eavesdropping.

■ How does the court work?

Eleven federal district judges serve on a rotating basis, usually for one week at a time. All judges have a maximum term of seven years with the FISA court.

And only one person has the power to appoint the judges: Chief Justice of the United States John Roberts.

Congress doesn't need to confirm which federal judges take on the added responsibility of serving on the FISA court.

The judges come from across the country—in fact, they have to come from at least seven of the US judicial circuits.

In theory, those judges can issue warrants from anywhere, said University of Texas law professor and CNN contributor Steve Vladeck. But in practice, the judges usually issue orders during the weeks when they're "on rotation" at the FISA court in Washington.

■ What was the original goal of the FISA court?

It started back in 1978 with the court's namesake, the Foreign Intelligence Surveillance Act. That law was enacted "to authorize electronic surveillance to obtain foreign intelligence information."

Back then, the Cold War was in full force. And foreign spying—not terrorism—was the big concern.

FISA also came in the wake of the Watergate scandal and after revelations that the government had been using national security as a pretext to spy on citizens, such as the FBI's spying on the Rev. Martin Luther King Jr.

The FISA court started by granting individual warrants for collecting certain pieces of electronic data. But big changes came in the 21st century.

■ What changed?

After the 9/11 terror attacks, the court started authorizing more sweeping collections of mass data.

In 2008, for example, changes in surveillance laws gave the attorney general and the national intelligence director more authority to order "mass acquisition" of electronic traffic, as long as it's related to a terror or espionage investigation.

In other words, a FISA court judge could authorize the collection of a telecom company's entire database of phone records, if it's deemed relevant to counterterrorism efforts.

■ Why has it come under criticism?

Controversy over the FISA court's broad powers blew up in 2013, when Edward Snowden revealed a secret court order approving the mass collection of metadata from telecom giant Verizon and Internet companies such as Apple, Facebook, Google, Microsoft and Yahoo.

That led to a heated debate about the limits of privacy and due process.

The FISA court does hear challenges, though. In 2013, Yahoo scored a win when FISC ruled that the government must publish court papers from 2008 detailing Yahoo's objections to releasing users' data without a warrant.

But there are other reasons the FISA court has come under fire.

Because it's closed off from the public and only hears the government's side, some say the court basically "rubber-stamps" any request from the government.

The FISA court does routinely send applications back to the government to be modified and narrowed, Vladeck said. But the vast majority of applications eventually get approved.

Between 1979 and 2015, virtually all requests for surveillance were approved by the FISA court, though some were modified, according to the Electronic Privacy Information Center, a privacy watchdog group.

And a 2016 Justice Department report showed that of the 1,457 requests made to the FISA court in 2015 for permission to conduct electronic surveillance, one was withdrawn by the government. As for the rest, "FISC did not deny any applications in whole, or in part," the Justice Department said.

★ ★ ★ ★ ★

Looking back to 2014, here is an article by Dia Kayyali titled "The Way the NSA Uses Section 702 Is Deeply Troubling; Here's Why" that was posted at eft.org (Electronic Frontier Foundation) on May 9, 2014.

The most recent disclosure of classified NSA documents revealed that the British spy agency GCHQ sought unfettered access to NSA data collected under Section 702 of the FISA Amendments Act. Not only does this reveal that the two agencies have a far closer relationship than GCHQ would like to publicly admit, it also serves as a reminder that surveillance under Section 702 is a real problem that has barely been discussed, much less addressed, by Congress or the President.

In fact, the "manager's amendment" to the USA FREEDOM Act, which passed unanimously out of the House Judiciary Committee, has weakened the minimal changes to Section 702 that USA FREEDOM originally offered. Although Representative Zoe Lofgren–who clearly understands the import of Section 702–offered several very good amendments that would have addressed these gaps, her amendments were all voted down. There's still a chance though–as this bill moves through Congress it can be strengthened by amendments from the floor.

Section 702 has been used by the NSA to justify mass collection of phone calls and emails by collecting huge quantities of data directly from the physical infrastructure of communications providers. Here's what you should know about the provision and why it needs to be addressed by Congress and the President.

