The SAFE Act – Q & A

Requirement of a Probable Cause Order to Access U.S. Persons' Communications

Q. What are "backdoor searches"?

A. Section 702 authorizes warrantless surveillance and so it can only be targeted at foreigners outside the United States. But it inevitably sweeps in Americans' communications. To protect Americans' constitutional rights, Congress directed the government to "minimize" the retention and use of this information. Instead, intelligence agencies routinely run electronic queries of Section 702 data for the express purpose of finding and reviewing Americans' phone calls, text messages, and emails. The FBI performed 200,000 of these warrantless "backdoor searches" in 2022 alone.

Q. What are some of the abuses that have resulted from this practice?

A. In recent years, the FBI has engaged in what the FISA Court called "persistent and widespread" violations of the internal rules governing backdoor searches. Violations include searches for the communications of members of Congress; multiple U.S. government officials, journalists, and political commentators; more than 19,000 donors to a congressional campaign; and "tens of thousands" of Americans engaged in "civil unrest," including racial justice protesters.

Q. Didn't the FBI's recent procedural changes put a stop to these violations and abuses?

A. No. The intelligence community cites only the *percentage* drop in violations in the hope of obfuscating the massive quantity of improper queries that are continuing to occur. According to the government's own numbers, violations are continuing to occur at a rate of *4,000 per year*. And flagrant abuses are still happening, such as searches for the communications of a U.S. Senator, a state senator, and a state court judge who contacted the FBI to report civil rights violations by a local police chief.

Q. How does the SAFE Act address these problems?

A. The SAFE Act allows intelligence agencies to search Section 702 data for Americans' communications without any court order, but if the search returns results (which happens in less than two percent of cases), the agencies must obtain a warrant or FISA Title I order before accessing the content of the communications. This requirement includes exceptions for exigent circumstances, consent (in cases where the subject of the search is a potential victim of a foreign plot), and certain cybersecurity-related searches. It also permits queries for metadata without any court approval.

Q. Would this warrant requirement jeopardize national security?

A. No. While the ability to collect and review *foreigners'* communications under Section 702 provides significant national security value, the Privacy and Civil Liberties Oversight Board (PCLOB), after an extensive review, concluded that the government had provided "little justification … on the relative value of the close to 5 million [backdoor] searches conducted by the FBI from 2019 to 2022." In the few instances in which backdoor searches proved useful, the Chair of the PCLOB observed that the government either would have been able to get a warrant or could have invoked one of the exceptions in the SAFE Act.

Q. The administration says that a warrant requirement "reflects a lack of understanding about how these queries work," because the government "almost never" has probable cause when it conducts these searches. Isn't that a good argument against requiring a warrant?

A. Contrary to the administration's claim, the SAFE Act's sponsors fully understand that the government is routinely examining Americans' private communications without anything approaching probable cause. That's exactly *why* the SAFE Act includes a warrant requirement: to end this violation of Americans' constitutional rights.

Q. The administration says that the exception for situations involving "imminent death or serious bodily harm" will "rarely" apply. Is that true?

A. We hope so! But those are also the cases in which it is most vital that the government have quick access to information. An exception is hardly meaningless because it applies in the rare instance where it could prevent imminent harm. Indeed, courts have long recognized the vital importance of an "exigent circumstances" exception to the Fourth Amendment, and the SAFE Act—far from imposing an impossible standard—mirrors the exception courts have adopted.

Q. How does the exception for "consent" work?

A. In cases where the subject of the query is a potential victim of a foreign plot, the government can perform the query with that person's consent. The administration suggests that obtaining consent could take too long in situations where there is a rapidly unfolding threat. If the threat is sufficiently severe, however, the government could invoke the exigent circumstances exception. Moreover, nothing prevents the government from obtaining advance consent from a list of high-risk targets of espionage (e.g., high-ranking officials) or cyberattacks (e.g., providers of critical infrastructure). Again, the idea of a consent exception is not a radical and untested notion; it is *standard practice* under the Fourth Amendment, and law enforcement agencies regularly take advantage of it.

Q. What if, as the administration says, "it is often not clear whether the person is a victim or perpetrator of malicious activity?"

A. In such cases, the person is a potential suspect, and the query results could become the primary basis to prosecute them. This is precisely the scenario in which the government should be required seek a warrant. If the government lacks probable cause and no exigent circumstances exist, it should not be reading an American's private communications.

Q. How does the SAFE Act accommodate the need to protect against cyberattacks?

A. There are four exceptions that together provide the government with ample power to quickly conduct queries and obtain needed information to discover and respond to potential cyberattacks. First, the bill does *not* require any warrant or court approval to conduct metadata queries. This is essential for cybersecurity because, as the government itself has highlighted, its use of U.S. person queries in the cyber context has focused on tracing network traffic and suspicious internet contact efforts. Second, the bill provides a direct exception for queries focused on malware code, which will cover many types of cyberattacks (e.g., exploitation of zero-day vulnerabilities). Third, for spear phishing and denial of service attacks, the government can obtain consent from potential victims (including advance consent from a list

of high-risk targets, as noted above). And fourth, where an attack may have imminent kinetic effects (e.g., attacks targeting hospitals or critical infrastructure), the government may invoke the "exigent circumstances" exception.

