Bellarmine Law Society Review

Volume XV | Issue I Article V

Foreign Surveillance Turned Domestic: The Foreign Intelligence Surveillance Act (FISA) On Trial

Benjamin Ward
Boston College, wardbs@bc.edu

FOREIGN SURVEILLANCE TURNED DOMESTIC: THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA) ON TRIAL

BENJAMIN WARD [1]

Abstract: This review first contextualizes the history of the Foreign Intelligence Surveillance Act (FISA) and explores the ways that its scope has expanded through amendments such as Section 702. In addition, this review considers the procedures used in FISA surveillance, with a focus on the practices of minimization and querying. With this grounding, the review then investigates a recent case (United States v. Hasbajrami) where the defendant, a U.S. person, challenged the use of FISA and Section 702 against him. The court ruled that warrantless Section 702 surveillance, as it was carried out against Hasbajrami, violated his Fourth Amendment protections. However, the court ultimately ruled in favor of the government, pursuant to the good faith exception. After analyzing the logic of the ruling, the review assesses the impact for future investigations. Finally, the review offers a three-tiered approach to limiting FISA overreach in the future, looking at legislative, corporate, and individual steps.

[1] Benjamin Ward is a graduating senior at Boston College, where he majors in International Studies and has a minor in Faith, Peace and Justice. He is interested in the intersection of law and ethics. Next year, Ben will continue his education at Boston College Law School. Finally, he has many thanks for Prof. Ashly Scheufele, JD, for her guidance and support in the legal writing process.

Introduction

In this article, I begin with a review of the Foreign Intelligence Surveillance Act (FISA) and its evolution to contextualize the current discussion about balancing national security and individual privacy. I then turn to a recent ruling where FISA evidence factored into the arrest and conviction of a U.S. person. This case illustrates how FISA impacts the lives and privacy of U.S. persons, despite the statute's stated foreign scope. After discussing why the ruling is worth our attention, I will work through how this ruling is a good starting point for a broader discussion of how to limit government overreach while also protecting national security. I offer three levels of limitations in this discussion: legislative, corporate, and individual. Striking the balance between individual privacy and national security is deeply complex, so I intend for this article to be a starting point to grapple with these questions and consider the different roles of societal actors.

Overview

History of the Foreign Intelligence Surveillance Act (FISA)

In 1978, Congress passed the Foreign Intelligence Surveillance Act (FISA) to enable law enforcement agencies to work around Fourth Amendment protections in foreign intelligence investigations and "get court orders for wiretaps and searches with a much lower standard of proof than required in a criminal investigation."[2] FISA warrants are issued by the Foreign Intelligence Surveillance Court (FISC), whose proceedings "are sealed and remain secret to even the subject of the warrant."[3] The powers of surveillance granted by FISA were enhanced by the USA Patriot Act (2001), most notably by expanding circumstances where surveillance is

[2] Paul T. Jaeger, John Carlo Bertot, and Charles R. McClure, "The Impact of the USA Patriot Act on Collection and Analysis of Personal Information Under the Foreign Intelligence Surveillance Act," *Government Information Quarterly* 20, no. 3 (July 2003): 297, https://doi.org/10.1016/S0740-624X(03)00057-1.

[3] Jaeger, Bertot, and McClure, "The Impact of the USA Patriot Act," 298.

acceptable, adding a bolstered secrecy clause that further limits disclosures about FISA investigations, and broadening the power to surveil electronic communications.[4] It is important to note, however, that the USA Patriot Act did not alter the exclusively foreign scope of FISA. While these laws were passed to promote national security, particularly against the threat of terrorism, they have the potential to undermine Americans' civil liberties.

