MITCHELL | HAMLINE School of Law

Mitchell Hamline Law Review

Volume 46 | Issue 5 Article 4

2020

My Brother's Keeper: Using the Intelligence Toolbox on Domestic Terrorism

Brandon Carmack

MY BROTHER'S KEEPER: USING THE FOREIGN INT ELLIGENCE TOOLBOX ON DOMESTIC TERRORISM

Brandon Carmack

"It is impossible to expel evil from the world in its entirety, but it is possible to constrict it within each person." – Alexander Solzhenitsyn

I. INTRODUCTION

I remember the morning of April 19, 1995. I was seven years old and confused by the rubble that consistently flashed across my television. Words like "Oklahoma City Bombing" hung in the air, and Timothy McVeigh became synonymous with evil. I remember the morning of September 11, 2001. I was thirteen years old and confused by the rubble that consistently flashed across my television. Words like "9/11" hung in the air, and Osama Bin Laden became synonymous with evil.

Recent decades have forced the intelligence community to monitor pendulum shifts in various expressions of terrorism. The early nineties raised questions about *foreign* terrorism as Al-Qaeda took responsibility for attempted bombings at the World Trade Center. The mid-nineties

raised questions of *domestic* terrorism with the Oklahoma City Bombing. The pendulum returned to foreign terrorism after Al-Qaeda attacked U.S. embassies in Kenya and Tanzania in 1998, and, of course, the World Trade Center in 2001.

However, in the last five years, the pendulum of concern has once again swung to domestic terrorism.[1] Mass shootings dominate the news cycle. Each violent episode gives rise to riveting discussions concerning gun violence in the United States. But rarely do these discussions consider how the United States' current law enforcement infrastructure could be used to identify and prevent such tragedies.

Recent testimony to the House Homeland Security Committee indicates an increase in domestic terrorism incidents in recent years.[2] In 2013, Americans suffered twenty domestic terrorism incidents.[3] In 2014, that number grew to twenty-nine.[4] A smaller uptick occurred in 2015, reaching thirty-eight incidents.[5] But by 2016, that number nearly doubled

---

[1] *See* Adam Goldman, *F.B.I., Pushing to Stop Domestic Terrorists, Grapples with Limits on Its Power*, N.Y. TIMES (June 4, 2019), https://www.nytimes.com/2019/06/04/us/politics/fbi-domestic-terrorism.html [https://perma.cc/Y92Q-WLJT]. "The increase in [domestic terrorism] arrests marks something of a return to the 1990s, when the F.B.I. devoted significant resources to infiltrating and dismantling violent white supremacist and right-wing militia organizations from which lethal terrorists like David Lane and Timothy McVeigh emerged." *Id.*

[2] *See* Michael C. McGarrity, *Confronting the Rise of Domestic Terrorism in the Homeland*, FBI (May 8, 2019), https://www.fbi.gov/news/testimony/confronting-the-rise-of-domestic-terrorism-in-the-homeland [https://perma.cc/NR49-SMEH] (Statement Before the House Homeland Security Committee) ("We believe domestic terrorists pose a present and persistent threat of violence and economic harm to the United States; in fact, there have been more arrests and deaths caused by domestic terrorists than international terrorists in recent years.").

[3] *National Consortium for the Study of Terrorism and Responses to Terrorism 2013 Results*, UNIV. OF MD. GLOBAL TERRORISM DATABASE, https://www.start.umd.edu/gtd/search/Results.aspx?page=1&casualties_type=b&casualties_max=&start_year=2013&start_month=1&start_day=1&end_year=2013&end_month=12&end_day=31&dtp2=all&country=217&expanded=no&charttype=line&chart=overtime&ob=GTDID&od=desc#results-table [https://perma.cc/YL29-5S7S].

[4] *National Consortium for the Study of Terrorism and Responses to Terrorism 2014 Results*, UNIV. OF MD. GLOBAL TERRORISM DATABASE, https://www.start.umd.edu/gtd/search/Results.aspx?page=1&casualties_type=b&casualties_max=&start_year=2014&start_month=1&start_day=1&end_year=2014&end_month=12&end_day=31&dtp2=all&country=217&expanded=no&charttype=line&chart=overtime&ob=GTDID&od=desc#results-table [https://perma.cc/6Z3H-RH2K].

[5] *National Consortium for the Study of Terrorism and Responses to Terrorism 2015 Results*, UNIV. OF MD. GLOBAL TERRORISM DATABASE, https://www.start.umd.edu/gtd/search/Results.aspx?page=2&casualties_type=b&casualties_

to sixty-seven.[6] In 2017 and 2018, that number stayed nearly the same—sixty-six[7] and sixty-seven, respectively.[8]

As a result of the alarming rise in domestic terrorism, we must ask whether the Constitution provides room for more government action against it. Policy leaders should begin by looking at various tools available to the foreign intelligence community to determine what might be legally permissible and practical in a domestic context. Obviously, not all foreign tools would be permissible for domestic use. For example, drone strikes on U.S. soil would violate constitutional due process (though the Justice Department has permitted drone strikes against U.S. citizens on foreign soil).[9] But what about material support statutes or enhanced interrogation techniques? Each tool in the foreign intelligence community must maintain an independent legal basis for domestic application. This paper evaluates the constitutional limits of employing foreign surveillance techniques against domestic terrorism suspects.

The Constitution shields the American citizen much differently than a foreign enemy combatant. Coupled with rapidly evolving technology, the prospect of enhanced government surveillance should cause discomfort

---

max=&start_year=2015&start_month=1&start_day=1&end_year=2015&end_month=12&end_day=31&dtp2=all&country=217&expanded=no&charttype=line&chart=overtime&ob=GTDID&od=desc#results-table [https://perma.cc/JWT6-RJAT].

[6] *National Consortium for the Study of Terrorism and Responses to Terrorism 2016 Results*, UNIV. OF MD. GLOBAL TERRORISM DATABASE, https://www.start.umd.edu/gtd/search/Results.aspx?expanded=no&casualties_type=b&casualties_max=&start_year=2016&start_month=1&start_day=1&end_year=2016&end_month=12&end_day=31&dtp2=all&success=yes&country=217&ob=GTDID&od=desc&page=1&count=20#results-table [https://perma.cc/7D7S-TESW].

[7] *National Consortium for the Study of Terrorism and Responses to Terrorism 2017 Results*, UNIV. OF MD. GLOBAL TERRORISM DATABASE, https://www.start.umd.edu/gtd/search/Results.aspx?start_yearonly=&end_yearonly=&start_year=2017&start_month=1&start_day=1&end_year=2017&end_month=12&end_day=31&asmSelect0=&country=217&asmSelect1=&dtp2=all&success=yes&casualties_type=b&casualties_max= [https://perma.cc/2RLJ-6AU6].

[8] *National Consortium for the Study of Terrorism and Responses to Terrorism 2018 Results*, UNIV. OF MD. GLOBAL TERRORISM DATABASE, https://www.start.umd.edu/gtd/search/Results.aspx?start_yearonly=&end_yearonly=&start_year=2018&start_month=1&start_day=1&end_year=2018&end_month=12&end_day=31&asmSelect0=&country=217&asmSelect1=&dtp2=all&success=yes&casualties_type=b&casualties_max= [https://perma.cc/AA85-N7UF].

[9] *See* OFFICE OF LEGAL COUNSEL, U.S. DEP'T OF JUSTICE, APPLICABILITY OF FEDERAL CRIMINAL LAWS AND THE CONSTITUTION TO CONTEMPLATED LETHAL OPERATIONS AGAINST SHAYKH ANWAR AL-AULAQI (July 16, 2010), https://fas.org/irp/agency/doj/olc/aulaqi.pdf [https://perma.cc/385F-WX3G].

and resistance. Americans have rightly favored their freedom over their security since the days of the American Revolution. But what if we could be slightly more secure without sacrificing freedoms? Is this possible?

