HEDGING OUR BETS: WHY CONGRESS SHOULD ENACT A TRIPARTITE FRAMEWORK TO REGULATE THE USE OF FOREIGN INTELLIGENCE INFORMATION IN CRIMINAL INVESTIGATIONS

*Cynthia Anderson**

To be prepared for war is one of the most effectual means of preserving peace.

- George Washington

First Annual Address, Jan. 8, 1790[1]

INTRODUCTION

Imagine that the government is attempting to locate a compound that houses an international narcotics operation, which it suspects is located somewhere in a rural, mountainous area. The government needs to gather as much information as it can about the size and layout of the compound in order to make strategic decisions about the most logical course of action. The National Geospatial-Intelligence Agency (NGA)[2] is tasked with mapping and imaging the area where the compound is believed to be located, and it is able to find a group of several large buildings surrounded by a high wall. The images also tell a story. It is winter, and all of the buildings are covered with freshly fallen snow, except one.

* *Juris Doctor*, American University Washington College of Law 2016. I would like to thank Professor Jennifer Daskal and Angela Urbano for the guidance they provided while writing this article. Their comments proved invaluable. I would also like to thank Professor Stephen Vladeck for introducing me to, and fostering my interest in, national security law and issues of executive power.

1 Edward Walker, Addresses and Messages of the Presidents of the United States, from Washington to Harrison 21 (1841).

2 *See infra* Part I.A (providing further information about the legal authorities underlying the NGA and the categories of intelligence collection).

The most logical explanation is that the building is kept at a significantly higher temperature than the others. Based on analysts' experience, the reason it is kept at a higher temperature is likely to illegally grow marijuana.[3]

If the government chose to instigate a criminal investigation and eventual prosecution, should the images gathered under the NGA's foreign intelligence authorizations be shared with law enforcement? The Supreme Court has held that the government must obtain a warrant to gather evidence in criminal investigations by using technology not generally available to the public.[4] However, neither the Supreme Court nor Congress has specified how that affects the use of information collected legally, yet without a warrant, pursuant to the NGA's foreign intelligence authorizations. As technology increasingly provides the government with the ability to obtain information equally relevant to both foreign intelligence and criminal terrorism, as well as narcotics investigations, a clear-cut answer is paramount to guide the Executive branch and to ensure protection of constitutional rights. This article argues that foreign intelligence information can be used in criminal investigations only for a limited subset of crimes, and that Congress should legislate to codify the standards used for approving use of foreign intelligence information in criminal investigations.

This article proceeds in three sections. Part I explains the purpose and structure of the United States Intelligence

---

[3] Police in the Netherlands have discovered illegal growing operations during snowstorms when the roof of one house is conspicuously free of snow. *See, e.g.*, Harriet Alexander, *Dutch Police Catch Cannabis Growers After Spotting Snow-Free Roof*, THE TELEGRAPH (Feb. 10, 2015, 11:44 AM), http://www.telegraph.co.uk/news/worldnews/europe/netherlands/11402633/Dutch-police-catch-cannabis-growers-after-spotting-snow-free-roof.html (recounting instances where Dutch police raided houses based on a lack of snow and noting that British authorities had used the same technique, both to successfully find illegal growing operations and where the occupants simply had a wood stove).

[4] Kyllo v. United States, 533 U.S. 27, 40 (2001). The Kyllo Court emphasized that a significant concern with use of thermal imaging to detect heat from marijuana grown illegally indoors was that it allowed the government "to explore details of the home that would previously have been unknowable without physical intrusion." *Id.* Thus, the holding is only peripherally implicated where, as here, technology is used not to obtain details about the inside of the home, but to view the home at all. The decision was also made in the context of a criminal investigation, not a foreign intelligence investigation. *See id.* at 29 (explaining that a thermal imaging device was used to determine that heat lamps were being used in the defendant's home, and that that information was used to get a criminal search warrant).

Community (IC) and the domestic legal authorities under which it operates. It next discusses the relatively sparse judicial record providing a Fourth Amendment framework within which to consider requirements for using foreign intelligence information. Finally, it reviews policy considerations affecting Congress' decision whether to legislate.

Part II of this article first argues that current statutory authorities do not adequately define when foreign intelligence information can be shared with law enforcement for use in criminal investigations. It next argues that Congress should proactively legislate to establish how the Executive can choose to share foreign intelligence information with the law enforcement community. Finally, it argues that the Fourth Amendment reasonableness requirement compels implementation of use restrictions for information gathered under foreign intelligence authorities.

Part III of this article recommends that Congress enact a tripartite framework to ensure compliance with the reasonableness requirements of the Fourth Amendment. The suggested tripartite framework would function as follows: first, sharing foreign intelligence information with law enforcement for investigations of foreign intelligence crimes is allowed subject to internal Executive policies and procedures; second, sharing foreign intelligence information with law enforcement for investigations of domestic national security crimes is allowed only upon approval of the President or the Attorney General of the United States; finally, sharing foreign intelligence information with law enforcement for investigations of normal crimes is limited to specified crimes and requires judicial authorization.

This article attempts to provide a reasonable solution to the problem created by the increasingly common overlap between activities legitimately subject to foreign intelligence surveillance and those constituting a violation of domestic criminal law. It assumes that any foreign intelligence information was legally and constitutionally collected and then seeks to determine how that information can constitutionally be shared with law enforcement.[5]

---

[5] This article does not address the question of whether current statutory authorities regulating foreign intelligence collection are constitutional in their own right. For some examples of the debate over the Foreign Intelligence Surveillance Act (FISA), *compare* Nicholas J. Whilt, *The Foreign Intelligence Surveillance Act: Protecting the Civil Liberties that Make Defense of our Nation Worthwhile*, 35 SW. U. L. REV. 361 (2006) (arguing that the Patriot Act amendments to FISA were unconstitutional because they fail to protect against government abuse), *with* Jennifer L. Sullivan, Note, *From "the Purpose" to "a*

I. BACKGROUND

Foreign intelligence collection has long been an important function of government in the United States and abroad. There are several recognized types of intelligence activities through which information is collected, such as signals intelligence and human intelligence. Statutory authorization for the IC to use these collection methods has varying degrees of specificity, but there is little Congressional guidance on how the information can permissibly be used after it is collected. The Supreme Court has not provided boundaries for permissible use either, though a number of circuit courts have determined that foreign intelligence is exempt from the Fourth Amendment's warrant requirement.[6] This section will discuss the limits that exist on Executive authority to use foreign intelligence in a criminal investigation and subsequently, the reasonableness of its use under the Fourth Amendment.

A. Foreign Intelligence in the United States

Intelligence is information gathered to enable government policy-makers to make informed decisions about national security and international relations.[7] Intelligence collection has been an integral function of governments since biblical times,[8] and the

Significant Purpose": Assessing the Constitutionality of the Foreign Intelligence Surveillance Act Under the Fourth Amendment, 19 NOTRE DAME J. L. ETHICS & PUB. POL'Y 379 (2005) (arguing that the Patriot Act does not violate either the warrant or reasonableness requirement of the Fourth Amendment).