■ Most of the discussion around the NSA has focused on the phone records surveillance program. Unlike that program, collection done under Section 702 captures content of communications. This could include content in emails, instant messages, Facebook messages, web browsing history, and more.

■ Even though it's ostensibly used for foreign targets, Section 702 surveillance sweeps up the communications of Americans. The NSA has a twisted, and incredibly permissive, interpretation of targeting that includes communications about a target, even if the communicating parties are completely innocent. As John Oliver put it in his interview with former NSA General Keith Alexander: "No, the target is not the American people, but it seems that too often you miss the target and hit the person next to them going, 'Whoa, him!'"

■ The NSA has confirmed that it is searching Section 702 data to access American's communications without a warrant, in what is being called the "back door search loophole." In response to questions from Senator Ron Wyden, former NSA director General Keith Alexander admitted that the NSA specifically searches Section 702 data using "U.S. person identifiers," for example email addresses associated with someone in the U.S.

■ The NSA has used Section 702 to justify programs in which the NSA can siphon off large portions of Internet traffic directly from the Internet backbone. These programs exploit the structure of the Internet, in which a significant amount of traffic from around the world flows through servers in the

United States. In fact, through Section 702, the NSA has access to information stored by major Internet companies like Facebook and Google.

■ Section 702 is likely used for computer security operations. Director of National Intelligence James Clapper noted Section 702's use to obtain communications "regarding potential cyber threats" and to prevent "hostile cyber activities." Richard Ledgett, Deputy Director of NSA, noted the use of intelligence authorities to mitigate cyber attacks.

■ The FISA Court has little opportunity to review Section 702 collection. The court approves procedures for 702 collection for up to a year. This is not approval of specific targets, however; "court review [is] limited to 'procedures' for targeting and minimization rather than the actual seizure and searches." This lack of judicial oversight is far beyond the parameters of criminal justice.

■ Not only does the FISA Court provide little oversight, Congress is largely in the dark about Section 702 collection as well. NSA spying defenders say that Congress has been briefed on these programs. But other members of Congress have repeatedly noted that it is incredibly difficult to get answers from the intelligence community, and that attending classified hearings means being unable to share any information obtained at such hearings. What's more, as Senator Barbara Mikulski stated: "'Fully briefed' doesn't mean that we know what's going on." Without a full picture of Section 702 surveillance, Congress simply cannot provide oversight.

■ Section 702 is not just about keeping us safe from terrorism. It's a distressingly powerful surveillance tool. While the justification we've heard repeatedly is that NSA surveillance is keeping us safer, data collected under Section 702 can be shared in a variety of circumstances, such as ordinary criminal investigations. For example, the NSA has shared intelligence with the Drug Enforcement Agency that has led to prosecutions for drug crimes, all while concealing the source of the data.

■ The President has largely ignored Section 702. While the phone records surveillance program has received significant attention from President Obama, in his speeches and his most recent proposal, Section 702 remains nearly untouched.

■ The way the NSA uses Section 702 is illegal and unconstitutional–and it violates international human rights law. Unlike searches done under a search warrant authorized by a judge, Section 702 has been used by the NSA to get broad FISA court authorization for general search and seizure of huge swathes of communications. The NSA says this is OK because Section 702 targets foreign citizens. The problem is, once constitutionally protected communications of Americans are swept up, the NSA says these communications are "fair game" for its use.

■ Innocent non-Americans don't even get the limited and much abused protections the NSA promises for Americans. Under international human rights law to which the United States is a signatory, the United States must respect the rights of all persons. With so many people outside the United States keeping their data with American companies, and so much information being

swept up through mass surveillance, that makes Section 702 the loophole for the NSA to violate the privacy rights of billions of Internet users worldwide.

The omission of Section 702 reform from the discourse around NSA surveillance is incredibly concerning, because this provision has been used to justify some of the most invasive NSA surveillance. That's why EFF continues to push for real reform of NSA surveillance that includes an end to Section 702 collection.

You can help by educating yourself and engaging your elected representatives. Print out our handy one-page explanation of Section 702. Contact your members of Congress today and tell them you want to see an end to all dragnet surveillance, not just bulk collection of phone records.