This paper argues that it is possible to strike such a balance. Section 702 of the Foreign Intelligence Surveillance Act (FISA) already provides the structure for constitutionally enhancing surveillance against domestic terrorism suspects.[10] However, while this proposal falls within the boundaries of the Constitution, political concerns likely prevent its adoption. Part II of this article provides an overview of Section 702 and outlines the proposed language for its domestic counterpart. Part III then analyzes the constitutional limits on that proposal. Finally, this article identifies and addresses the political limitations that likely prevent this reform in Part IV.

By way of preface, I do not argue that adopting Section 702 into the domestic context will solve the problem of domestic terrorism. Indeed, even if passed, its implementation would face significant practical challenges for the Federal Bureau of Investigation (FBI). Rather, the goal of this paper is to encourage the intelligence community to consider whether foreign intelligence tools are appropriate for combating domestic terrorism. It may be that federal criminal statutes already provide the needed tools to address the pendulum's return to domestic terror. Be that as it may, the goal of this proposal is more than mere navel-gazing—I simply hope to inspire a fresh conversation on what our Constitution allows, despite our political reservations.

II. DOMESTICATING SECTION 702: A LEGISLATIVE PROPOSAL

In December of 2018, Dakota Reed adorned his Seattle bedroom with white supremacist propaganda.[11] With this as a backdrop, Reed recorded himself holding two AR-15's while announcing he was "fixing to shoot up" a local school.[12] He posted this video on Facebook. Only a month prior, Reed wrote on his Facebook wall that he was "shooting for

[10] *See generally* The FISA Amendments Act: Q&A, OFF. OF DIR. OF NAT'L INTELLIGENCE (Apr. 18, 2017), https://www.dni.gov/files/icotr/FISA%20Amendments%20Act%20QA%20for%20Publication.pdf [https://perma.cc/THW4-LNRV]; *see also* Section 702 Overview, OFF. OF DIR. OF NAT'L INTELLIGENCE, https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf [https://perma.cc/S5HV-582L].

[11] Goldman, *supra* note 1.

[12] *Id.*

30 Jews."[13] The FBI investigated Reed. Finding the threat too vague, they passed his case off to local law enforcement.[14] Reed pled guilty to making bomb threats and served a one-year sentence.[15]

According to the *New York Times*, Reed's case highlights typical limits on the FBI's domestic terrorism efforts: "Agents cannot always rely on federal law, unlike in so-called international terrorism cases where statutes were enacted to address the threat after the 9/11 attacks. Instead, the FBI often turns to local prosecutors to charge people they are concerned might be planning domestic attacks."[16] The proposal outlined in this paper can close one of these gaps in federal law. Using FISA's Section 702 model, Congress could pass legislation allowing the FBI to target potential domestic terrorists that trigger an Artificial Intelligence (AI) system integrated on social media platforms. The AI system would be built on already-existing FBI behavioral analytics. Once a suspect triggers this system, the FBI would have a legal basis to engage in upstream and selector surveillance of that individual.

A. Section 702—A Foreign-Target Surveillance Tool

Due to FISA's clandestine nature, significant confusion and speculation exist around it. Section 702 provides no exception. The following section briefly summarizes Section 702 and the debate surrounding the scope of the FBI's access (the "Backdoor Loophole").

In the FISA Amendments Acts of 2008, Congress added Section 702 to authorize "sweeping and suspicionless programmatic surveillance targeting individuals outside the United States."[17] In essence, Section 702 gave the Foreign Intelligence Surveillance Court (FISC) oversight over "the surveillance, for foreign intelligence purposes, of foreigners overseas."[18]

---

[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *See id.* ("'Law enforcement needs more effective tools,' said Mary McCord, a former top national security prosecutor who has drafted a proposed statute to criminalize the stockpiling of weapons intended to be used in a domestic terrorist attack. 'I recognize the very legitimate concerns of those in the civil rights community, but I would hope that their concerns could be addressed through oversight.'").
[17] STEPHEN DYCUS ET AL., COUNTERTERRORISM LAW 305 (Rachel Barkow et al. eds., 3d ed. 2016).
[18] *Id.* at 306.

Specifically, Section 702 affords the intelligence community two surveillance tools: "PRISM" and "upstream" data collection.[19] First, PRISM collection allows the government to send a "selector" (e.g., an email address) to an electronic communications service provider in the United States (i.e., an Internet Service Provider (ISP)).[20] Section 702 compels the ISP to provide the National Security Agency (NSA) with all communication from that email address (or whatever selector the agency chose).[21] PRISM only involves *electronic* communications—not telephone calls.[22] While the NSA receives all communications collected through PRISM, it shares only limited portions of that information with the Central Intelligence Agency (CIA) and FBI.[23] Second, Section 702 provides "upstream" data collection. Upstream differs from PRISM collection in multiple ways: (1) upstream compels assistance from providers controlling the "'backbone' over which . . . internet communications transit" rather than just the cooperation of ISP's;[24] (2) upstream collection includes telephone communications and electronic communications;[25] and (3) only the NSA receives upstream communications.[26]

In 2017, Congress limited upstream searches.[27] For example, Section 702 originally permitted "about" communications, whereby the NSA can collect communications including a selector of a targeted person. This means that when the NSA targets a selector, it can obtain any communications discussing that selector, rather than just communication "to" or "from" that selector.[28] However, Congress revised this provision in

[19] DAVID MEDINE ET AL., PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 7 (2014).

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *See* Emma Kohse, *Summary: The FISA Amendments Reauthorization Act of 2017*, LAWFARE (Jan. 28, 2018), https://www.lawfareblog.com/summary-fisa-amendments-reauthorization-act-2017 [https://perma.cc/A4BT-TPAN].

[28] *See* Andrew Crocker & David Ruiz, *How Congress's Extension of Section 702 May Expand the NSA's Warrantless Surveillance Authority*, ELEC. FRONTIER FOUND. (Feb. 1, 2018), https://www.eff.org/deeplinks/2018/02/how-congresss-extension-section-702-may-expand-nsas-warrantless-surveillance [https://perma.cc/ZK87-N5J6] ("Under downstream, the government requires companies like Google, Facebook, and Yahoo to turn over messages 'to' and 'from' a selector—gaining access to things like emails and Facebook messages.").

the 2017 renewal.[29] That revision terminated the "about" communications searches unless the Director of National Intelligence (DNI) and Attorney General (AG) provide Congress with a thirty-day notice to renew the program.[30] Section 702 also permits "multiple communications transactions."[31] This allows the NSA to collect any communications included in a thread "to," "from," or "about," the selector, so long as one end of the communications transaction involves a non-U.S. foreign individual.[32]

However, Congress placed various limitations on Section 702. First, Section 702 prohibits the intentional targeting of "United States persons."[33] Of relevance here, the amendment proscribes surveillance of "any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States."[34] In other words, Section 702 only permits targeted surveillance of non-U.S. citizens.

Second, by its very placement in FISA, Section 702 remains subject to FISC review. Importantly, the FISC reviews the minimization procedures for the inadvertent collection of U.S. persons and any retention or dissemination procedures regarding that data.[35] Additionally, the FISC ensures all surveillance procedures comply with both Section 702 and the Fourth Amendment.[36]

---

[29] *See id.*

[30] *Id.* (In 2017, Congress expressly terminated the "about communications" practice when it voted to reinstate Section 702).

[31] MEDINE ET AL., *supra* note 19, at 7.