[6] *See* United States v. Duggan, 743 F.2d 59 (2d Cir. 1984); United States v. Houng, 629 F.2d 908 (4th Cir. 1980); United States v. Buck, 548 F.2d 871 (9th Cir. 1977).

[7] MARK M. LOWENTHAL, INTELLIGENCE: FROM SECRETS TO POLICY 1, 4–5 (4th ed. 2009). Secrecy is key to intelligence gathering because of the nature of intergovernmental politics. *See id.* at 1 (explaining that the fact that governments hide some information from each other creates a cycle where governments seek to learn confidential information, and then to hide the ability to do so). Secrecy is, however, in direct conflict with the "openness that is an inherent part of a representative [democracy]." *Id.* at 17. This can create a tension between a government's need for an effective intelligence system and its underlying values.

[8] GLENN HASTEDT, ESPIONAGE: A REFERENCE HANDBOOK 76 (2003) (noting that there are "more than 100 references to spying and intelligence gathering" in the Bible).

United States is no exception.[9] Though statutory authorizations establishing the modern IC were not enacted until the end of World War II (WWII),[10] intelligence activities occurred during virtually every American war up to that point.[11] Indeed, in 1799, Congress recognized the importance of intelligence activities to the national security when it made spying within the Navy punishable by death.[12]

Although intelligence collection is not a new concept, it is important to frame this discussion in terms of what kind of information the U.S. government has categorized as relating to foreign intelligence. The two primary statutory authorities regulating foreign intelligence, the National Security Act of 1947 (National Security Act) and the Foreign Intelligence Surveillance Act (FISA) each define foreign intelligence differently.[13] The National Security Act uses more general terms, classifying it as "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities."[14] FISA more specifically describes the types of activities or conduct to which the foreign intelligence information should relate, and describes the necessary standard if the information concerns a United States person.[15] In particular, it refers to the ability to protect against certain actions by "a foreign power or by an agent of a foreign power"—a term of significance in other portions of the statute authorizing specific surveillance activities.[16]

---

[9] *See id.* at 2 (describing, among other examples, the Culper Net spy ring, which helped to expose Benedict Arnold during the Revolutionary War).

[10] LOWENTHAL, *supra* note 7, at 19 (recognizing the National Security Act of 1947 as what "gave a legal basis to the intelligence community").

[11] *See* HASTEDT, *supra* note 8, at 2–9 (providing examples of wartime espionage between the Revolutionary War and WWII).

[12] Act of Mar. 2, 1799, ch. 24, art. 1, cl. 35 (1799) (prohibiting activities "in the nature of" spying, as well as delivering "any seducing letter or message" from the enemy).

[13] Both authorities are discussed in greater detail, *infra* Part I.A.2–3.

[14] 50 U.S.C. § 3003(2) (2012). This is nearly identical to the phrasing used in Executive Order 12,333, a major non-statutory source regulating foreign intelligence collection. Exec. Order No. 12333 § 3.5(e), *reprinted as amended in* 50 U.S.C. § 3001 (2012).

[15] 50 U.S.C. § 1801(e) (2012) (requiring the information to be necessary to protect against attack or other specified harms if it concerns a United States person, though it must merely relate to such harms for non-U.S. persons). A United States person is a citizen, a lawful permanent resident, or certain entities such as U.S. corporations. *Id.* § 1801(i).

[16] *Id.* § 1801(e)(1)(A)–(C).

1. General Purpose and Uses

Foreign intelligence is used to protect national security and to inform diplomatic relations.[17] It provides policymakers with "context, . . . and an assessment of risks, benefits, and likely outcomes" upon which to base their decisions.[18] One obvious example of an issue of importance in foreign intelligence would be plans for a domestic terrorist attack. But it is also important for the President to be aware of any planned actions by allies that could result in the United States' obligation to commit troops or other aid.[19]

Policy makers use foreign intelligence information for a number of different purposes, including: setting Executive policy;[20] drafting effective legislation;[21] informing military action;[22] guiding discussions with other nations via the diplomatic process;[23] determining whether domestic security measures need to be enhanced, and where;[24] detaining or turning foreign operatives,

---

17 *See* LOWENTHAL, *supra* note 7, at 4–5 (explaining that governments must keep apprised of the "actions, policies, and capabilities" of not only their enemies, but of "neutrals, friends, or even allies" as well).

18 *Id*. at 3.

19 *Id*. at 5 (providing as an example the Japanese attack on Pearl Harbor, which Hitler likely would have discouraged, had he known in advance, to keep the United States out of WWII).

20 *See* JAMES IGOE WALSH, THE INTERNATIONAL POLITICS OF INTELLIGENCE SHARING 110–11 (2010) (explaining that one significant counterterrorism effort involves implementing policies to disrupt a group's recruitment and financing efforts, which intelligence can help accomplish by identifying the "grievances" that cause people to support the group). Intelligence also informs a number of standard reports, such as the President's Daily Brief and National Intelligence Estimates (NIEs), which represent the official analysis of the entire IC on a given issue. LOWENTHAL, *supra* note 7, at 63.

21 *See* LOWENTHAL, *supra* note 7, at 181 (noting that Congress "controls all [government] expenditures, makes [national security] policy in its own right, and performs oversight" of the IC).

22 The drone program is one example of how intelligence methods can support military actions. Drones can capture images that allow for tactical planning by military leaders. *Id.* at 37, 89. More controversially, the Predator drone carries Hellfire missiles and is able to immediately fire on identified targets "instead of having to relay the information to nearby air or ground units." *Id.* at 88.

23 *See* WALSH, *supra* note 20, at 112 (recognizing that differing intelligence capabilities lead the United States to coordinate counterterrorism efforts with other countries, but that unrelated political issues sometimes result in a country limiting cooperative counterterrorism efforts). Identifying political issues in advance could allow the United States to take steps to address the problem and thus keep counterterrorism efforts in place.

24 *See* Sir David Omand, *The Limits of Avowall: Secret Intelligence in an Age*

criminals, or terrorists so that they will provide additional information;[25] and, prosecuting individuals to prevent additional criminal actions that would harm the national security.[26]

2. Types of Authorized Collection

The National Security Act defines "Intelligence Community" to include six standalone agencies or offices,[27] as well as a number of intelligence offices located within larger organizations.[28] Each has a defined role within or without the boundaries of the United States.[29] The actions that the agencies are authorized to perform are generally categorized by their broader function as one of four types of intelligence: human intelligence (HUMINT), geospatial intelligence (GEOINT), measurement and signatures intelligence (MASINT), or signals intelligence (SIGINT).[30] Each of these may have various subtypes, such as communications intelligence (COMINT) as a function of SIGINT.[31]

---

of Public Scrutiny, *in* NATIONAL INTELLIGENCE SYSTEMS: CURRENT RESEARCH AND FUTURE PROSPECTS 235, 237 (Gregory F. Treverton & Wilhelm Agrell eds., 2009) (explaining that actionable intelligence information has led to decisions such as cancelling flights and restricting travelers from taking liquids on planes).