★ ★ ★ ★ ★

Looking back to 2017, here is an article by Josh Magness titled "FISA Section 702: Is Warrantless Surveillance National Security or a Hit to Privacy?" that was posted at mcclatchydc.com on March 1, 2017.

Section 702 of the Foreign Intelligence Surveillance Act might be necessary to protect U.S. National Security or it might infringe on the privacy rights of Americans—it just depends on who you ask.

The debate over what works and what doesn't within the section, which grants the Director of National Intelligence and Attorney General ability to authorize warrantless surveillance of non-US citizens located abroad, was the subject Wednesday at a House Judiciary Committee hearing.

Rep. Bob Goodlatte, the Republican chairman of the House Judiciary Committee, opened the meeting with a conciliatory tone. He began by claiming the section is "an important safeguard" before conceding that its opponents, many of them Democrats, fear it will infringe on the privacy of Americans whose communications may be inadvertently swept up during information collection on foreign targets.

"We must ensure that our protection doesn't come at the expense of cherished liberty," Goodlatte said. "Strong and effective national security tools like Section 702 and civil liberties can and must coexist."

The controversial section, codified into law in 2008 and renewed for five years in 2012, is set to expire Dec. 31. That deadline prompted lawmakers to host a hearing—the first part classified, the second unclassified—with national security experts, government officials and others experts lending their opinion on the provision.

Rep. Ted Lieu, a Democrat from California's 33rd Congressional District, asked the panel how Section 702 is constitutional under the Fourth Amendment if it leads to the inadvertent collection of the communications of Americans that can be used later by the FBI for any crime.

Jeffrey Kosseff, assistant professor in the United States Naval Academy's cyber science department, said only the collection of data, and not subsequent search of already-collected data, is a Fourth Amendment issue.

"The database can be later queried for information," he said. "The issue is whether the initial collection and entire program is lawful."

Elizabeth Goitein, co-director of the Liberty and National Security Program at the New York University School of Law, maintained her skepticism about the constitutionality of the law.

Both the FISA court and the federal government, Goitein said, have interpreted that Section 702 grants the right to collect information "to, from or about the target." That "about," she said, opens up the communications of many Americans to data collection if they mention a key term or person the National Security Agency and Office of the Director of National Intelligence is monitoring.

To solve this issue, Goitein, who said 250 million internet communications were swept up under Section 702 in 2011, said the government should seek "much stricter minimization procedures" to avoid sweeping up the information of American citizens.

One way to do that, she said, is to use an IP address as a proxy to determine whether information collected is from an American citizen or a foreign national.

Another way to maintain the surveillance powers of Section 702 while strengthening American trust in the system would be to require an annual review of how it operates, said Adam Klein, a senior fellow at the bipartisan Center for a New American Security think tank.

"Once a year, the director of national intelligence and the attorney general must submit to the (FISA court) a joint certification specifying how the program will be administered and what safeguards apply," he said.

Rep. Raúl Labrador, an Idaho Republican, tied the issue to the leaking of former National Security Advisor Michael Flynn's communications with Russia that eventually lost him his job. He said Flynn's ouster "had a chilling effect on me because I thought my political opponents could use my own personal information against me in the future."

"Your communications could be acquired under Section 702," Goitein responded, "and that is something that should concern you."

Section 702 gained notoriety after Edward Snowden leaked information about the existence of the PRISM Program, an NSA program that gathers data through U.S. internet companies. The program is a method of information collection run under Section 702.

Under current law, the attorney general and director of national intelligence submit a request to the FISA court, asking to gather data from non-U.S. citizens under certain "targeting and minimization procedures"—monitoring non-U.S. citizens potentially harboring weapons of mass destruction, for example.

If the request is approved, the NSA can gather information on any non-U.S. citizen who falls under those parameters for up to a year period. Before the section became law, the two had to seek approval from the FISA court for the data collection of each individual non-U.S. citizen.

It still remains to be seen what would take the place of Section 702 after it expires—and whether privacy concerns would be answered.

In his statements before the panel, Rep. John Conyers of Michigan, the ranking Democrat in the committee, reminded his colleagues that the future of the law, while still uncertain, must eventually be reauthorized or replaced.