[32] *Id.*

[33] 50 U.S.C. § 1881a(b)(1)–(5) (2018); *see also* 50 U.S.C. § 1801(i) (2018) (defining a "United States person" as "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, as defined in subsection (a)(1), (2), or (3) [of this section].").

[34] 50 U.S.C. § 1881a(d) (2018).

[35] *See* DYCUS ET AL., *supra* note 17, at 306.

[36] *See* Am. Civil Liberties Union v. Clapper, 785 F.3d 787, 793 (2015) (citing 50 U.S.C. § 1803) ("[T]he Foreign Intelligence Surveillance Act of 1978 ("FISA") . . . established a special court, the Foreign Intelligence Surveillance Court ("FISC"), to review the government's applications for orders permitting electronic surveillance.").

B. The "Backdoor Loophole"—Section 702's Current Domestic Use

The Backdoor Loophole matters to the analysis because it demonstrates how confusion over processes can lead to erroneous conclusions of law. Clarifying these clandestine practices provides a subtle, yet important step to providing the FBI with necessary tools against domestic terrorism.

Critics misunderstand the FBI's access to Section 702 information and argue that Section 702's drafters "overlooked how law enforcement uses intelligence information."[37] Specifically, critics allege that FBI officials examine Section 702 databases using "'U.S. person identifiers' (terms or indicators that are linked to a U.S. person)," arguing "[n]o search warrant is required to query such information."[38] Additionally, critics argue that, although Section 702 "imposes a low level of judicial scrutiny for the creation of the large pools of information in 702 databases," there is no higher scrutiny for such targeted intrusion on that person's "heightened privacy interest."[39] Thus, critics conclude that "[w]hile the standards for querying Section 702 data are well-suited for foreign intelligence purposes, they are woefully inadequate for law enforcement purposes."[40] However, these arguments confuse how FBI queries occur, and provide a limited presentation of the implicated law.

Former FBI special agent Asha Rangappa has outlined two clarifications for how these queries occur. First, in 2011, the FBI developed the Data Integration and Visualization System (DIVS), which aggregates data from multiple government databases.[41] Scholars suggest DIVS resulted from the 9/11 Commission's recommendation that the intelligence community unify "their knowledge in a network-based information sharing system that transcends traditional government boundaries."[42]

---

[37] Mieke Eoyang & Gary Ashcroft, *Why Electronic Surveillance Reform is Necessary*, THIRD WAY (Feb. 28, 2017), https://www.thirdway.org/memo/why-electronic-surveillance-reform-is-necessary [https://perma.cc/QF8Z-4QGP].

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] Asha Rangappa, *Don't Fall for the Hype: How the FBI's Use of Section 702 Surveillance Data Really Works*, JUST SECURITY (Nov. 29, 2017), https://www.justsecurity.org/47428/dont-fall-hype-702-fbi-works [https://perma.cc/EL5Q-8SP2].

[42] *Id.*

Second, some of the Section 702 PRISM data is provided to the FBI through DIVS, comingled with all the data in DIVS.[43] Section 702 data is explained as "'federated' *within* DIVS":[44]

> This means that while a query may return a 702 "hit"—i.e., an indication that FISA-related information related to the queried selector exists—neither the metadata nor the content of that communication is immediately accessible to all agents. Only agents who work national security cases, have gone through FISA training, and have the appropriate clearance levels may continue to access the full 702 data at this stage. Agents working "ordinary" criminal cases, who do not have this training and clearance, would need to have an agent with the appropriate FISA clearance access the 702 data, and only after obtaining approval from both her own supervisor and the national security agent's supervisor to rerun the query.[45]

Proponents of the Backdoor Loophole draw two important conclusions from this system. First, agents are not able to conduct Section 702-only searches: "[T]here is no such thing as doing an independent, 702-only 'search,' even just for surface connections between non-content selectors, or 'metadata.'"[46] Second, when the agent conducts the query, "*she does not know* whether or not the search will result in a 702 'hit.'"[47] Based on the foregoing, proponents argue that reform efforts requiring the FBI to show "relevance" for a "metadata query" fail to recognize there is "no such thing as a 'metadata query.'"[48] Thus, "[t]his policy would require the FBI to go to court for every single search its 14,000 agents conduct each day."[49] In daily practice, DIVS only returns data appropriate for the clearance level and need-to-know basis of the individual conducting the search. This screening process is automated according to the classified nature of the data and security clearance credentials associated with an agent's profile.

---

[43] *Id.*
[44] *Id.*
[45] *Id.*
[46] *Id.*
[47] *Id.*
[48] *Id.*
[49] *Id.*

C. The Proposal

Section 702 provides a framework for advanced, constitutional surveillance of domestic terrorism. As a prevention tool, Section 702 could provide the FBI with needed intelligence to intercept violent domestic acts before they occur. Specifically, Section 702 contains four fundamental categories that could be mirrored into the domestic realm: (a) targeted surveillance; (b) private sector participation; (c) limited timeframe; and (d) judicial oversight over targeting and mitigation procedures.[50] These elements could be used to build a domestic terrorism prevention statute that complies with constitutional limits on surveillance.

1. Targeted Surveillance

Section 702 authorizes the AG and DNI to "target[] persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[51] Such targeting is limited to non-U.S. persons located outside of the United States and cannot be used to gain information about either a U.S. person or any person located inside the U.S.[52] Section 702(b) is controversial because the electronic communications of U.S. persons are still being acquired inadvertently if such U.S. persons communicate with a foreign target under surveillance.[53]

---

[50] 50 U.S.C §§ 1881a(b)(1)–(3) (2018) (discussing targeted surveillance); 1881a(h)(2)(A)(vi) (outlining private sector participation); 1881a(a) (explaining limited time frame); 1881a(d)(2)–(e) (providing judicial review and minimization procedures).

[51] Foreign Intelligence Amendments Act of 2008, 50 U.S.C § 1881a(a) (2008).

[52] § 1881a(b)(1)–(4).

[53] *See* Robyn Greene, *Unintentional Noncompliance and the Need for Section 702 Reform*, LAWFARE (Oct. 5, 2017), https://www.lawfareblog.com/unintentional-noncompliance-and-need-section-702-reform [https://perma.cc/7UHT-QJKE] ("This most recent query violation is part of a long history of inadvertent improper searches of Section 702-acquired data for U.S. persons and non-U.S. persons' communications alike."). *But see* Shreve Ariail, *The High Stakes of Misunderstanding Section 702 Reforms*, LAWFARE (Dec. 6, 2017), https://www.lawfareblog.com/high-stakes-misunderstanding-section-702-reforms [https://perma.cc/P9V7-YTGW]. Ariail states:

> To the extent that anyone might suggest that the law on incidental interception is "unsettled" (which it is not) it is also worth considering, as Judge Gleeson did in *United States v. Hasbajrami* the Supreme Court's ruling in this area . . . . Other courts to address the incidental interception issue in other contexts have found similarly and no meaningful distinction between the constitutionality of incidental interception under the Section 702 program and incidental interception through other lawful surveillance has been identified.

Id.

Similarly, Congress should pass language, with limitations, providing the FBI with targeting tools for U.S. persons likely to engage in domestic terrorism. As under FISA, no U.S. person should be targeted, "solely upon the basis of activities protected by the first amendment."[54] However, if it is possible to protect the constitutional rights of U.S. citizens *while at the same time* protecting their lives, should we not strive for such a solution?

