CENTER FOR DEMOCRACY & TECHNOLOGY

CDT FISA 702 Issue Brief: A Warrant Rule for US Person Queries Would Not Prevent Victim-Focused Queries

A critical reform to Section 702 of the Foreign Intelligence Surveillance Act ("FISA 702") that Congress is considering is a warrant rule for US person queries: To run queries for Americans' communications obtained via FISA 702, the government would first need to obtain the same type of warrant that would be required for direct collection of those communications.[1] Such a warrant could be obtained under multiple authorities, including FISA Title I (based on probable cause that the target is an agent of a foreign power) and the Wiretap Act (based on probable cause that the surveillance will return evidence of a specified crime). The government has emphasized that some of its US person queries are conducted on identifiers associated with *victims* of foreign plots, and claimed it would be impossible to run victim queries if a warrant rule is imposed. This is untrue.

A Warrant Rule Would Not Prohibit Victim-Focused Queries as a Matter of Law

Critics of reform have claimed that a warrant rule would make it legally impossible to run queries on the identifiers of individuals not suspected of wrongdoing (such as victims). Earlier this year assistant director of the FBI's Directorate of Intelligence Tonya Ugoretz argued that for queries of cyberattack victims, "because the … U.S. person [whose] information that we are querying is not the target of investigation, we would not be able to meet the standard for a warrant." The President's Intelligence Advisory Board report on FISA 702 similarly claimed that prior victim-focused queries would have been impossible with a warrant rule "because there would have been no probable cause that the user of the U.S. selector was a foreign power or agent of a foreign power." An intelligence community issue brief also implied that all victim queries would be blocked because "the IC may not have probable cause to believe the U.S. person is a foreign power or agent of a foreign power."

These claims that a warrant requirement would preclude victim-focused queries are inaccurate as a matter of law. 18 USC 2518—the Wiretap Act rule for obtaining a warrant that could be used as a model for a warrant requirement for US person queries—requires a judge to determine that a particular crime has occurred, and that "there is probable cause for belief that particular communications concerning that offense will be obtained through such interception." Thus, a warrant rule would not require that the subjects of all queries be targets of investigations or suspected agents of foreign powers. Victims' identifiers *could* be queried on as well, so long as the government could show a judge there was probable cause that such a query would return evidence of a specifically enumerated offense; existence of a victim means there is a crime for which evidence can be sought.

The Department of Justice Has Repeatedly Obtained Warrants for Victim-Focused Searches

The claim that it is impossible to obtain warrants focused on victims is also disproven by precedent. The Department of Justice has repeatedly received court approval for search warrants that pertain to victims:

- *Dismantling the Kelihos Botnet (April 2017):* The government applied for several search warrants to access victims' computers infected with the Kelihos botnet malware, disrupt communications with the botnet, and obtain IP addresses and routing information from infected computers. The warrants permitted law enforcement to redirect victims' Kelihos-infected computers to a substitute server and to record their IP addresses and associated routing information, which then could be provided to Internet service providers.[2]
- *Disrupting the Joanap Botnet (January 2019):* The government used search warrants to access victims' devices to disrupt the North Korean Joanap botnet. The original warrant allowed the FBI to search compromised computers, and a renewal warrant allowed the government to direct compromised computers to connect with FBI controlled computers. The warrants, which were authorized based on probable cause of computer crimes, also allowed the government to then collect limited identifying information about other Joanap-infected peers (i.e., IP addresses, port numbers, and connection timestamps).[3]

- *Microsoft Exchange Server Web Shell Removal (April 2021):* After disrupting a Microsoft Exchange Server vulnerability, the FBI and CISA found a number of web shells (code that provides malicious hackers with a backdoor to continually access web servers) still present on victims' devices. The FBI conducted operations pursuant to a search warrant that authorized it to search servers of hacking victims and remove web shells, based on probable cause that the searches would uncover evidence of computer crimes.[4]
- *Cyclops Blink Malware Removal (April 2022):* The government used a search warrant—authorized based on probable cause of computer crimes—to access vulnerable Internet-connected firewall devices and remove malware known as "Cyclops Blink." The warrant permitted the FBI to electronically access victim devices to (1) retrieve data from the malware, (2) remove the malware, and (3) block remote access to the device's management panel.[5]
- *SNAKE Malware Removal (May 2023):* The Department of Justice completed an operation to remove Russian malware known as "Snake" by accessing compromised devices. The court authorized the FBI to hack into victims' computers that were compromised by Snake, and to seize electronically stored information based on probable cause of violations of computer crime laws.[6]

These cases make clear that obtaining a warrant for victim-focused searches is neither impossible nor even a novel concept for the Department of Justice. It has repeatedly engaged in this practice, and could do so in obtaining a warrant for FISA 702 US person queries.