[25] *See* LOWENTHAL, *supra* note 7, at 97, 101 (explaining that one of the fundamental methods of Human Intelligence based collection is agent acquisition, and that relationships must sometimes be built with terrorists or narco-traffickers willing to penetrate a group for personal gain). *Cf.* David S. Kris, *Law Enforcement as a Counterterrorism Tool*, 5 J. NAT'L SEC. L. & POL'Y 1, 36–37 (2011) (explaining the legal basis for military detention of terrorists under the laws of war).

[26] *See* Kris, *supra* note 25, at 2 (recognizing law enforcement and criminal prosecution as one key tool in the fight against terrorism). Critics question whether foreign intelligence authorities are simply used as an "end run" around the Fourth Amendment requirements for criminal investigations. *See, e.g.*, Matthew R. Hall, *Constitutional Regulation of National Security Investigation: Minimizing the Use of Unrelated Evidence*, 41 WAKE FOREST L. REV. 61, 102–03 (2006) (expressing concerns about pre-textual use of FISA to obtain evidence for criminal investigations with no relation to national security).

[27] 50 U.S.C. § 3003(4) (2012) (listing the Office of the Director of National Intelligence, the Central Intelligence Agency, the National Security Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, and the National Reconnaissance Office).

[28] *See id.* (referencing, inter alia, intelligence elements within the armed forces, the FBI, the DEA, and the Department of Energy).

[29] *See* 50 U.S.C. § 3036 (2012) (stating the CIA has no "internal security functions," though it is responsible for coordinating all efforts by the IC to collect intelligence outside of the United States "through human sources").

[30] STEPHEN DYCUS ET AL., COUNTERTERRORISM LAW 130–31 (2d ed. 2012) (citing LOWENTHAL, *supra* note 7, at 82–105).

[31] LOWENTHAL, *supra* note 7, at 91.

HUMINT encompasses the activities most commonly associated with spying, such as working with informants in foreign organizations.[32] The Central Intelligence Agency (CIA) coordinates all HUMINT activities abroad, while the Federal Bureau of Investigation (FBI) is responsible for domestic HUMINT activities.[33] The Defense Intelligence Agency is tasked with managing HUMINT activities for the Department of Defense (DOD).[34]

GEOINT involves the mapping and imaging of geographic areas, some of which include manmade structures.[35] It may involve the use of satellites, airplanes, or drones to capture images or film of an area.[36] The NGA is responsible for the United States' GEOINT activities, and it can operate both domestically and abroad.[37] The hypothetical scenario described in the Introduction of this article involved the use of GEOINT to provide actionable foreign intelligence information.

MASINT attempts to determine "weapons capabilities and industrial activities" by taking measurements and readings.[38] For instance, it could involve using infrared imagery to show the heat reflected from certain surfaces or multispectral imagery to record radiation levels.[39] MASINT can be used to track narcotics activities or to determine whether a party has access to nuclear materials.[40] It is not a function of any specific agency, though both the DIA and the NGA are responsible for some MASINT collection.[41]

Finally, SIGINT is perhaps the most controversial,[42] yet most

---

32 *See* HASTEDT, *supra* note 8, at 52 (explaining that "classic human espionage" involves infiltrating organizations to "directly acquire" needed information and materials).

33 *See* 50 U.S.C. § 3001 (2012).

34 50 U.S.C. § 3038(b)(5) (2012).

35 LOWENTHAL, *supra* note 7, at 82.

36 *Id.* at 82–83.

37 *See* 50 U.S.C. § 401 (2012) ("The Director of the National Geospatial-Intelligence Agency is designated the Functional Manager for geospatial intelligence."); LOWENTHAL *supra* note 7, at 89 (noting that the NGA "is not restricted in its activity within the United States," though it cannot support law enforcement).

38 LOWENTHAL, *supra* note 7, at 96.

39 *Id.* at 83, 96.

40 *Id.* at 96.

41 *Id.* at 97.

42 *See, e.g.*, James Risen & Laura Poitras, *N.S.A. Report Outlined Goals for More Power*, N.Y. TIMES (Nov. 22, 2013), http://www.nytimes.com/2013/11/23/us/politics/nsa-report-outlined-goals-for-more-power.html (discussing leaked NSA

highly regulated, aspect of United States intelligence.[43] The NSA is responsible for U.S. SIGINT activities.[44] It involves the interception of signals containing metadata, electronic emissions, or the content of communications.[45] One example was the Section 215 metadata program, which allowed for bulk collection of call record information and enabled the NSA to search the data to find potential associates of known terrorists.[46] Many of the most recent cases addressing constitutionality of foreign intelligence authorizations under the Fourth Amendment have been in relation to SIGINT authorities utilized by the NSA.

3. Foreign Intelligence Sharing with Law Enforcement

The majority of statutory requirements detailing the necessary procedures to use foreign intelligence information in criminal investigations are located in FISA. FISA regulates the collection of foreign intelligence by means of: (1) electronic surveillance directed at a foreign power or agent of a foreign power when there is "no substantial likelihood" that a United States person was party to the communication;[47] (2) electronic surveillance directed at a foreign power or agent of a foreign power when the locations to be under surveillance are expected to be used by a foreign power or its agent, and a significant purpose of the surveillance is to obtain foreign intelligence information;[48] (3) business records for investigations requiring foreign intelligence information or to protect against international terrorism;[49] (4) installation of pen registers or trap and trace devices to obtain foreign intelligence

documents and "public outcry over the NSA's domestic operations").

[43] *Compare* 50 U.S.C. § 1804 (2012) (providing detailed instructions for how and when the government can apply for a court order to conduct electronic surveillance for foreign intelligence purposes), *with* 50 U.S.C. § 3036(d) (2012) (providing just four brief subsections delineating the CIA's responsibilities).

[44] *See supra* note 33.

[45] *See* LOWENTHAL, *supra* note 7, at 91–92.

[46] STEPHEN DYCUS ET AL., 2014–2015 SUPPLEMENT: NATIONAL SECURITY LAW FIFTH EDITION AND COUNTERTERRORISM LAW SECOND EDITION 128 (2014). After significant public outcry, the Section 215 program was terminated through enactment of the USA FREEDOM Act of 2015. *See also* Cody M. Poplin, *NSA Ends Bulk Collection of Telephony Metadata under Section 215*, LAWFARE (Nov. 30, 2015, 3:47 PM), https://www.lawfareblog.com/nsa-ends-bulk-collection-telephony-metadata-under-section-215.

[47] 50 U.S.C. § 1802(a)(1) (2012) (requiring only approval of the Attorney General).

[48] *Id.* § 1804(a) (requiring a court order from the FISA Court).