Section 702

FISA was amended in 2008 by the FISA Amendments Act (FAA) to include Section 702, which allows for the Attorney General (AG) and the Director of National Intelligence (DNI) to jointly authorize the surveillance of non-U.S. persons, circumventing even the streamlined, secretive FISC warrant process.[5] A U.S. person is defined as a "citizen of the United States or an alien lawfully admitted for permanent residence."[6] The goal of Section 702 is to empower national security agencies to adapt to modern forms of electronic surveillance to collect foreign intelligence information. In practice, the AG and DNI authorize the surveillance of certain categories of people, allowing intelligence agencies to determine the particular individuals to target.[7] Section 702 allows for surveillance to proceed without a court order/warrant, which, according to the Office of the DNI, is critical to national security because security services "couldn't always meet the probable cause standard."[8] One key aspect of Section 702 is that the

[4] Jaeger, Bertot, and McClure, "The Impact of the USA Patriot Act," 299-300.
[5] The Privacy and Civil Liberties Oversight Board, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," September 28, 2023, 2, https://documents.pclob.gov/prod/Documents/OversightReport/d21d1c6b-6de3-4bc4-b018-6c9151a0497d/2023%20PCLOB%20702%20Report,%20508%20Completed,%20Dec%203,%202024.pdf. ("PCLOB")
[6] *Foreign Intelligence Surveillance Act (FISA)*, 50 U.S. Code § 1801(i)
[7] PCLOB, 35.
[8] Office of the Director of National Intelligence, "Section 702 Overview," n.d., 2, https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf.

target of surveillance must be reasonably believed to be located outside of the United States, and any targeting must not intentionally intercept data which was sent or received by a U.S. person.[9]

Given the wider surveillance powers granted by FISA Section 702, the risk of "reverse targeting" must be considered. Reverse targeting refers to the practice of intentionally targeting someone outside the country to obtain communications with a person within the United States.[10] Using Section 702 to intentionally target U.S. persons and circumvent the Fourth Amendment is plainly unlawful. However, the incidental collection of data on U.S. persons does occur and creates questions of how Fourth Amendment protections apply. To better understand how incidental collection occurs, a brief overview of Section 702 procedure is necessary.

Surveillance Procedure

First, the government identifies a specific "selector" for surveillance, which may include a target's email address or telephone number.[11] With the compelled assistance of communication service providers, the government collects data on targets (those who are reasonably believed *not to* be U.S. persons).[12] Despite procedures to reduce instances of incidental collection of data on U.S. persons, the reality is that U.S. persons are inadvertently swept up in these surveillance operations. This occurs when a selector email/phone has had contact with a U.S. person, meaning that any contact between the target and the U.S. person also gets intercepted. For example, if a target exchanges emails with a U.S. person, both sides of the exchange are collected, sweeping data on the U.S. person into the surveillance. This incidental collection of data from U.S. persons without a warrant raises Fourth Amendment concerns.

Minimization & Querying

[9] *FISA*, §1802(a)(1)(b)
[10] PCLOB, 36.
[11] PCLOB, 59.
[12] PCLOB, 67.

Government agencies each have their own "minimization" procedures to "reduce the privacy and civil liberties impact of the acquisition, retention, and dissemination of incidentally collected U.S. person information."[13] According to the U.S. Code, surveillance data on U.S. persons must be minimized within 72 hours *unless* the data is useful in understanding foreign intelligence, is evidence of a crime that has occurred, or is authorized for retention by the Attorney General under the belief that the data indicates bodily harm/death to any person.[14] These exceptions to minimization procedures are vague, based on subjective evaluations of what might be useful, giving wide latitude to security services to retain data on U.S. persons.

As a result, not all data is minimized, and troves of unminimized data are stored in massive agency databases.[15] These databases have not been purged of data from U.S. persons. An agent can search through these databases through a process called "querying."[16] The data resulting from a query is presumed to have already been lawfully obtained through a FISA Section 702 surveillance operation.[17] Through querying these massive, unminimized databases, the government can gain access to communications data of U.S. persons, incidentally collected through a prior Section 702 surveillance operation targeting a non-U.S. person for foreign intelligence purposes. Some refer to this procedure as "backdoor searching," which is a circuitous loophole that creates an opportunity for security services to collect sensitive, personal data from U.S. persons without a warrant.[18] Evidence resulting from an alleged "backdoor search" was the primary issue in *United States v. Hasbajrami,* 2016 U.S. Dist. LEXIS 30613 (United States District Court for the Eastern District of New York, March 8, 2016, Filed).