One FBI agent recommends the use of AI on social media platforms to predict signs of imminent danger.[55] In 2017, the FBI's National Center for the Analysis of Violent Crime (NCAVC) and Behavioral Threat Assessment Center published findings of behavioral analytics of violent persons.[56] The report states:

> By engaging in the assessment and management process as soon as a person of concern is identified, threat managers are more likely to succeed in preventing a violent outcome. Steering a person in a different direction early on may mean offering assistance to someone who needs it before that person concludes violence is necessary.[57]

Specifically, the FBI's Behavioral Analysis Unit (BAU) mapped certain traits and characteristics of individuals who have committed some act of mass or extreme violence.[58] Recognizing there may be no exhaustive list of such traits and characteristics, the report distinguishes "risk factors" from "warning behaviors," which, when combined, could predict potential acts of violence.[59]

---

[54] Foreign Intelligence Amendments Act of 2008, 50 U.S.C § 1805(a) (2008).

[55] Interview with Anonymous FBI Agent (Nov. 19, 2019) (on file with the author). The FBI has in fact already explored AI's policing capabilities. *See, e.g.*, Robert Davidson, *Automated Threat Detection and the Future of Policing*, LEB (Aug. 8, 2019) https://leb.fbi.gov/articles/featured-articles/automated-threat-detection-and-the-future-of-policing [https://perma.cc/Y9RT-89XY].

[56] *See generally* MOLLY AMMAN ET AL., FBI, MAKING PREVENTION A REALITY: IDENTIFYING, ASSESSING, AND MANAGING THE THREAT OF TARGETED ATTACKS (2017), https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view [https://perma.cc/Q7LA-TN4M].

[57] *Id.* at 5.

[58] *Id.* at 21 ("Threat assessment is a multifaceted process, stemming from a holistic analysis of the pattern of behaviors displayed by a person of concern.").

[59] *Id.* at 29–32.

Risk factors involve "existing realities about the person of concern that may increase the risk of violence he poses in a given situation."[60] Such factors include violence exposure, mental health, weapon access, problematic behavioral history, and social/environmental concerns.[61] Conversely, warning behaviors are "dynamic and represent changes in patterns of behavior that may be evidence of increasing or accelerating risk."[62] Categorically, these behaviors include pathways to violence, fixation, identity (i.e., taking on a pseudo-warrior identity), novel aggression, energy burst, leakage (communicating intent to harm a third person), directly communicated threats, approach (i.e., attempts to gain access to, or surveillance of, a targeted location), end-of-life planning, and last-resort behaviors.[63]

Analyzing these behaviors allows the FBI to determine the threat levels of various individuals. The FBI compares this threat assessment system to the weather assessment system of the National Weather Service (NWS).[64] For example, when monitoring tornadoes, the NWS uses weather patterns to predict if conditions require: (i) no message, (ii) a tornado watch, or (iii) a tornado warning.[65] When the chance of a tornado is not "measurably above the base rate," the NWS remains silent on tornado updates (no message).[66] But when conditions are just right, the NWS will alter its alert to either "watch" or "warning."[67] Similarly, the BAU adopts a similar structure to determine: (i) the appropriate level of concern; and (ii) how imminent that concern may be.[68] The FBI's report states, "[a] concern level does not predict violence likelihood but rather expresses the extent to which conditions may facilitate violence potential."[69]

The report goes on to discuss the fact that many of these behaviors are evidenced through social media and electronic communication. Social media leakage, once located, "can be a very effective source of information regarding the person's mindset and future plans. Social media review

---

[60] *Id.* at 29.
[61] *Id.* at 29–32.
[62] *Id.* at 32.
[63] *Id.* at 32–36.
[64] *Id.* at 23.
[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] *Id.*

should begin as soon as a case is opened and continue until concerns are abated."[70]

Behavioral analytics on social media accounts has already existed for several years through the use of AI.[71] Today, it is commonly used to detect advertising opportunities,[72] remove "hateful accounts,"[73] and even analyze and predict terrorist recruiting and public relations behavior.[74]

Integrating AI and the behavioral analytics already established at the FBI could provide a non-content-based solution to targeting U.S. citizens. If the FBI can integrate its current threat forecasting scheme into an AI software, then Congress could grant the FBI the capabilities to target U.S. persons based on that threat determination, rather than on the content of that person's conduct or speech. Such a red flag "warning" could provide the FBI with a sufficient basis to secure a warrant for the target's electronic communications *on that social media platform*.[75] The idea is to provide the FBI with proactive tools that constitutionally protect U.S. citizens from other U.S. citizens.

---

[70] *Id.* at 50. According to this report,

A study of targeted violence incidents at schools revealed that in over 75% of the cases studied at least one person had information that the offense was being planned. Most were peers, such as a friend, a schoolmate, or a sibling. Some peers knew about the plan because the offender "leaked" it. Leakage on social media could take the form of writings, images, videos, and even "likes." An example of social media leakage occurred in a European case. Hours before a 2011 assault on a youth camp, the offender posted a video online which appeared to advocate violence toward specific religious and political groups. About 90 minutes before his offense, he posted a 1,500+ page "manifesto" online, describing two years of preparation for violence. It is worth noting that neither of these posts included a direct threat.

Id.

[71] *See* Tina Shahid, *Social Media AI: How Did the History of AI Lead Up to It?*, SYNTHESIO (Feb. 27, 2019), https://www.synthesio.com/blog/social-media-ai-history-of-ai/ [https://perma.cc/94BE-HL82].

[72] *See* 9series Solutions, *The Impact of Artificial Intelligence on Social Media*, MYSTORY (June 7, 2019), https://yourstory.com/mystory/the-impact-of-artificial-intelligence-on-social-me [https://perma.cc/J9PL-UQM9].

[73] *Id.*

[74] DANIEL ZENG ET AL., SOCIAL MEDIA ANALYTICS AND INTELLIGENCE 14 (IEEE Computer Society, 2010), https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5678581 [https://perma.cc/5DBP-VNK7].

[75] This assumes no "public safety" exception would apply to the warrant requirement. *See* Mincey v. Arizona, 437 U.S. 385, 393–94 (1978) (stating "warrants are generally required . . . unless 'the exigencies of the situation' make the needs of law enforcement so compelling that the warrantless search is objectively reasonable.").

2. Private Sector Participation

Section 702 mandates private companies, such as ISPs, to comply with FISA requests for electronic communications.[76] The government compensates these companies for their compliance and absolves them of any liability that may result.[77] Finally, Section 702 provides these electronic communication service providers with an opportunity to challenge such intelligence directives under the Fourth Amendment.[78]

This same structure can be applied to social media companies. For example, this statute proposed in this article would include language requiring social media companies to integrate AI software that is based on the FBI's preexisting behavioral indicators of imminent violence. Essentially, this would automate and de-humanize the process of determining threatening behavior.[79]

Like Section 702, Congress should require the ongoing transfer of "red flags" to the FBI. Using the NWS example above, when Facebook's "domestic terror AI" flags a person as a "tornado warning," that signal would be immediately available to the FBI for further investigation. Additionally, the new statute should provide the same protections to social media companies that Section 702 provides to electronic communications companies. The FBI could compensate social media companies for the cost of transferring and providing the data. It could also provide protection from any civil liability arising from the data sharing.

3. Limited Timeframe

Under Section 702, an order permitting the DNI and AG to target non-U.S. persons only survives for one year.[80] This limitation prevents boundless and open surveillance on foreign persons by requiring the agencies to maintain certifications of relevance on an annual basis.[81] Should Congress pass a statute mandating early AI detection, several methods of time limitation arise. First, Congress could limit the "front end" of the investigation. For example, once the FBI receives a "red flag

---

[76] 50 U.S.C. § 1881a(i)(1), (5) (2018).

[77] 50 U.S.C. § 1881a(i)(2)–(3).

[78] 50 U.S.C. § 1881a(i)(4), (6).

[79] *See* K.A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 1, 66 (2003) ("The automated analysis of potentially relevant transactional data while shielding the exposure of individual identity to a generalized search protects privacy by maintaining anonymity, which in turn preserves autonomy.").