[49] *Id.* § 1861(a) (requiring a court order from the FISA Court).

information or protect against international terrorism;[50] and (5) physical searches in the United States to obtain foreign intelligence information, so long as the premises are under the control of a foreign power or its agent.[51]

In order to share information with law enforcement, FISA requires the intelligence agency that obtained the information to include a statement indicating that any foreign intelligence information obtained under FISA can only be used in criminal proceedings if prior approval is received from the Attorney General.[52] For both physical searches and electronic surveillance there are also "minimization procedures" to determine when information can be retained or disseminated.[53] The minimization procedures provide that: (1) information can be retained and disseminated to law enforcement if it "is evidence of a crime which has been, is being, or is about to be committed[;]" but (2) prohibits retention or dissemination of information related to a United States person for longer than 72 hours without a court order or a determination by the Attorney General that "the information indicates a threat of death or serious bodily harm."[54]

---

[50] *Id*. § 1842 (requiring a court order from the FISA Court).

[51] *Id*. § 1822 (requiring only approval of the Attorney General).

[52] *See id.* § 1806(b) (electronic surveillance); *Id.* § 1825(c) (physical searches); *Id.* § 1845(b) (pen records and trap and trace devices). This is likely because defendants must be notified if the information will be "enter[ed] into evidence or otherwise use[d] or disclose[d] in any trial, hearing, or other proceeding[.]" *See id.* § 1806(c)–(d) (electronic surveillance); *Id.* § 1825(d)–(e) (physical searches); *Id.* § 1845(c)–(d) (pen records and trap and trace devices). However, the authority providing for access to business records for foreign intelligence or international terrorism investigations does not require approval of the Attorney General for use of the information. *See id.* § 1861(h) (not mentioning approval by the Attorney General for use in criminal proceedings).

[53] *See* 50 U.S.C. § 1806(a) (2012) (requiring compliance with statutory minimization procedures for electronic surveillance); *Id.* at § 1825(b) (requiring adoption of minimization procedures for physical searches). Though information obtained through an authorized collection of business records does have minimization procedures, the information is explicitly allowed to be retained and disseminated if it is "evidence of a crime which has been, is being, or is about to be committed," even if it is related to a United States person. *Id.* at § 1861(g)(2)(C), (h). Additionally, information obtained using pen registers or trap and trace devices does not have minimization procedures at all. *See id*. § 1842 (not including any required minimization procedures, though the Attorney General is required to ensure promulgation of appropriate privacy procedures); *Id.*, at § 1845 (not including any required minimization procedures or mention of limiting dissemination).

[54] *See* 50 U.S.C. § 1801(h)(3)–(4) (2012) (electronic surveillance); *Id.* at § 1821(4)(C)–(D) (physical searches) (note that because the seventy-two hour restriction applies only to information related to U.S. persons, there is no statutory limitation on retaining and disseminating evidence of a crime by a non-

The National Security Act makes only scattered reference to when and how foreign intelligence information can be retained and disseminated to law enforcement for a criminal investigation. Section 3039 allows the IC to collect information upon request of a law enforcement agency if the information is related to a non-United States person and is collected outside of the United States.[55] Additionally, although outside of the National Security Act, section 3365 of Title 50 provides that foreign intelligence information can be disclosed to Federal officials when that information would assist them in performing their duties.[56]

Although other guidance does exist to regulate the use of foreign intelligence information, the President promulgates and maintains those authorities. For instance, Executive Order 12,333 (EO 12,333 or the Order) regulates IC activities not otherwise regulated by statute.[57] The Order allows for collection, retention, and dissemination of information if it "may indicate involvement in activities that may violate federal, state, local, or foreign laws[.]"[58] That portion of EO 12,333 does not define dissemination, but participation in law enforcement activities is later explicitly allowed in order to investigate "clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities[.]"[59]

Additionally, in 2014 President Obama published Presidential Policy Directive 28 (PPD-28) in response to controversies surrounding the nation's SIGINT activities.[60] Much of PPD-28 is

---

U.S. person).

55 50 U.S.C. § 3039(a) (2012) (note that information collected under this authority would likely be considered normal criminal evidence, rather than foreign intelligence information, because criminal law enforcement officials requested its collection for use in a criminal investigation).

56 *Id*. at § 3365(1) (the provision does specify that use of the information is still subject to limitations on unauthorized disclosure). Though the statute has been cited only twice in case law, it was used in one case to uphold as valid transmission of foreign intelligence information from the IRS to the FBI and, ultimately, to intelligence officials for the Russian Federation. *See* Zahedi v. Dep't of Justice, No. 10-694-JO, 2011 U.S. Dist. LEXIS 53024, at *1, *5–7 (D. Or. May 6, 2011).

57 Exec. Order No. 12,333 § 2.2, 46 F.R. 59941, *reprinted as amended in* 3CFR 1981, https://www.archives.gov/federal-register/codification/executive-order/12333.html (indicating that the Order provides authority "in addition to and consistent with" other laws).

58 *Id*. at § 2.3(i).

59 *Id*. at § 2.6(b).

60 President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), (transcript available at https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-

not applicable to a discussion of when foreign intelligence information can be used in criminal investigations. However, it does provide that the same dissemination standards for personal information that apply to United States persons under EO 12,333 are to be utilized for all collected information.[61]

B. Fourth Amendment Requirements for Foreign Intelligence Collection

In normal criminal investigations, the Fourth Amendment requires the government to obtain a warrant prior to conducting most searches or seizures.[62] However, the Supreme Court has recognized that the same protections are not always required in the context of national security investigations.[63] Instead, reasonableness has been largely accepted as the touchstone for determining whether evidence gathered through foreign intelligence authorizations is constitutional under the Fourth Amendment.[64] Thus far, the boundaries of reasonableness have only been defined by federal circuit courts.[65]

---

intelligence) (acknowledging that PPD-28 was issued in response to concerns about the NSA's bulk metadata collection programs).

[61] Presidential Policy Directive 28 § 4(a)(i) (Jan. 17, 2014), http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities. However, since it applies only to dissemination regulated by EO 12,333, PPD-28 does not extend to non-U.S. persons the same rights afforded to U.S. persons by statute. *See supra* note 55 and accompanying text (describing FISA's differing dissemination standards for U.S. persons versus non-U.S. persons).

[62] U.S. CONST. amend. IV ("The right of the people to be secure . . . against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause[.]"). *See, e.g.*, Horton v. California, 496 U.S. 128, 133 (1990) (explaining that searches and seizures are presumptively unreasonable unless authorized by a search warrant, subject to certain exceptions).

[63] United States v. U.S. District Court (*Keith*), 407 U.S. 297, 323 (1972) ("We do hold . . . that prior judicial approval is required for [domestic national security surveillance] and that such approval *may be made in accordance with such reasonable standards as the Congress may prescribe*." (emphasis added)).

[64] *See, e.g.*, *In re* Sealed Case No. 02-001, 310 F.3d 717, 742 (FISA Ct. Rev. 2002) (explaining that to resolve whether an amendment to the Foreign Intelligence Surveillance Act was constitutional, the question is whether the procedures prescribed are reasonable under the Fourth Amendment).