"As the sunset of this authority draws near," Conyers said, "the manner in which one collects, maintains and disseminates this information is only lawful if Congress says it is."

★ ★ ★ ★ ★

An article by Debbie Lord titled "What is a FISA Warrant?" was posted at ajc.com on Feb. 1, 2018. Following is the article.

Here's a look at the FISA Court and FISA warrants.

■ What is the FISA Court?

A warrant to wiretap someone suspected of spying with or for a foreign government is issued by the Foreign Intelligence Surveillance Court—or FISA Court. The court is actually a tribunal whose actions are carried out in secret. The tribunal has the authority to grant warrants for electronic surveillance. The court has 11 members, all federal judges. The judges serve seven-year terms. The chief justice of the U.S. Supreme court selects the judges.

■ When was this court established?

The Foreign Intelligence Surveillance Act of 1978 created the court and set up the rules for wiretapping of suspected spies.

■ What is its mission?

The court was set up to either approve or deny warrants requested by the United States government for surveillance of foreign spies inside of the United States.

That warrant requests and the intelligence gathering is generally done by federal law enforcement agencies or U.S. intelligence agencies. The authorization allows for wiretapping a "foreign power or an agent of a foreign power" (which could include American citizens) suspected to be engaged in espionage or terrorism. Methods used in an investigation include electronic surveillance, physical searches and other actions. Generally, the attorney general signs the warrant requests.

■ How does it work?

When an agency requests a warrant from the FISA Court, the request falls to one of the 11 judges who sit on the court. It is up to that judge to either deny or approve the request for a surveillance warrant. If the request is denied, there is an avenue for appeal of the ruling, but that has happened only a handful of times in the history of the court.

■ Is there any other way to get surveillance warrant?

An alternate way a warrant for surveillance can be obtained is if the U.S. attorney general declares an emergency and authorizes the employment of the surveillance. The attorney general must notify a judge on the FISA Court, and must, within seven days, apply for a warrant for the action.

■ What rules must they follow?

While the proceedings are secret, there are rules that have to be followed. The statute that created FISA Courts bars targeted electronic surveillance in the United States unless there is evidence that a foreign power or agent of a foreign power is involved. Also, there has to be evidence that the facility—an email address or phone number, for instance—is being used by the foreign power or agent. In addition, the government must show that the information to be collected is "relevant" to any investigation of foreign espionage or terrorism.

The warrants are generally issued for up to 12 months, and they authorize the government to collect "bulk information." That means that while Americans on U.S. soil who are not agents of a foreign government are not targeted, information collected could include communication between U.S. citizens.

■ Can public see these warrants, they can see others?

The court's dealings are secret, the hearings closed to the public. Records are made and kept, but those records are generally not made available to the public.

■ How many have been turned down?

As of 2013, the FISA court has denied only 12 warrants since its inception. It has granted more than 34,000 requests since its inception.

★ ★ ★ ★ ★

The following list titled "Current Membership—Foreign Intelligence Surveillance Court" is posted at us courts.gov.

■ Rosemary M. Collyer (presiding)—District of Columbia—March 8, 2013—March 7, 2020

■ James E. Boasberg—District of Columbia—May 19, 2014—March 18, 2021

■ Rudolph Contreras—District of Columbia—May 19, 2014—May 18, 2023

■ Anne C. Conway—Middle District of Florida (11th)—May 19, 2016—May 18, 2023

■ Raymond J. Dearie—Eastern District of New York (2nd)—July 2, 2012—July 1, 2019

■ Claire V. Eagan—Northern District of Oklahoma (10th)—February 13, 2013—May 18, 2019

■ James P. Jones—Western District of Virginia (4th)—May 19, 2015—May 18, 2022

■ Robert B. Kugler—District of New Jersey (3rd)—May 19, 2017—May 18, 2024

■ Michael W. Mosman—District of Oregon (9th)—May 4, 2013—May 3, 2020

■ Thomas B. Russell—Western District of Kentucky (6th)—May 19, 2015—May 18, 2022

■ F. Dennis Saylor IV—District of Massachusetts (1st)—May 19, 2011—May 18, 2018