[80] 50 U.S.C. § 1881a(a).

[81] 50 U.S.C. § 1881b(b)(1)(F).

warning" from a social media's AI platform, the statute could limit how long the FBI has to secure a warrant. This would prevent the FBI from retroactively seeking a warrant from somebody who triggered a "warning" status at a previous time, but currently no longer does. Second, the statute could limit the "back end" of the investigation. This would limit a court order allowing the FBI to investigate a suspect's electronic communications to a specific timeframe (e.g., one year, similar to Section 702 limitations).

4. Judicial Review

Section 702 provides judicial review for both the submitted certifications for surveillance and the procedures used during the investigation to ensure compliance with FISA.[82] Furthermore, Section 702 provides appeals processes to review the FISC's initial determination.[83]

Congress could similarly provide for judicial review of the FBI's certification through an Article III court and subject it to Fourth Amendment jurisprudence. "Domestic terrorism," while defined in a criminal statute, carries no criminal penalties.[84] This is because, so far, all acts of domestic terrorism have been covered by criminal law.[85] Consequently, Article III courts are adequate for reviewing the constitutionality of a domestic surveillance search.

Additionally, Congress should grant the court jurisdiction over the FBI's domestic surveillance procedures, based on its authority granted under Article III of the Constitution. Section 702 expressly enumerates targeting, minimization, and querying procedures as subject to FISC jurisdiction.[86] Similarly, Congress should outline the appropriate procedures for targeting and minimization procedures for domestic surveillance and subject those procedures to judicial review.

---

[82] 50 U.S.C. § 1881a(j).

[83] 50 U.S.C. § 1881a(j)(4).

[84] 18 U.S.C. § 2331(5). *But see* Barbara McQuade, *Proposed Bills Would Help Combat Domestic Terrorism*, LAWFARE (Aug. 20, 2019), https://www.lawfareblog.com/proposed-bills-would-help-combat-domestic-terrorism [https://perma.cc/UA2P-N7QC] ("[Proposed legislation making domestic terrorism a crime] would provide much-needed tools to federal agents and prosecutors who sometimes find themselves without adequate means for addressing domestic terrorism.").

[85] *See* Robert Chesney, *Should We Create a Federal Crime of "Domestic Terrorism"?*, LAWFARE (Aug. 8, 2019), https://www.lawfareblog.com/should-we-create-federal-crime-domestic-terrorism [https://perma.cc/K6XF-2DFE] ("We do not have a situation in which persons who are involved in terrorist attacks somehow end up walking free, or getting improperly light sentences, due to a gap in the scope or calibration of criminal laws.").

[86] 50 U.S.C. § 1881a(j)(2).

A. Conclusion

In summary, the language of Section 702 affords Congress a structure utilizing limited surveillance measures to prevent acts of domestic terrorism. If national leaders prioritized this issue over their political safety, they would quickly learn there is room for both common sense domestic safety policy and constitutional liberties.

Authorizing the FBI to access Section 702 data is likely a necessary, yet insufficient, tool for solving the problem of domestic terrorism. The concept of sharing such information raises questions of boundaries as to constitutional and political limitations. Those limitations are addressed in turn in the following sections.

III. CONSTITUTIONAL LIMITATIONS ON THE DOMESTIC USE OF SECTION 702

James Manson leads an organization called the "Atomwaffen," a group *Vox* describes as a "particularly radical alt-right group . . . openly encouraging supporters to plan and commit 'lone wolf' attacks on African Americans, Jews, and other minority groups."[87] Manson authored *Siege*, a newsletter published between 1980 to 1986, urging his readers to engage in "individual acts of violence," which "could add up, destabilizing the American political system and bringing on a race war."[88]

In 2015, Dylann Roof responded to Manson's call for individual acts of violence when he opened fire in a black church in Charleston, South Carolina, killing nine people.[89] He did so with "the explicit intent of sparking a 'race war' [in America]."[90] Two researchers at the Anti-Defamation League have reported four examples of individuals motivated by Roof to commit similar acts.[91] One of the individuals said that he wanted to "pull a Dylann Roof," and "make the news some more and

---

[87] Zack Beauchamp, *An Online Subculture Celebrating the Charleston Church Shooter Appears to be Inspiring Copycat Plots*, VOX (Feb. 7, 2019, 3:35 PM), https://www.vox.com/policy-and-politics/2019/2/7/18215634/dylann-roof-charleston-church-shooter-bowl-gang [https://perma.cc/YA3B-BFXT].

[88] *Id.*

[89] *Id.*

[90] *Id.*

[91] *Hardcore White Supremacists Elevate Dylann Roof to Cult Hero Status*, ANTI-DEFAMATION LEAGUE (Feb. 6, 2019), https://www.adl.org/blog/hardcore-white-supremacists-elevate-dylann-roof-to-cult-hero-status [https://perma.cc/RE42-2VZD].

shoot some Jews."[92] Permeating social media sites, Roof's followers (referred to as the Bowl Gang) spread continued calls to violence in the name of the new "race war."[93]

This section identifies when these statements invoke presidential and congressional war powers. Next, it examines constitutional protections U.S. citizens maintain against those war powers. Specifically, this section considers whether: (1) an automated AI alert to the FBI constitutes a Fourth Amendment search; and (2) such threatening speech falls under the First Amendment's protection.

A. Limits on Constitutional Powers: War Powers

The *Prize Cases* provide perspective on these questions during the Civil War.[94] While Congress recessed in 1861, President Lincoln ordered a blockade of Southern ports after Southern forces attacked Fort Sumpter.[95] Union forces then captured four neutral vessels that allegedly violated the blockade.[96] The defendants argued they were mere "insurgents" or "traitors" rather than "belligerents" or "enemies," proscribing the usual consequences of war.[97] The owners of these vessels argued this conflict did not constitute traditional criteria for war, as the conflict did not arise between nations.[98]

The Court responded by clarifying that Article II vests the "whole Executive power" in the Presidency.[99] The court interpreted that power as not only licensing the President to respond to foreign threats but *binding* him "to resist force by force," that is, "to accept the challenge without waiting for any special legislative authority."[100] Important for our purposes, the Court clarified that "whether the hostile party be a foreign invader, or States organized in rebellion, it is none the less a war, although the declaration of it be 'unilateral.'"[101] The Court also highlighted the fact that Congress ratified President Lincoln's actions, arguing such ratification

---

[92] Beauchamp, *supra* note 87; *see also* Hardcore White Supremacists Elevate Dylann Roof to Cult Hero Status, *supra* note 91.
[93] *Id.*
[94] The Prize Cases, 67 U.S. (2 Black) 635, 668 (1862).
[95] *Id.* at 637.
[96] *Id.*
[97] *Id.* at 667.
[98] *Id.*
[99] *Id.* at 668.
[100] *Id.*
[101] *Id.*

supported the argument that "war" existed. Therefore, Lincoln's actions were constitutionally permitted.[102] Consequently, the Court deferred to the President's characterization of the conflict as a "civil war" and the defendants as "belligerents" because this characterization was a "question to be decided by him, and this Court must be governed by the decisions and acts of the political department of the Government to which this power was entrusted."[103]

The "War on Terror" follows the *Prize Cases*' recipe for proscribing war. Commentators have argued the presidential war powers and their congressional ratification through the Authorization for Use of Military Force (AUMF) are limited because Al-Qaeda and its affiliates are not traditional nation-state enemies.[104] But as other academics have noted, the peculiarity of the war opponent has not prevented previous use of presidential war powers.[105] The Mexican-American War, Civil War, and Spanish-American War all required military engagement with military opponents maintaining "no formal connection to the state enemy."[106] Additionally, other past authorizations of force have been directed at *non*-military officials or state actors "such as slave traders, pirates, and Indian tribes."[107]

It follows, then, that Congress' ability to declare war, and the President's ability to prosecute war, are not limited to traditional notions of state actors engaged in open warfare against the United States. However, does the Constitution permit executing such powers against U.S. citizens?