[65] *See* DYCUS, *supra* note 46, at 181–92 (discussing cases suggesting the existence of a foreign intelligence exception to the Fourth Amendment's warrant requirement and noting that the Supreme Court has not granted certiorari on any appeals).

1. The National Security and Foreign Intelligence Exceptions

The Supreme Court's only guidance regarding Fourth Amendment requirements was decided in the context of a domestic national security investigation. In *United States v. United States District Court*,[66] (*Keith*), the government conducted warrantless electronic surveillance against three individuals who were later charged with conspiracy to destroy public property.[67] The property in question was a CIA office in Ann Arbor, Michigan, and the surveillance was conducted pursuant to a longstanding Executive practice of requiring only the approval of the Attorney General for wiretaps used in national security investigations.[68] Although the target of the conspiracy was the CIA, both the activities and the organization being investigated were wholly domestic.[69]

As a case of first impression, the Court used the opportunity to limit government discretion in the national security context by holding that prior judicial approval is necessary for surveillance of domestic organizations.[70] At the same time, the Court established that the Fourth Amendment did not require the same protections for "domestic security surveillance" as are required for ordinary crime.[71] Rather, the Fourth Amendment would be satisfied if Congress created a statutory framework detailing the processes and procedures to be utilized for the government to receive judicial authorization.[72] The Court emphasized reasonableness as the

---

66 *See Keith*, 407 U.S. at 299, 323.

67 *Id.* at 299.

68 *Id.* (note that because only the Attorney General's authorization was required under this practice, neither Congress nor the judiciary could act as a check on Executive discretion).

69 *Id.* at 308–09.

70 *Id.* at 321.

71 *Id.* At 322 (recognizing that the purpose and methods necessary to conduct surveillance for national security purposes differ from ordinary criminal investigations and that specificity in court applications is often not feasible).

72 *Keith*, 407 U.S. at 323 (suggesting as an example that Congress could (1) alter the probable cause requirements so that the affidavit "should allege other circumstances more appropriate" to national security investigations, (2) allow for applications to be heard only in a specially designated court due to the sensitivity of the topic, and (3) alter the time and reporting requirements from those required under Title III for criminal investigations). Congress essentially adopted the Court's suggested framework when it enacted FISA. *See also* Donald Q. Cochran, *Material Witness Detention in a Post-9/11 World: Mission Creep or Fresh Start?*, 18 GEO. MASON L. REV. 1, 35–36 (2010) (recognizing the parallels between FISA and the *Keith* framework).

standard against which Congress' legislation should be drafted.[73] In deciding the case, the Court also went to great pains to specify that its holding was not meant as judgment regarding surveillance of "foreign powers, within or without this country."[74]

Some lower courts have utilized the statement in *Keith* to assert the existence of a foreign intelligence exception to the Fourth Amendment warrant requirement.[75] For instance, in *United States v. Butenko,*[76] the defendants were charged with conspiracy to communicate information related to the national defense to a foreign government.[77] After the circuit court initially held that there was insufficient evidence offered by the government to support one of the charges in the indictment, the government disclosed additional evidence gathered through warrantless wiretaps.[78] In determining whether the information was illegally obtained, the court acknowledged the *Keith* holding regarding surveillance of domestic organizations.[79] It concluded, however, that the strong public interest in "the efficient operation of the Executive's foreign policy-making apparatus" counterbalanced the benefits of prior judicial authorization.[80] The court thus held that in determining whether a search was reasonable, courts should analyze whether obtaining foreign intelligence information was the primary purpose, rather than applying the traditional probable

---

[73] *Keith*, 407 U.S. at 322–23 ("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.").

[74] *Id.* at 308.

[75] *See* United States v. Butenko, 494 F.2d 593, 605–06 (3d Cir. 1974) (holding that there is an exception to the warrant requirement when surveillance is conducted primarily for foreign intelligence purposes). *See also,* United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973) (holding that only Executive approval is necessary to conduct electronic surveillance for foreign intelligence purposes "because of the President's constitutional duty to act for the United States in the field of foreign relations, and his inherent power to protect national security in the context of foreign affairs). *But see Zweibon* v. Mitchell, 516 F.2d 594, 653 (D.C. Cir. 1975) (rejecting the argument that a domestic organization's activities are exempted from the warrant requirement when the activities affected foreign affairs, and rejecting, in dicta, that any warrantless "foreign security surveillance" would be reasonable under the Fourth Amendment).

[76] United States v. Butenko, 494 F.2d 593 (3d Cir. 1974).

[77] *Id.* at 596.

[78] *Id.*

[79] *Id.* at 605.

[80] *Id.* at 605 (comparing the strong public interest in obtaining timely foreign intelligence information to the public interests justifying other exceptions to the warrant requirement, such as search incident to arrest).

cause standard.[81]

Although most cases discussed were decided in relation to electronic surveillance, the warrant requirement may not apply to physical searches conducted for foreign intelligence purposes either. In *United States v. Ehrlichman,*[82] a government agent faced criminal charges because he coordinated the burglary of a psychiatrist's office to obtain information about a patient who had leaked classified information.[83] The defendant argued that the search complied with the Fourth Amendment because "it was undertaken pursuant to the President's delegable constitutional prerogative in the field of foreign affairs to authorize such a search."[84] However, neither the President nor the Attorney General gave prior authorization to conduct the search.[85] The D.C. Circuit rejected the defendant's assertion, noting that "if Presidential approval is to replace judicial approval for foreign intelligence gathering, the personal authorization of the President or . . . the Attorney General, is necessary to fix accountability and centralize responsibility[.]"[86]

Although the Supreme Court has never ruled on the validity of the foreign intelligence exception, there are other Fourth Amendment doctrines that support the idea that some protections do not apply in the foreign intelligence context. By statute and Executive order, the target of foreign intelligence surveillance will

---

[81] *Id.* at 606. This concept of requiring the "primary purpose" to have been collecting foreign intelligence information was more fully developed by the Fourth Circuit in 1980. *See infra* the discussion regarding *United States v. Truong*, Part I.B.2.

[82] United States v. Ehrlichman, 546 F.2d 910 (D.C. Cir. 1976).

[83] *Id.* at 914 (the patient, Daniel Ellsberg, had been indicted for his role in the publication of the Pentagon Papers).

[84] *Id.*

[85] *Id.* at 925.