Many Victim Queries Could Be Exempt From Warrant Requirements

All warrant rules contain limited but reasonable exceptions, such as when individuals consent to a search or in exigent circumstances. These exceptions would also apply to a warrant requirement for US person queries. In discussing victim queries, the government has emphasized scenarios such as cyberattacks on infrastructure and plots to kidnap or assassinate US government officials. Such scenarios could often be addressed by obtaining the consent of the victim. For example, after the Colonial Pipeline hack, the FBI could have obtained consent to run a query of communications collected under Section 702 with the company name, IP address, or other company identifiers as a selector as it undertook its investigation.

A Consistent Warrant Rule Is Critical to Preventing Abuse

Having a consistent warrant rule for US person queries of FISA 702 data—including for victim-focused queries—is not just feasible, it is also essential to preventing misconduct. Some of America's worst surveillance abuses were conducted under the pretext of protecting victims, including surveillance of Dr. Martin Luthor King Jr. and other civil rights leaders and nefarious COINTELPRO activities.[7] Additionally, improper US person queries—such as of a sitting Congressman—have been justified as seeking to determine if the American was the target of a foreign influence operation. There will certainly be instances where the government seeks to conduct queries on the identifiers of victims for legitimate reasons, and it should be able to do so based on a probable cause showing that such queries will return evidence, in emergencies, or with the consent of the victim. But a blanket exemption would needlessly open the door to misconduct.

For more information, please contact Jake Laperruque, Deputy Director of CDT's Freedom, Security & Technology Project, at jlaperruque@cdt.org, or Project Director Greg Nojeim at gnojeim@cdt.org.

Endnotes

1 This issue brief generally refers to "US person queries" as shorthand for queries for communications content, which we believe should require a warrant. The government also conducts queries that return communications metadata rather than content - under proposed reforms, such queries would *not* require a warrant, and could be made with court approval based on the lower standard that is required for compelled disclosure of metadata.

2 Appl. for a Search Warrant ("Kelihos Search Warrant") at 5, *In re Appl. for a Warrant to Under Rule 41 of the Federal Rules of Criminal Procedure to Disrupt the Kelihos Botnet*, Case No. 3:17-mj-00-135-DMS (D.Alaska), https://www.justice.gov/opa/press-release/file/956521/download.

3 Appl. for a Search Warrant at 4, *In re Botnet of Compromise Computers*, Case No. 18-MJ-02739 (C.D. Cal), https://perma.cc/5XAW-WTZT.

4 Aff. in Support of an Appl. under Rule 41(b)(6)(B) for a Search Warrant, I*n re Application for a Warrant to Search Certain Microsoft Exchange Servers Infected with Web Shells*, Case No. 4:21-mj-755 (S.D. Tex.), https://perma.cc/6QJY-VVFG.

5 Aff. by Telephonic or Other Reliable Electronic Means In Support of an Application for Search Warrants at 6, *In re Application for Warrants to Search Certain Servers Controlling Cyclops Blink Botnet*, Case No. 22-437 (W.D. Pa.), https://perma.cc/9HKY-6BK9.

6 Aff. in Support of an Appl. under Rule 41(b)(6)(B) for a Search Warrant, *In the Matter of the Search of Information Associated with Computers Constituting the Snake Malware Network*, Case No. 23-mj-0428 (E.D.N.Y.), https://perma.cc/C4G7-BDHS.

7 See, Jake Laperruque, The Center for Democracy & Technology, "There Is No "Defensive Search" Exception to the Fourth Amendment: Why a Consistent Warrant Rule Is Necessary to Fix FISA Section 702," May 1, 2023. https://perma.cc/8DF5-C7HK.