---

[13] *FISA,* §1801(h)
[14] *FISA*, §1801(h)(1–4)
[15] PCLOB, 155.
[16] PCLOB, 88.
[17] PCLOB, 88.
[18] PCLOB, 185.

Section 702 On Trial: Hasbajrami

Facts

The defendant, Hasbajrami, was subject to an investigation by the Federal Bureau of Investigation's Joint Terrorism Task Force (JTTF).[19] In 2011, JTTF agents arrested Hasbajrami and charged him with attempting to provide material support to a terrorist organization.[20] Hasbajrami was a legal permanent resident located within the United States, making him a U.S. person. The defendant was arrested while traveling to Pakistan, where he allegedly planned to join a terrorist organization and later fight against U.S. forces. The government disclosed that some of the evidence used in the case against Hasbajrami was obtained through FISA collection, and the defendant was convicted after he pleaded guilty. After Hasbajrami was already serving his sentence, the government made a further disclosure that some of the evidence against him originated from a warrantless FISA Section 702 query. The absence of the warrant for the Section 702 surveillance was significant because it may have violated Hasbajrami's constitutional rights as a U.S. person. Based on this disclosure, the court permitted Hasbajrami to withdraw his initial guilty plea and filed a motion to exclude the Section 702 evidence.[21]

Procedural History

In 2015, the United States District Court for the Eastern District of New York ruled on Hasbajrami's motion to exclude the Section 702 evidence, and the court released a memorandum

[19] *United States v. Hasbajrami,* 2016 U.S. Dist. LEXIS 30613 (United States District Court for the Eastern District of New York, March 8, 2016, Filed).
[20] *United States v. Hasbajrami,* 2024 U.S. Dist. LEXIS 239431, 2025 WL 447498 (United States District Court for the Eastern District of New York, February 10, 2025, Filed). Substantial portions of this decision remain redacted. Specific details of the investigation are omitted. However, the general facts of the case are well defined. This analysis is limited to the unredacted opinion issued in February 2025.
[21] *United States v. Hasbajrami,* 2024.

explaining the opinion in 2016.[22] In the opinion, Judge John Gleeson denied the motion to suppress on the grounds that even though the surveillance constituted a search without a warrant on a U.S. person, the search met the reasonableness standard.[23] The initial target of surveillance was a legitimate, non-U.S. target, and thus, the warrantless Section 702 surveillance is unproblematic. The court ruled that the incidental interception of Hasbajrami's data, despite being a U.S. person, did not require a warrant because the initial surveillance was legitimate. Gleeson wrote: "When surveillance is lawful in the first place—whether it is the domestic surveillance of U.S. persons pursuant to a warrant, or the warrantless surveillance of non-U.S. persons who are abroad—the incidental interception of non-targeted U.S. persons' communications with the targeted persons is also lawful."[24]

Hasbajrami appealed this ruling, and the United States Court of Appeals for the Second Circuit issued a ruling in 2019. The Circuit Court ruled in agreement with the District Court that the incidental surveillance of the defendant was not in itself a violation of the Fourth Amendment. However, the Circuit Court took issue with the procedures used to store and query the data on the defendant. The Court stated that "the storage and querying of information raises challenging constitutional questions, to which there are few clear answers in the case law."[25]

The Circuit Court acknowledged that there was some precedent on how to treat querying, citing an earlier Oregon District Court ruling that "subsequent querying of a § 702 collection, even if U.S. person identifiers are used, is not a separate search and does not make § 702