In *Hamdi v. Rumsfeld*, the Court considered whether the war powers of the Constitution could be applied against a United States citizen.[108] Specifically, the Court considered whether a United States citizen maintained a right to habeas corpus despite his detainment as an enemy combatant. There, the Court held that "[w]hatever power the United

---

[102] *See id.* at 671 (noting Congress ratified the President's action).

[103] *Id.* at 670 ("The proclamation of blockade is itself official and conclusive evidence to the Court that a state or war existed which demanded and authorized a recourse to such a measure, under the circumstances peculiar to the case.").

[104] *See, e.g.*, Bruce Ackerman, *The Emergency Constitution*, 113 YALE L.J. 1029, 1032–34 (2004) (noting that "[t]he wars with Afghanistan and Iraq were wars; the struggle against Osama bin Laden and al Qaeda is not."); *see also* David Cole, *Enemy Aliens*, 54 STAN. L. REV. 953 (2002).

[105] Curtis A. Bradley & Jack L. Goldsmith, *Congressional Authorization and the War on Terrorism*, 118 HARV. L. REV. 2047, 2067 (2005).

[106] *Id.*

[107] *Id.* at 2066.

[108] *See generally* Hamdi v. Rumsfeld, 542 U.S. 507 (2004).

States Constitution envisions for the Executive in its exchanges with other nations or with enemy organizations in times of conflict, it most assuredly envisions a role for all three branches when individual liberties are at stake."[109] Because of Hamdi's U.S. citizenship and right to due process, the *Hamdi* court refused to apply the Constitution's war powers against the defendant.[110]

Hamdi stands for the proposition that even if Congress has sanctioned the President to "resist force by force," such force may not be applied to a United States citizen without the courts' involvement.[111] Therefore, to the extent domestic terrorism involves U.S. citizens, any "force" against those citizens may not be granted without a blessing from all three branches of government.[112] In other words, even if Congress granted and the Executive approved some sort of force against domestic terrorism, U.S. citizens are still entitled to due process.[113] While Congress has not explicitly proscribed the intelligence community to war against domestic terrorism, this backdrop informs the Constitutional limits on congressional and executive war powers.

In light of the *Prize Cases* and *Hamdi*, it follows that the President has the authority to "resist force by force"; however, when applied to U.S. citizens, such force is subject to a court's determination of due process. Thus, if Congress decides to authorize the Executive to apply foreign intelligence tools against U.S. citizens, that authorization must be subject to judicial scrutiny.

As outlined above, by adopting Section 702's judicial review language, the statute proposed in this paper satisfies *Hamdi*'s required judicial scrutiny. By providing both a "front-end" judicial review of the FBI's warrant request for electronic communications and a "back end"

---

[109] *Id.* at 536. *But see* United States v. United States Dist. Court for Eastern Dist. Of Mich., Southern Division (*Keith*), 407 U.S. 297, 310 (1972) ("Implicit in [the President's War Powers] duty is the power to protect our Government against those who would subvert or overthrow it by unlawful means. In the discharge of this duty, the President—through the Attorney General—may find it necessary to employ electronic surveillance to obtain intelligence information on the plans of those who plot unlawful acts against the Government.").

[110] *Id.* at 2651.

[111] *Hamdi*, 542 U.S. at 581–83 (Thomas, J., dissenting).

[112] *Id.* at 535.

[113] *But see* U.S. DEP'T OF JUSTICE, *supra* note 9, at 38 (discussing the legality of drone strikes against U.S.-citizen terrorist, al-Aulaqi) ("Because al-Aulaqi is a U.S. citizen, the Fifth Amendment's Due Process Clause, as well as the Fourth Amendment, likely protects him in some respects even while he is abroad.").

judicial review of the FBI's procedures, a domestic version of Section 702 would provide extensive judicial scrutiny, preventing overreach of presidential and congressional war powers.

B. Constitutional Liberties: First and Fourth Amendment Considerations

United States v. United States District Court, otherwise known as the "*Keith* case," remains the leading authority on domestic surveillance.[114] Decided before the enactment of FISA, the *Keith* court refused to extend a "national security" exception to the warrant requirement for domestic surveillance.

1. Keith v. Proposed Domestic Terrorism Statute: Factual Distinctions

Despite *Keith*'s assumed applicability to domestic surveillance questions, its factual distinctions from current domestic terrorism compel different legal conclusions concerning the scope of domestic surveillance. First, *Keith* arose when U.S. citizens bombed a CIA office in Ann Arbor, Michigan.[115] That is, *Keith* arose when U.S. citizens enacted violence *against their own government.* In contrast, the domestic terrorism currently imperiling the United States involves acts of violence targeting innocent U.S. citizens. While subtle, this factual distinction impacts First Amendment considerations.

Second, in *Keith*, the government wiretapped the defendants' communications without a warrant.[116] There, the defendants' communications were private phone conversations.[117] They were not public communications. The statutory language suggested in this paper would determine risks based on language and data placed into public discourse.

Third, and perhaps most critically, *Keith* was decided before 9/11. Consequently, *Keith* analyzed the FBI's actions through a lens of traditional law enforcement, rather than through the "prevention" lens

---

[114] United States v. United States Dist. Court for Eastern Dist. Of Mich. (Keith) 407 U.S. 297 (1972); *see* Chesney, *supra* note 85 ("There has not been any significant appetite, since the 1970s, for crafting a purely domestic surveillance system along the lines the Supreme Court suggested in the famous *Keith* case.").

[115] *Keith*, 407 U.S. at 299.

[116] *Id.* at 300–01.

[117] *Id.* at 299.

established by the 9/11 Commission Report.[118] The proposed domestic terrorism statute arises from the intelligence community's new prevention charge. While human rights are not subject to the changing needs of government, the law makes clear that certain rights are abrogated by certain actions (e.g., murder may deprive a citizen of her right to liberty, or even life). The question here is whether public disregard for human life can create a legal basis for the government to engage in preventive measures.

2. Fourth Amendment Distinctions

These factual distinctions compel different legal conclusions. First, the government's actions in *Keith* clearly constituted a "search," whereas the surveillance proposed in this paper would not. Second, even if the proposed amendment constituted a search, post-*Keith* Fourth Amendment jurisprudence has provided applicable exceptions to the warrant requirement.

To begin, while the government's actions in *Keith* clearly constitute a Fourth Amendment "search," the proposed amendment does not. Only six years before *Keith*, *Katz v. United States* ruled that federal wiretaps of phone conversations violated the Fourth Amendment.[119] Before *Katz*, the legal test for whether a search had occurred was whether the government physically trespassed onto a person's "constitutionally protected area."[120] *Katz* transitioned the test to consider whether the government violated a person's "reasonable expectation of privacy."[121] In 2012, *United States v. Jones* held that both tests are appropriate for determining whether a Fourth Amendment search occurred.[122]

However, subsequent cases have held that government intrusions on social media sites do not constitute searches for purposes of the Fourth Amendment. In 2011, the City of New York charged Malcom Harris with disorderly conduct for his involvement in "Occupy Wall Street." There, the court held "[t]here can be no reasonable expectation of privacy in a

[118] THOMAS H. KEAN & LEE HAMILTON, THE 9/11 COMMISSION REPORT 364 (Authorized ed. 2004).

[119] Katz v. United States, 389 U.S. 347, 353 (1967) ("The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment.").