[86] *Id.* at 926. Although the *Ehrlichman* opinion is far from a ringing endorsement of the foreign intelligence exception, it is worthy of note for two reasons. First, just one year earlier the D.C. Circuit had rejected in dicta the view that a foreign intelligence exception could exist. *See* Zweibon v. Mitchell, 516 F.2d 594, 653 (D.C. Cir. 1975) (rejecting the argument that a domestic organization's activities are exempted from the warrant requirement when the activities affected foreign affairs, and rejecting, in dicta, that any warrantless "foreign security surveillance" would be reasonable under the Fourth Amendment). Second, the district court in *Ehrlichman* had explicitly rejected the idea that the President, rather than a warrant, could ever provide authorization for a physical search to gather foreign intelligence information. United States v. Ehrlichman, 546 F.2d 910 (D.C. Cir. 1974). In that context, the circuit court's decision was surprisingly supportive of the existence of a foreign intelligence exception for physical searches.

generally be a non-United States person, limiting the circumstances under which the Fourth Amendment could be held to apply.[87] In *United States v. Verdugo-Urquidez*,[88] a Mexican citizen was arrested for charges related to his involvement in a drug cartel after issuance of a U.S. arrest warrant, but at his home in Mexico.[89] After his arrest and transfer to the United States, agents of the U.S. Drug Enforcement Agency (DEA) coordinated with local Mexican officials to conduct a search of the defendant's home.[90] Because the DEA agents did not obtain a search warrant, the defendant moved to suppress the evidence as having been collected in violation of the Fourth Amendment.[91] The Court rejected the defendant's argument, holding that a non-U.S. citizen, without "significant voluntary connection[s]"[92] to the United States, did not have Fourth Amendment protections for a search conducted outside of the United States.[93]

In his dissenting opinion, Justice Brennan took issue with the conclusion that the defendant did not have a "sufficient connection" to the United States because the government was prosecuting him for violation of U.S. law and would be holding him in a U.S. prison.[94] Although the majority did not respond directly to Brennan's argument, it did discuss the "significant and deleterious consequences for the United States in conducting activities beyond its boundaries"[95] if Fourth Amendment protections were extended to aliens outside of the United States.[96] Rather, the Court determined that the political branches must impose any restrictions on searches or seizures affecting non-U.S. persons outside of the United States.[97]

---

87 *See supra* note 14, and accompanying text.

88 United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).

89 *Id.* at 262.

90 *Id.*

91 *Id.* at 263.

92 *Id.* at 271.

93 *Id.* at 274–75.

94 *Verdugo-Urquidez*, 494 U.S. at 283 (Brennan, J., dissenting) ("The 'sufficient connection' is supplied not by Verdugo-Urquidez, but by the Government.").

95 *Id.* at 273.

96 *Id.* (emphasizing the "foreign policy operations" that would be affected by such a rule, like operations by the armed forces to protect national security interests).

97 *Id.* at 275 ("If there are to be restrictions on searches and seizures which occur incident to [an American response to the violation of our laws outside our borders], they must be imposed by the political branches through diplomatic understanding, treaty, or *legislation*." (emphasis added)).

The Fourth Amendment's applicability for overseas searches has also been limited in relation to United States persons, at least at the circuit court level. In *In re Terrorist Bombings* (Fourth Amendment Challenges),[98] the Second Circuit utilized the holding in *Verdugo-Urquidez* to determine whether the Fourth Amendment applied to searches involving U.S. citizens outside of the United States.[99] Although it acknowledged that it was "well settled" that the Fourth Amendment applies to U.S. citizens abroad,[100] the court held that the warrant clause does not apply.[101] The court cited dicta in *Verdugo-Urquidez* in which the Supreme Court noted that a warrant issued to authorize a search outside of the United States "'would be a dead letter'" to the foreign government.[102] The court further reasoned that application of the warrant clause was inappropriate because of "(1) the complete absence of any precedent in our history for doing so, (2) the inadvisability of conditioning our government's surveillance on the practices of foreign states, (3) a U.S. warrant's lack of authority overseas, and (4) the absence of a mechanism for obtaining a U.S. warrant."[103]

2. The Reasonableness Requirement

In order to meet the Fourth Amendment's reasonableness requirement, circuit courts initially held that foreign intelligence collection could only be excepted from the warrant requirement where obtaining foreign intelligence information was the "primary purpose" of the investigation. Although this requirement was stated without explanation six years earlier in *Butenko, United States v. Truong*[104] was later considered the preeminent case supporting the primary purpose doctrine.[105] In *Truong*, the government conducted a prolonged period of warrantless searches and wiretaps against the defendant, who provided classified

98 United States v. Odeh, 552 F.3d 157 (2d Cir. 2008).

99 *Id.* at 167.

100 *Id.*

101 *Id.* at 171.

102 *Id.* at 168 (citing Verdugo-Urquidez, 494 U.S. at 274).

103 *Id.* at 172. The court rejected the foreign intelligence exception as explained in Butenko and Truong because it concluded that the primary purpose doctrine applied the exception too narrowly. *See id.* at 172 (holding that the warrant clause does not apply to a search conducted abroad even if the primary purpose of the search was not collecting foreign intelligence information).

104 United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980).

105 Robotti, *infra* note 114, and accompanying text.

documents to a government informant.[106] Although the government knew that the defendant was breaking the law by attempting to provide classified information to the North Vietnamese government, it was initially unsure who within the government was leaking the information to the defendant.[107] Eventually the government learned who the leak was, but it continued to conduct warrantless surveillance of the defendant as a foreign intelligence investigation.[108]

The Fourth Circuit recognized the existence of a foreign intelligence exception to the warrant requirement.[109] It emphasized that the exception applied only when investigating "a foreign power, its agent or collaborators" because the surveillance otherwise resembles a normal criminal investigation.[110] It also held that the proper test for whether the warrantless surveillance was reasonable is to determine whether the surveillance was "conducted 'primarily' for foreign intelligence reasons."[111] Thus, while it upheld the surveillance conducted to determine Truong's source as reasonable, it excluded evidence obtained after internal DOJ memoranda indicated that a criminal prosecution was being initiated.[112]

The *Truong* primary purpose test became the standard in Fourth Amendment foreign intelligence jurisprudence in the years after it was decided.[113] Indeed, the Justice Department even utilized the concept in designing its procedures regulating the interaction between the law enforcement and foreign intelligence portions of the FBI.[114] After the September 11th attacks, the 9/11

---

106 *Truong*, 629 F.2d at 911. The defendant did not know, of course, that his contact was a government informant. *Id.*

107 *Id.* at 911–12.

108 *Id.* at 912.

109 *Id.* at 915.

110 *See id.* ("When there is no foreign connection, the executive's needs become less compelling[.]").

111 *See id.* (suggesting that a balancing test weighing individual privacy interests against government interests should be used to determine reasonableness, and that the government's foreign policy concerns only outweighed privacy interests where foreign intelligence collection was the primary purpose of the investigation).

112 *Truong*, 629 F.2d at 916.

113 *See* William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance,* 50 AM. U. L. REV. 1, 84–85 (2000) (recognizing that lower courts had applied the *Truong* primary purpose standard since it was decided in 1980).