[22] *United States v. Hasbajrami,* 2016.
[23] *United States v. Hasbajrami,* 2016.
[24] *United States v. Hasbajrami,* 2016; citing *United States v. Mohamud,* 2014 U.S. Dist. LEXIS 85452, 2014 WL 2866749 (United States District Court for the District of Oregon, Portland Division June 24, 2014, Filed).
[25] *United States v. Hasbajrami,* 945 F.3d 641, 2019 U.S. App. LEXIS 37583, 2019 WL 6888567 (United States Court of Appeals for the Second Circuit December 18, 2019, Decided).

surveillance unreasonable under the Fourth Amendment."[26] The Circuit Court stated, however, that it did not find the logic of that ruling to be persuasive. Due to a lack of information on the specific nature of the storage and querying of Hasbajrami's data, the Circuit Court remanded the case back to the District Court, directing the District Court to specifically analyze the constitutionality of querying and whether it constituted a separate Fourth Amendment event. If deemed a separate Fourth Amendment event, the querying would require a warrant.

The United States District Court for the Eastern District of New York ruled again on this case in 2024 and released the first opinion in January 2025.[27] The District Court's opinion, which focused on querying, is detailed below.

Fourth Amendment Violation

The District Court in *Hasbajrami* ruled that the government's query into Section 702-obtained communications from the defendant constituted a separate Fourth Amendment event. Judge DeArcy Hall affirmed that "a search that relies on an initial warrant or exception to the warrant requirement is limited by its original justification, and to intrude further on lawfully acquired items requires new and independent approval."[28] Therefore, the government's querying implicated Hasbajrami's Fourth Amendment rights and required independent justification for the fruits of the query to be lawfully introduced as evidence at trial. The collection of data on the defendant was not, in itself, problematic (as established by the Circuit Court).

The issue arises in that the data on Hasbajrami was stored, and then *later queried* from an agency database.[29] Even though the data was in the possession of the government (in a database), the court ruled that the government needed a separate warrant to query this data. The opinion

[26] *United States v. Hasbajrami,* 2019; citing *United States v. Mohamud,* 2014.
[27] An updated version of the opinion was released in February 2025, with no significant changes. The February decision is cited in this review.
[28] *United States v. Hasbajrami,* 2024.
[29] *Hasbajrami v. United States*, 2024.

relied on the Supreme Court decision in *Riley v. California*, which held that law enforcement officers could not, without a warrant, search the digital contents of a cell phone lawfully seized during an arrest.[30] This precedent has been applied to computers as well: the government "should not be able to comb through…computers plucking out new forms of evidence that the investigating agents have decided may be useful, at least not without obtaining a new warrant."[31] The District Court in Hasbajrami (2024) applied this precedent to the context of stored surveillance data, departing from the Oregon District Court's reasoning in *United States v. Mohamud*. Judge Hall concluded that "just as the officers in Riley were required to obtain a warrant to search the seized cell phone, so too was the government required to obtain a warrant to view Defendant's communications that were lawfully intercepted" pursuant to Section 702.[32]

Exclusion of Evidence: Good Faith Exception

Evidence that is acquired in violation of the Fourth Amendment is, as a general rule, inadmissible in court.[33] Courts apply the exclusionary rule to exclude unlawfully seized evidence and any fruits of this evidence.[34] The exclusionary rule functions by serving as a deterrent against law enforcement agencies using unlawful tactics, but is not without exception. Where the benefit of deterrence is outweighed by substantial social costs, for example, courts have ruled it is inappropriate to apply the exclusionary rule.[35]