[120] *See id.* at 352 (citing Olmstead v. United States, 277 U.S. 438, 457, 464, 466 (1928)).

[121] *Id.* at 360 (Harlan, J., concurring).

[122] United States v. Jones, 565 U.S. 400, 413 (2012).

tweet sent around the world. . . . So long as the third party is in possession of the materials, the court may issue an order for the materials from the third party when the materials are relevant and evidentiary."[123] The court for the U.S. District of Georgia followed suit in a case involving Facebook, holding "[the defendant] fails to acknowledge the lack of privacy afforded her by her selected Facebook setting. While [defendant] may select her Facebook friends, she cannot select her Facebook friends' friends . . . [making] her page available to potentially hundreds, if not thousands, of people whom she did not know."[124]

The proposed statute does *not* suggest that the FBI should monitor all social media profiles for clues of criminal activity. Rather, the statute merely proposes public-private partnerships that alert the FBI to conditions ripe for violence. These alerts are rooted in behavioral analytics the FBI already uses to determine violence and the imminence thereof. Further, these alerts are used for preventive, not prosecutorial, evidence-gathering purposes. The alerts merely provide a proactive means to alert the FBI to potential dangers, causing warrants to be obtained sooner than they otherwise may have been able to.

Second, even if an AI alerting system constituted a "search," it falls within the "public safety" exception to the warrant requirement. *Keith* held the government's domestic surveillance violated the Fourth Amendment because judicial approval occurred *after* the surveillance already occurred. The government argued that a "special circumstances" exception should be applied to the warrant requirement, given the distinctions between "domestic security" and criminal cases.[125] The Court rejected this argument, holding:

> The circumstances described do not justify complete exemption of domestic security surveillance from prior judicial scrutiny. Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech. Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such

[123] People v. Harris, 949 N.Y.S.2d 590, 593–94 (N.Y. City Crim. Ct. 2012) (citing 18 U.S.C. § 2703[d]; People v. Carassavas, 426 N.Y.S.2d 437 (Saratoga Cty. Ct. 1980)).

[124] Chaney v. Fayette Cty. Pub. Sch. Dist., 977 F. Supp. 2d 1308, 1315 (N.D. Ga. 2013).

[125] United States v. United States Dist. Court for Eastern Dist. Of Mich. (*Keith*), 407 U.S. 297, 318–19 (1972).

surveillances to oversee political dissent.[126]

Admittedly, not until the 1978 *Mincey v. Arizona* decision (six years after *Keith*) did the U.S. Supreme Court expand the "exigent circumstance" warrant exception to include public safety.[127] However, *Mincey* adopted a 1969 case from the Court of Appeals for the District of Columbia to expand the exception, which would have been available to *Keith* as well.[128] Regardless, *Keith* only recognized a limited number of exceptions to the warrant requirement: "[searches that] serve the legitimate needs of law enforcement officers to protect their own well-being and preserve evidence from destruction."[129] "Public safety" provides the very basis for the proposed statute. Falling squarely within the language of *Mincey*, the proposed amendment provides proactive alerts to the FBI of conditions that threaten public safety. Therefore, no warrant should be necessary for the AI alerts.

To suggest *Keith* forecloses any opportunity to conduct domestic surveillance based on a domestic version of Section 702 is to misunderstand the aforementioned factual and legal distinctions between *Keith* and the proposed statute. *Keith*'s holding may make sense in light of the government's surveillance involved there; however, it fails to reach a domestic version of Section 702 that would target U.S. citizens based on warning indicators arising from public social media posts. *Keith* left the door open for Congress to apply surveillance techniques against "domestic security" that differ from those used in traditional criminal law:

> Given those potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens.[130]

---

[126] *Id.* at 320.

[127] *See* Mincey v. Arizona, 437 U.S. 385, 392 (1978) (citing Wayne v. United States, 318 F.2d 205, 212 (D.C. Cir. 1969)) ("The need to protect or preserve life or avoid serious injury is justification for what would be otherwise illegal absent an exigency or emergency.").

[128] *Id.* (adopting *Wayne*, 318 F.2d at 212).

[129] *Keith*, 407 U.S. at 318.

[130] *Id.* at 322–23.

Based on the foregoing, the domestic version of Section 702, as outlined in this paper, would reasonably relate to the "legitimate need of Government for intelligence" and the "protected rights of our citizens."

3. First Amendment Distinctions

As the court explained in *Keith*, "National security cases, moreover, often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime."[131] Justice Powell cited Senator Gary Hart's speech, expressing First Amendment concerns with domestic surveillance in the name of national security:

> As I read it—and this is my fear—we are saying that the President, on his motion, could declare—name your favorite poison—draft dodgers, Black Muslims, the Ku Klux Klan, or civil rights activists to be a clear and present danger to the structure or existence of the Government.[132]

As the Keith court went on to say, "The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation."[133]

The FBI addressed this concern in its 2017 Behavior Analysis Unit report.[134] Specifically, the report concludes: "As a threat assessment strategy, monitoring a person of concern's communications is sometimes recommended; these may include publicly accessible social media or weblog ('blog') posts."[135] As the report highlights, however, the constitutional right to free speech does not extend to all forms of expression.[136] Particularly, the FBI points out "true threats" as a form of unprotected speech.[137] The report defines a "true threat" as intending "to communicate a serious expression of intent to commit unlawful violence

---

[131] *Id.* at 313.

[132] *Id.* at 314 (quoting 114 CONG. REC. 14750) (statement of Sen. Hart) ("The subsequent assurances, quoted in part I of the opinion, that § 2511(3) implied no statutory grant, contraction, or definition of presidential power eased the Senator's misgivings.").

[133] *Id.*

[134] *See* AMMAN, *supra* note 56, at 19.

[135] *Id.*

[136] *Id.*

[137] *Id.*

against an individual or group; he need not *intend to carry out* the threat."[138]

The report also recognizes the FBI must have "authorized purposes" for monitoring someone's speech. One authorized purpose is "trying to determine whether a person is exhibiting behaviors that pose a concern for significant and imminent violence."[139] It follows that using AI to monitor conditions for "significant and imminent" violence falls within First Amendment boundaries. Such a tool removes the FBI from "monitoring" speech. Rather, it informs the FBI, based on its own behavior analytics already in place, of early threats. It screens surveillance from being unequally applied based on political dissent or persuasion. Instead, the proposed language allows an objective "third party" to detect conditions ripe for concern, based on science-based factors of violence.

Conclusion

In summary, the proposed statute stands on all fours within constitutional limits on the executive branch and individual liberties. Additionally, the proposal is completely on point with balancing individual liberties and public safety. While *Keith* necessarily governs the limits on domestic surveillance, it explicitly leaves open the possibility for the type of surveillance considered here.

IV. UNDERCURRENTS IN COUNTERTERRORISM POLICY

Despite the constitutionality of this article's proposal, the fearmongering of politics will likely defeat it. One commentator notes that while he has "not seen anyone calling for an attempt to create a domestically focused analogue to . . . something akin to Section 702," such a proposal could "pass constitutional muster according to . . . *Keith*," but "smacks of authoritarianism."[140] The commentator correctly identifies political concerns over appearing "authoritarian." However, this provides a mere cursory explanation of the political concern. Instead, competing policy perspectives have arguably created three specific "tensions" surrounding questions of domestic terrorism in the intelligence community.

These tensions have confused and ultimately frustrated sound policy developments to address domestic terrorism. First, legal distinctions between foreign and domestic terrorism fail to reflect their factual

[138] *Id.* (citing Virginia v. Black, 538 U.S. 343, 359–60 (2003) (emphasis added).
[139] *Id.* at 20.
[140] *See* Chesney, *supra* note 85.

similarities. Second, after 9/11, the intelligence community faces new pressures to *prevent* atrocities, rather than merely *prosecute* those who commit them. Finally, inter-agency information sharing after 9/11 pulls domestic resources into international counterterrorism, without reciprocation.