114 Michael P. Robotti, *Grasping the Pendulum: Coordination Between Law Enforcement and Intelligence Officers Within the Department of Justice in a Post-*

Commission found that the structure of FBI and DOJ contributed to the failure to stop the attacks in advance because the structure prevented the flow of information.[115] In the wake of the Commission's report, Congress overrode the primary purpose requirement by statute, at least for searches conducted under FISA authorities.[116]

Since Congress' action, recent jurisprudence has rejected the idea that the primary purpose doctrine was ever a constitutional requirement. In 2002, *In re Sealed Case*[117] reviewed the new statutory provision requiring foreign intelligence to be a "significant purpose" of foreign intelligence surveillance under FISA.[118] The Court held that the primary purpose doctrine was not a fundamental requirement of the Fourth Amendment and that Congress had the authority to legislate the standard by which the government could conduct foreign intelligence surveillance.[119]

The FISA Court of Review also found that prosecution of foreign intelligence crimes was a reasonable use of foreign intelligence information so long as criminal prosecution was never the sole purpose of the surveillance.[120] In doing so, it emphasized the difference between the purposes of prosecuting foreign intelligence crimes and normal crimes.[121] The court prohibited using foreign intelligence authorizations when the sole purpose of the surveillance was a criminal prosecution; however, it did not extend the prohibition to the use of incidentally collected information to prosecute serious ordinary crimes.[122]

Several years after *In re Sealed Case* was decided, the FISA Court of Review provided a detailed analysis of reasonableness

---

"Wall" Era, 64 N.Y.U. ANN. SURV. AM. L. 751, 770–71 (2009).

115 *Id.* at 782.

116 *Id.* at 785. *See* 50 U.S.C. § 1804(a)(6)(B) (2012) (requiring applications to conduct surveillance under FISA to certify that obtaining foreign intelligence information is a "significant purpose" of the surveillance).

117 *In re* Sealed Case No. 02-001, 310 F.3d 717 (FISA Ct. Rev. 2002).

118 *Id.* at 728–29.

119 *Id.* at 746 (referencing the balancing test laid out in *Keith* for support).

120 *See id.* at 744 (comparing the purposes of prosecution for ordinary crimes and foreign intelligence crimes and acknowledging the distinction between the two under FISA).

121 *See id.* (noting that two main goals of ordinary criminal law are punishment and deterrence, but that the purpose of making foreign intelligence activities criminal is to provide another method of stopping the activity).

122 *See id.* at 731 (explaining that, under FISA "if through interceptions or searches, evidence of 'a serious crime totally unrelated to intelligence matters' is incidentally acquired, the evidence is '*not* . . . required to be destroyed'" (internal citations omitted)).

requirements under the Fourth Amendment for foreign intelligence surveillance. In *In re Directives,*[123] the Court held that, although the foreign intelligence exception exists, the Fourth Amendment reasonableness requirement must be met as determined by a totality of the circumstances test.[124] In upholding a FISA amendment that allowed the government "to direct communications service providers to assist it in acquiring foreign intelligence when those acquisitions targeted persons . . . believed to be located outside the United States[,]"[125] it emphasized that minimization procedures were one important aspect of the framework that made it reasonable under a totality of the circumstances analysis.[126]

The extent of minimization procedures imposed on collections under the Section 215 metadata program was more fully explained at the trial court level by the Foreign Intelligence Surveillance Court (FISC).[127] The Court's Primary Order, which detailed minimization procedures for the government, specified what standards the NSA must meet to disseminate information and what standards the FBI must meet should it receive foreign intelligence information.[128] In particular, the FBI was simply ordered to follow minimization procedures established under The Attorney General's Guidelines for Domestic FBI Operations (Sept. 29, 2008).[129] The NSA minimization procedures were detailed over

---

123 In re Directives Pursuant to Section 105b of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (FISA Ct. Rev. 2008).

124 *Id.* at 1012–13 (holding that even when the foreign intelligence exception applies, the Fourth Amendment reasonableness requirement must be met through a totality of the circumstances test).

125 *Id.* at 1006.

126 *See id.* at 1013–15 ("It is also significant that effective minimization procedures are in place. These procedures serve as an additional backstop against identification errors as well as a means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons."). The court also discussed pre-collection procedures, such as approval by the Attorney General to conduct surveillance, as factors contributing towards the reasonableness of FISA surveillance. *See* LOWENTHAL, *supra* note 7, at 91–92 (stating that Congress eliminated bulk metadata collection in 2015 through the USA FREEDOM Act).

127 *See In re Application,* No. BR 13-109, 11 (FISC Aug. 29, 2013) (Primary Order), http://www.fisc.uscourts.gov/sites/default/files/BR%2013-109%20Order-1.pdf.

128 *Id.* at 3–4.

129 *Id.* at 4. Note that these procedures applied when the FBI applied to the FISC to have information gathered by the NSA, and subsequently released to the FBI, under Section 215. *See id.* at 1–2 (explaining that the FBI had applied for production of certain records).

thirteen pages in the Primary Order, and included requirements such as restricting access to the metadata to only trained, authorized personnel, and obtaining approval of search terms from high-level officials at the NSA.[130]

C. Policy Considerations

Although the number of criminal investigations conducted based on foreign intelligence information is logically less than the number of ordinary criminal investigations, there are several policy considerations that make legislation a prudent course of action. First, by explicitly stating when the government may or may not choose to share foreign intelligence information for a criminal investigation, Congress would limit ambiguity of whether such actions were constitutional and discourage their occurrence in inappropriate circumstances. In the past, the IC has been shown to push the boundaries of constitutionality in times of stress, particularly where there was ambiguity in, or a lack of, legislative authorities. Additionally, by clarifying when information should be used in criminal prosecutions, Congress could encourage the choice to do so when it may be politically preferable to other options, such as the use of drone strikes or indefinite military detentions. But while there are ample reasons to support legislation, the negative consequences resulting from prior attempts to restrict IC involvement with law enforcement, namely "the Wall," must be considered in creating any new framework.

1. *Youngstown* Analysis of Executive Authority

Under Justice Jackson's Concurrence in *Youngstown Sheet & Tube Co. v. Sawyer*,[131] Executive authority can be measured

---

[130] *Id.* at 4–17.

[131] Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 634 (1952) (Jackson, J., concurring). Jackson's concurring opinion, and specifically the tripartite framework for analyzing execute power, has long set the standard for analyzing Presidential action. *See, e.g.*, Lawrence H. Tribe, *Transcending the Youngstown Triptych: A Multidimensional Reappraisal of Separation of Powers Doctrine*, 126 YALE L. J. 86, 86 (2016) (acknowledging the preeminence of the Jackson Youngstown framework in analyzing separation of powers issues. Jackson's concurring opinion, and specifically the tripartite framework for analyzing executive power, has long set the standard for analyzing Presidential action).

against three standards. First, if the President acts with express or implied statutory approval from Congress, his power is at its highest.[132] The action would be upheld as constitutionally valid so long as it was within Congress' power to legislate.[133] Second, if the President acts in an area where Congress has not legislated or where there is ambiguity, his power is in a "zone of twilight."[134] Here, action would have to rely solely on the Executive powers detailed in the Constitution and "any actual test of power is likely to depend on the imperatives of events and contemporary imponderables."[135] Finally, where the President acts in a way that is incompatible with express or implied statutory constraint, "his power is at its lowest ebb," and his action will be invalid in most cases.[136]

2. Effect of Legislative Ambiguity on IC Actions in Times of National Stress

History has shown that in times of national stress, the IC is apt to utilize any ambiguity in its authority to expand its surveillance programs to its furthest boundaries. While it is an understandable response to pressure from both Congress and the President, the programs often toe or cross the line of constitutionality. A 1970's report documented various constitutional abuses by the IC.[137] The pressures of the Cold War, mixed with a structure that left the agencies to their own devices, lead to an environment in which congressional authorization was largely bypassed and operations were conducted in violation of American constitutional rights.[138] For instance, the "Church Committee" found that the IC conducted

---

[132] *Youngstown*, 343 U.S. at 636.