---

[30] *Riley v. California*, 573 U.S. 373, 134 S. Ct. 2473, 189 L. Ed. 2d 430, 2014 U.S. LEXIS 4497, 82 U.S.L.W. 4558, 42 Media L. Rep. 1925, 24 Fla. L. Weekly Fed. S 921, 60 Comm. Reg. (P & F) 1175, 2014 WL 2864483 (Supreme Court of the United States June 25, 2014, Decided).
[31] *United States v. Sedaghaty,* 728 F.3d 885, 2013 U.S. App. LEXIS 22234, 2013-2 U.S. Tax Cas. (CCH) P50,492, 112 A.F.T.R.2d (RIA) 2013-5864 (United States Court of Appeals for the Ninth Circuit August 23, 2013, Decided).
[32] *United States v. Hasbajrami,* 2024.
[33] *Mapp v. Ohio,* 367 U.S. 643, 81 S. Ct. 1684, 6 L. Ed. 2d 1081, 1961 U.S. LEXIS 812, 84 A.L.R.2d 933, 86 Ohio L. Abs. 513, 16 Ohio Op. 2d 384 (Supreme Court of the United States June 19, 1961, Decided).
[34] *Segura v. United States,* 468 U.S. 796, 104 S. Ct. 3380, 82 L. Ed. 2d 599, 1984 U.S. LEXIS 150, 52 U.S.L.W. 5128 (Supreme Court of the United States July 5, 1984, Decided)
[35] *Utah v. Strieff,* 579 U.S. 232, 136 S. Ct. 2056, 195 L. Ed. 2d 400, 2016 U.S. LEXIS 3926, 84 U.S.L.W. 4430, 26 Fla. L. Weekly Fed. S 288 (Supreme Court of the United States June 20, 2016, Decided)

Despite the ruling that the querying of Hasbajrami's data was unconstitutional, the District Court rejected exclusion as a remedy. There are various exceptions to exclusion that may apply, and the District Court worked through the relevant exceptions in its discussion. The court determined that the Foreign Intelligence exception did not apply, nor did other factors (e.g. exigency) that would have made the warrantless search reasonable. Rather, the court determined that exclusion of Section 702 evidence was inappropriate because the good faith exception applied.[36]

The good faith exception applies when an agent of the state acts with "an objectively reasonable good-faith belief that their conduct is lawful."[37, 38] The District Court contends that when agents act in good faith, the deterrent rationale of the exclusionary rule loses its force.[39] In this case, the court ruled that the good faith exception applied because the surveillance agents did not (and could not) have known that the court would rule that querying required a separate warrant. In fact, the 2014 *United States v. Mohamud* ruling had indicated the opposite.

Impact of Ruling

The ruling by the District Court in *Hasbajrami* has now made it clear that querying requires a warrant, which means that a court must approve a query search of data, even if that data was initially acquired and stored lawfully under FISA Section 702. Therefore, it logically follows that a good-faith exception *could not* apply again to an agent who queries without a warrant. In the case of Hasbajrami, the court ruled that the good faith exception applied, even

[36] *United States v. Hasbajrami,* 2024.
[37] *Davis v. United States,* 564 U.S. 229, 131 S. Ct. 2419, 180 L. Ed. 2d 285, 2011 U.S. LEXIS 4560, 79 U.S.L.W. 4495, 68 A.L.R. Fed. 2d 665, 22 Fla. L. Weekly Fed. S 1144 (Supreme Court of the United States June 16, 2011, Decided)
[38] See also, *Herring v. United States,* 555 U.S. 135, 129 S. Ct. 695, 172 L. Ed. 2d 496, 2009 U.S. LEXIS 581, 77 U.S.L.W. 4047, 21 Fla. L. Weekly Fed. S 582 (Supreme Court of the United States January 14, 2009, Decided).
[39] See this argument made in *Davis*.

though Hasbajrami correctly advanced the argument that his Fourth Amendment rights had been violated.

Limiting Government Overreach

Balancing National Security and Civil Liberties

Laws like FISA and Section 702 enable important efforts that mitigate risk to Americans and American assets. However, unbridled access to surveil U.S. persons is a level of overreach that is unacceptable. The suggestions for restricting Section 702 that I advance below are aimed at both empowering security services to do their job while also protecting personal privacy. To do this, I propose legislative, corporate, and individual steps to establish a middle ground that keeps government surveillance accountable to judicial review.