Q. The bill's warrant requirement applies not just to U.S. persons (American citizens and legal permanent residents), but others inside the United States. Why is that? And is the administration correct that this would prevent the FBI from running a query if it learned that "an individual with connections to a major international terrorist organization had just arrived at JFK airport"?

A. FISA itself requires the government to obtain a probable cause order if it wants to conduct electronic surveillance of *either* a U.S. person *or* a person inside the United States. The SAFE Act's requirement is scoped to FISA to ensure that backdoor searches cannot be used to evade FISA's protections. While critically important, those protections are not overly demanding when it comes to non-U.S. persons: If the FBI can show that someone has "connections to a major international terrorist organization," it can certainly obtain a court order under Title I of FISA, and would therefore be able query the Section 702 data under the SAFE Act.

Q. Why should the government need a warrant to search lawfully collected information?

A. What renders warrantless surveillance under Section 702 "lawful" is the government's certification that it is targeting *only* foreigners abroad. Queries that target U.S. persons turn this premise on its head. Moreover, as the Second Circuit noted in this very context, "[L]awful collection alone is not always enough to justify a future search." That case is still ongoing, but the court clearly cast doubt on the constitutionality of warrantless U.S. person queries.

Reforms to limit government purchases of Americans' sensitive data from data brokers

Q. What problem do these reforms seek to solve?

A. Government agencies are increasingly using data brokers to evade constitutional and statutory privacy protections. For instance, the Supreme Court has held that the government needs a warrant to obtain cell phone location information, because this data can reveal highly sensitive information about a person's associations, habits, and even beliefs. But the government interprets this ruling to apply only when it *compels* the production of information, not when it pays for the data. Federal agencies are thus buying up massive databases of this Fourth Amendment-protected information without any legal process whatsoever, let alone probable cause and a warrant.

Q. How would the SAFE Act address this problem?

A. The SAFE Act prohibits law enforcement and intelligence agencies from purchasing Americans' data if they would otherwise need a warrant, court order, or subpoena to obtain it. It does not apply to information a person has made public (such as public-facing social media posts), information available through widely distributed media (such as newspapers), or information available from public records. It also has several exceptions, including for emergencies and for certain critical government functions. And if the government is unable to identify and exclude Americans' data from larger data sets, it allows the government to purchase the data set and then apply minimization procedures post-purchase.

Q. Why do these reforms belong on a bill to reauthorize Section 702?

A. The backdoor search loophole and the data broker loophole are two of the government's largest sources of warrantless access to Americans' Fourth Amendment-protected information. If Congress reforms Section 702 in isolation, the government will simply increase its reliance on data broker purchases. Achieving the underlying goal of Section 702 reform thus requires addressing both of these problems together.

Q. The administration says that "there is often no way to establish even a 'reasonable belief' of whether a particular individual was inside the United States at the time a particular piece of data was created." Doesn't that make the SAFE Act's reforms unworkable?

A. That's exactly why the SAFE Act allows the government to "overcollect" in cases where it cannot establish whether a given data set includes protected information. If the government later determines that information relates to a person inside the United States, it must purge the data unless one of several exceptions applies.

Q. The administration also argues that these reforms would "significantly limit the government's acquisition of all frontier AI systems (e.g. large language models)." Is that a serious concern?

A. The SAFE Act will have no effect on the government's acquisition of large language AI models that draw from open sources. Many AI models are trained on data from the Internet that would not qualify as protected data under the SAFE Act. If, however, the government seeks to acquire AI systems that ingest Americans' private, Fourth Amendment-protected data, that is extremely concerning and only underscores the need for this legislation.

Q. The SAFE Act imposes restrictions on government acquisition of Americans' personal data that do not apply to private companies. Why make that distinction?

A. Congress can and should consider legislation to more broadly protect the privacy of Americans' data. However, government collection of Americans' personal information is uniquely problematic. The government has a wide range of coercive powers over the American people that private companies simply don't have, including the power to investigate, arrest, jail, deport, tax, audit, and fine. That is why the Fourth Amendment applies to the government and not to private actors.

Q. Won't foreign governments, such as those of China, Russia, or Iran, still be able to purchase this data?

A. As the administration points out, it is in the process of developing regulations to "prevent the large-scale transfer of Americans' sensitive personal data to countries of concern." Congress is working to rapidly advance legislation that would do the same; last month the House passed the Protecting Americans' Data from Foreign Adversaries Act by a 414-0 vote. In the meantime, the fact that China does not respect Americans' privacy rights is no reason for our own government to show the same disrespect. We should not emulate the Chinese government when it comes to upholding basic freedoms, including freedom from unwarranted government scrutiny. We hold the U.S. government to a higher standard, and rightly so.