A. Foreign/Domestic Terrorism Distinctions

First, legal distinctions between foreign and domestic terrorism fail to reflect their factual similarities. On the one hand, these distinctions make sense. Most obviously, foreign terrorism often (though certainly not always) involves non-U.S. citizens. Thus, any counterterrorism efforts are limited by statutory rights afforded to non-U.S. persons—not by the Constitution. This was especially obvious during questions of habeas corpus, detention, torture, and military tribunals.

Additionally, foreign acts of terror invoke different laws than acts of domestic terror. Foreign terrorism can implicate any number of international or humanitarian laws. Conversely, domestic terrorism involves acts usually criminalized by federal or state law.[141]

On the other hand, there are a few factual distinctions between foreign and domestic terrorism. Both involve acts of violence in the name of a higher call or mission. Both represent extremities in their higher call. Both draw significant attention due to the extensive damages and deaths they often create. Former FBI special agent Ali Soufan summarized this tension:

> America's law enforcement agencies, intelligence community and court system all treat these two scenarios differently. Those differences in treatment mask instructive similarities between these two forms of organized hate. Having spent almost 25 years fighting jihadi terrorism here and abroad, I see disturbing parallels between the rise of Al Qaeda in the 1990s and that of racist terrorism today.[142]

The degree of legal separation assumes a degree of factual distinction that does not exist between foreign and domestic terrorism. Consequently, policymakers hesitate to narrow the legal distinctions for fear of public

---

[141] *See* Shirin Sinnar, *Separate and Unequal: The Law of "Domestic" and "International" Terrorism*, 117 MICH. L. REV. 1333, 1339 (2019).

[142] Ali H. Soufan, *I Spent 25 Years Fighting Jihadis. White Supremacists Aren't So Different.* N.Y. TIMES (Aug. 5, 2019), https://www.nytimes.com/2019/08/05/opinion/white-supremacy-terrorism.html [https://perma.cc/V89D-KRX9].

scrutiny or constitutional intrusions. In sum, this fear prevents the pursuit of effective reform.

B. From Prosecution to Prevention

Second, after 9/11, the intelligence community faces new pressures to *prevent* atrocities, rather than merely *prosecute* those who commit them. In the 9/11 Commission Report, the Commission argues future intelligence efforts "should be accompanied by a preventive strategy that is as much, or more, political as it is military."[143]

The intelligence community's renewed focus on prevention expanded to the FBI—a new focus for an organization that traditionally sees itself as a law enforcement agency. In 2004, then-FBI Director Robert Mueller summarized this shift:

> Nearly a century ago, the FBI was created to investigate criminal activity that had begun to cross county and state lines . . . . Immediately following 9/11, the FBI's number one priority became the prevention of terrorist attacks. This required a systematic approach examining all aspects of Bureau operations . . . . [including] how we disseminate our intelligence information.[144]

Four years after 9/11, the *Los Angeles Times* published an article titled, *Go on the Offensive Against Terror*.[145] Calling for expansive intelligence efforts and the renewal of the USA PATRIOT Act, the article reflects a shift in American expectations on its intelligence community: do not just find the bad guys; keep them from ever doing this again.

Failure to recognize this shift in the intelligence community frustrates reasonable surveillance policy discussions. If we understood that some surveillance was used to prevent harm rather than criminalize behavior, we might be more comfortable with discussing reasonable solutions.

---

[143] KEAN & HAMILTON, *supra* note 118, at 364.

[144] Robert S. Mueller III, FBI Director, Speaker at the Kansas State University Landon Lecture Series (Apr. 13, 2004), https://www.k-state.edu/media/newsreleases/landonlect/muellertext404.html [https://perma.cc/7WWK-4X6X].

[145] John Yoo, *Go on the Offensive Against Terror*, L.A. TIMES, (July 13, 2005), https://www.latimes.com/archives/la-xpm-2005-jul-13-oe-yoo13-story.html [https://perma.cc/995C-NWVE].

C. Foreign Tools Unavailable for Domestic Terrorism

Finally, inter-agency information sharing after 9/11 pulls domestic resources into international counterterrorism, without reciprocation. According to former FBI Director Mueller, "Today, criminal and terrorist threats increasingly have [] international dimension[s]. . . . By September 11, 2001, we knew the world . . . was growing smaller and more interconnected in an evolving crime landscape."[146] Consequently, as Mueller summarizes, "The age of global threats has moved the Bureau into an age of global partnerships."[147]

But as the threat pendulum swings back to domestic terrorism, tools available to fight against international terrorism have not been available to the FBI for a similar threat. Currently, the intelligence community enjoys legal latitude to deploy a series of tools against foreign terrorism. As stated in the introduction of this paper, material support statutes, drone strikes, and enhanced interrogation are all afforded to the foreign intelligence community.

Post 9/11, some efforts to erode the "wall" between intelligence and criminal agencies have helped. For example, in 2001, President Bush's Justice Department reformed FISA to make foreign intelligence only "a purpose" of a FISA application, rather than "the purpose."[148] While such steps reflect a willingness to support the FBI's efforts, the intelligence community still preserves many institutional structures to resolve immediate problems. For example, the FBI's FISA request may take up to four months to be approved.[149] Furthermore, the request must still involve *foreign* intelligence, prohibiting FBI surveillance on individuals like Dakota Reed who threaten shootings at local schools. In sum, the Constitution allows for significant progress to be had in inter-agency communication and information sharing.

V. CONCLUSION: TEAR DOWN THE WALL

On September 11, 2001, the entire United States felt the smoke and debris that hovered over New York, Pennsylvania, and Washington D.C. The intelligence community stood stunned, wondering what it had missed. As reports of Massoui, Hazmi, and Mihdhar came to light, the intelligence

[146] *See* Mueller, *supra* note 144.
[147] *Id.*
[148] *See* Inspector General Report, *A Review of the FBI's Handling of Intelligence Information Related to the September 11 Attacks* (June 2006).
[149] Interview with Anonymous FBI Agent, *supra* note 55.

community faced the sickening reality that the "wall" between intelligence and criminal agencies provided terrorists with institutional support.

But, if you ask the average citizen on the street what concerns them more: a foreign terrorist attack or a private citizen going rogue most would likely express fear of a domestic attack.[150] In the wake of the El Paso and Dayton shootings, President Trump promised, "We can and will stop this evil contagion."[151] He directed the FBI to identify the necessary tools and said he would provide them with "whatever they need." "We must shine light on the dark recesses of the Internet and stop mass murders before they start," President Trump said.[152]

While imperfect, the proposal in this paper may merely spark a discussion concerning what foreign tools could be constitutionally applied to domestic terrorism and be effective to that end. It provides a constitutional framework for preventive action while respecting civil liberties. If politics be its demise, I only hope that in the process, this proposal inspires conversations that support both our safety and individual freedoms.

[150] *See* Vera Bergengruen & W.J. Hennigan, *"We Are Being Eaten from Within." Why America Is Losing the Battle Against White Nationalist Terrorism*, TIME MAG. (Aug. 8, 2019), https://time.com/5647304/white-nationalist-terrorism-united-states/ [https://perma.cc/3BXV-RJAD] ("White supremacy is a greater threat than international terrorism right now.").

[151] Donald Trump, President of the United States, Remarks by President Trump on the Mass Shootings in Texas and Ohio (Aug. 5, 2019), https://www.whitehouse.gov/briefings-statements/remarks-president-trump-mass-shootings-texas-ohio [https://perma.cc/6WZF-XE56].

[152] *Id.*