Legislative: Amending Section 702

Section 702 of the FISA Amendments Act (FAA) is codified in 50 USC § 1881a. Currently, the statute outlines the following requirement for querying unminimized data on a U.S. person:

> Federal Bureau of Investigation personnel must obtain prior approval from a Federal Bureau of Investigation supervisor (or employee of equivalent or greater rank) or attorney who is authorized to access unminimized contents or noncontents obtained through acquisitions authorized under subsection (a) for any query of such unminimized contents or noncontents made using a United States person query term.[40]

This requirement can be circumvented, however, if the agent has "a reasonable belief that conducting the query could assist in mitigating or eliminating a threat to life or serious bodily harm."[41] Other than the requirement of a supervisor's approval, the statute does not require a

[40] *FISA,* §1881a (f)(3)(a)(i)
[41] *FISA*, §1881a (f)(3)(a)(ii)

warrant or court order to run a query. To better reflect the District Court decision in *United States v. Hasbajrami (2024)*, I propose a legislative amendment to 50 USC §1881a.

Specifically, the statute should reflect that running a query requires a warrant from the FISC. Due to the sensitive nature of national security investigations, there must be exceptions to this warrant requirement, such as exigent circumstances.[42] These exceptions rely on the standard of reasonableness, meaning that security services would have latitude to run queries without a warrant, but must then be prepared to defend those actions as reasonable in court. By amending 50 USC §1881a to include a warrant requirement for queries, Congress would add a measure of protection for U.S. persons in the form of judicial oversight, while still preserving the power of security services to run such queries.

Corporate: The Role of Telecommunication Companies

A key element of the FISA telecommunications surveillance process is the compelled assistance of electronic communication service providers (ECSPs). FISA requires that, if an ECSP receives a surveillance request from the government, it must "immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition."[43] An intelligence agency on its own does not have access to a person's email correspondence. Rather, the agency requests that the relevant email service provider share that user's data. The government compensates the company "at the prevailing rate" for the requested information.[44] Given the critical role that ECSPs play in government investigations, they are

[42] *United States v. McConney,* 728 F.2d 1195, 1984 U.S. App. LEXIS 25576 (United States Court of Appeals for the Ninth Circuit February 10, 1984, Decided); exigency defined as "circumstances that would cause a reasonable person to believe that entry (or other relevant prompt action) was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts."
[43] *FISA*, §1881a (i)(1)
[44] *FISA*, §1881a (i)(2)

sometimes referred to as "surveillance intermediaries."[45] While the government wields significant power of compulsion over these surveillance intermediaries, there are legal steps that an ECSP can take to resist transferring user information.

An ECSP may challenge a request from the government by filing a petition to the Foreign Intelligence Surveillance Court (FISC) and following appeal procedures up to the Supreme Court.[46] Given ECSP's crucial role in the Section 702 process, some commentators argue that these companies have the power to shape and negotiate surveillance practices in a more meaningful way than even the courts.[47] When an ECSP resists a data request from the government, it forces the surveillance agency to justify its request in court. Therefore, ECSPs have the power to force surveillance agencies to undergo a more thorough process of judicial review. Along with this logic, some argue that the ECSPs are best equipped to pursue surveillance-related litigation (rather than individuals), given the experience these companies have with surveillance requests and the legal resources at their disposal.[48] Therefore, I argue that in addition to a legislative amendment to FISA Section 702, ECSPs ought to take a more active role in protecting users' privacy from government oversight.

There are competing incentives for an ECSP to assist or resist government surveillance. The obvious incentive to assist is that doing so puts the company in good graces with its regulators. Telecommunication companies also are (or should be) driven by profit-maximization, and therefore, there remains a strong incentive to protect their public reputation. Current events play a large role in this incentive matrix. For example, in the wake of the 9/11 attacks, ECSPs,

[45] "Developments in the Law: More Data, More Problems," *Harvard Law Review* 131, no. 6 (2018): 1722, https://www.jstor.org/stable/pdf/44865881.pdf.
[46] *FISA*, §1881a (i)(4)
[47] "More Data, More Problems," 1722.
[48] "More Data, More Problems," 1739.

without precedent, yielded almost entirely to the needs of security services.[49] Here, the companies perhaps acted out of patriotism, a sentiment shared by consumers at the time. In contrast, after the Snowden disclosures, many ECSPs began to challenge national security-compelled assistance requests.[50] This behavior reflected consumer aversion to the perception of "big brother" surveillance. These examples demonstrate the key role ECSPs play in the surveillance process and provide a precedent for resisting government overreach, particularly when doing so aligns with consumer sentiment.

Individual: The Role of Consumers

Compared to courts and corporations, the individual holds relatively little power in the process of resisting government surveillance. Nonetheless, there are important steps for individuals to take to counter government overreach in the realm of surveillance. One commentator summarizes some of the methods of individual resistance as the following: "voting, litigating, hiding, and buying."[51] The first method, voting, involves electing privacy-minded officials. It remains uncertain, however, the degree to which individually elected officials can influence the massive structure of the national security apparatus. Litigating refers to individuals suing the government for privacy infractions. The issues of harm and standing make litigating at the individual level quite challenging, especially given that most surveillance occurs in secret (i.e., a person would generally never know that surveillance occurred).[52] Hiding refers to individual efforts to protect data, such as encrypting communications. There is value in this step, but the reality is that the government can often still interpret or break encryptions.[53] While these

[49] "More Data, More Problems," 1725.
[50] "More Data, More Problems," 1726.
[51] Ryan Calo, "Can Americans Resist Surveillance?" *The University of Chicago Law Review* 83, no. 23 (2016): 30.
[52] Calo, "Can Americans Resist Surveillance?" 34.
[53] Calo, "Can Americans Resist Surveillance?" 38.

individual tactics should certainly not be written off, there is most value in the method of 'buying,' or using market pressure to influence ECSPs to take steps to protect their consumers' privacy.

In the previous section, I argued that ECSPs have immense power to protect individual privacy if properly incentivized to do so. Therefore, the most effective individual strategy to resist surveillance may be to give telecommunication companies the incentive they need to resist compelled assistance and force judicial review. To be sure, there are challenges to this tactic. For example, promises of privacy by a company are relatively unenforceable, leaving the consumer with few resources in the event of surveillance cooperation. One commentator highlights that it is extremely unlikely that the Federal Trade Commission (FTC) would penalize an ECSP for deceptive statements if that company is cooperating with *another* government enforcement agency, as would be the case in a surveillance collection.[54]

I argue, however, that the risk of large-scale consumer mistrust is incentive enough for ECSPs to at least make efforts to respect privacy. If not, more privacy-minded companies will win over consumer bases. Therefore, an individual can resist surveillance overreach by being informed about the policies of the telecommunication companies they use and selecting ECSPs that best align with the level of privacy that they desire. This market pressure, at least on a large scale, has the potential to encourage ECSPs to add more hurdles to the practice of compelled assistance.

Conclusion

The Foreign Intelligence Surveillance Act, including the more recent Section 702, empowers the government to perform critical national security functions. Through its use, FISA

[54] Calo, "Can Americans Resist Surveillance?" 41.

Section 702 has grown into a pathway to deploy intelligence resources against U.S. persons, a reality that deeply contravenes the stated scope of FISA. Through a series of highly secretive procedures, and despite policies of minimization, data on U.S. persons is stored and used in investigations and trials, as seen in the case against Hasbajrami. The recent ruling in *United States v. Hasbajrami (2024)* has set an important precedent that querying data is its own Fourth Amendment event and thus requires a court-issued warrant. Building off this important ruling, I propose a three-level approach to resisting government overreach in surveillance. On the legislative level, I urge amending Section 702 to reflect the *Hasbajrami* reasoning and require a warrant for any querying of FISA data. On the corporate level, I argue that electronic communication service providers have a role to play in resisting (not flatly rejecting) compelled assistance requests to require some degree of judicial review. Finally, at the individual level, I argue that individual consumers have a role to play in shaping market pressures to encourage ECSPs to keep government surveillance in check.