[133] *See id.* at 636, 636 n.2 (providing as an example the Presidential authority to determine whether a "prohibition of the sale of arms and munitions" should go into effect in relation to a specific foreign conflict, which was upheld in United States v. Curtiss-Wright Exp. Corp., 299 U.S. 304 (1936)).

[134] *Id.* at 637.

[135] *Id.*

[136] *Id.* The Presidential action would only be allowed if it both fell within the President's constitutional powers, and Congress had acted without any constitutional basis. *Id.*

[137] *See* S. REP. NO. 94-755, bk. 2, at III (1976), https://www.intelligence.senate.gov/sites/default/files/94755_II.pdf ("This has been demonstrated in the intelligence field where, too often, constitutional principles were subordinated to a pragmatic course of permitting desired ends to dictate and justify improper means.").

[138] *See id.* at 22 (finding that the Cold War environment lead to an expansion of domestic intelligence activities and inadequate Congressional oversight).

many investigations based solely on an individual's political activities.[139] Although there were similar occurrences during WWII, "[n]o statutes were passed to prevent the kind of improper activity which had been exposed[,]" leaving self-regulation to occur within the Executive branch.[140]

More recently, in the wake of the 9/11 attacks, the NSA implemented the Terrorist Surveillance Program absent any congressional authorization.[141] The program was meant to provide surveillance coverage for an area not addressed by current law; specifically, situations in which one party to communication was located in the United States, but the other was located abroad.[142] Congress later adopted the program as an amendment to FISA, but legal commentators question whether the program was constitutional under only the President's constitutional powers.[143]

3. Public Concern Regarding Drone Strikes and Detention of Terrorists

Despite arguments by critics that broad foreign intelligence authorities will be used to pretextually pursue criminal investigations, the government has used several prominent non-prosecutorial programs in the fight against terrorism.[144] Drone strikes, for instance, have been a key part of the U.S. strategy in the fight against ISIS.[145] Indeed, drone strikes have been used

---

139 *Id.* at 7. Targets included the Women's Liberation Movement, Dr. Martin Luther King Jr., and the NAACP, to name a few. *Id.* at 7–8.

140 *Id.* at 21. While some of the activities were never prohibited by Congress, others—such as programs opening domestic mail and committing breaking and entering—were done in spite of existing legislation. *Id.* at 13–14.

141 DYCUS, *supra* note 30, at 222.

142 *Id.* at 222, 228.

143 *Id.* at 228, 232. The Section 215 bulk metadata collection program was also considered an unconstitutional expansion of the statutory authorization by the executive branch by legal commentators. *See, e.g.*, Orin Kerr, *Second Circuit Rules, Mostly Symbolically, That Current Text of Section 215 Doesn't Authorize Bulk Surveillance*, WASH. POST (May 7, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/05/07/second-circuit-rules-mostly-symbolically-that-current-text-of-section-215-doesnt-authorize-bulk-surveillance/?utm_term=.ad6bd61e9ed4 (agreeing with the Second Circuit that the text of Section 215 did not authorize the bulk metadata collection program).

144 *See supra* notes 21, 24, 25, and accompanying text (noting the use of foreign intelligence information to support drone and military detention programs, and explaining concerns about pretextual use of authorities for criminal investigations).

145 *See* Chelsea J. Carter et al., *U.S. Jet Fighters, Drones Strike ISIS Fighters, Convoys in Iraq*, CNN (Aug. 9, 2014, 12:43 AM), http://www.cnn.com/

throughout the War on Terror, with more than 100 instances being reported in Yemen alone.[146] Informational drone missions are a valid use of foreign intelligence information to support military operations, but the practice as it relates to airstrikes has received criticism in the international community.[147]

The United States has also utilized military detention of suspected terrorists at Guantanamo Bay as a method of combatting terrorism, with the intention of keeping the detainees out of the federal court system. Some of the detainees have been tried using military commissions, a practice that some argue is not legally justified,[148] while others have been subject to indefinite detention without trial.[149] The program has been the subject of several scandals over the years, including allegations that the detainees were tortured.[150]

4. The "Primary Purpose" Doctrine and "the Wall"

After 9/11, there was a congressional investigation into what lead to the intelligence failures that allowed for a successful attack on U.S. soil.[151] The report found that Department of Justice

2014/08/08/world/iraq-options/ (explaining that the U.S. strategy in the fight against ISIS relies on airstrikes, which are conducted through the use of fighter jets and drones).

146 *See Five Killed in Yemen Drone Strike*, AL JAZEERA (June 14, 2014), http://www.aljazeera.com/news/middleeast/2014/06/drone-strike-kills-armed-fighters-yemen-201461414184887079 6.html (reporting on a U.S. drone strike that killed an al-Qaeda leader).

147 *See, e.g.*, Ed Pilkington & Ryan Devereaux, *US Defends Drone Strikes as 'Necessary and Just' in Face of UN Criticism*, THE GUARDIAN (Oct. 25, 2013, 3:23 PM), http://www.theguardian.com/world/2013/oct/25/un-drones-us-policy-debate (explaining the United Nations had criticized drone strikes due to the ability to use them in secret and resulting accountability issues).

148 *See Detention*, AM. CIVIL. LIBERTIES UNION, https://www.aclu.org/national-security/detention (last visited Feb. 8, 2017) (arguing that the War on Terror does not implicate the laws of war such that indefinite military detentions are legal, and providing additional resources on U.S. military detention practices for terrorists).

149 *See* Daphne Eviatar, *Another Terrorism Conviction, Another Reminder It's Time to Close Guantanamo*, HUFFINGTON POST (Jul. 19, 2014, 5:29 PM), http://www.huffingtonpost.com/daphne-eviatar/another-terrorism-convict_b_5353801.html (questioning the claim that detainees "have committed crimes yet cannot be prosecuted").

150 *See* Devin Dwyer, *Force-Feeding at Gitmo: Obama's 'Torture' Debate*, ABC NEWS (Dec. 11, 2014, 12:09 PM), http://abcnews.go.com/Politics/force-feeding-gitmo-obamas-torture-debate/story?id=27531783 (reporting on allegations of force-feeding used on some detainees).

151 NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., 9/11 COMMISSION

procedures meant to ensure compliance with the "primary purpose" doctrine had resulted in a "wall" between law enforcement and intelligence officers that prevented communication of important information.[152] It was postulated that, had the "wall" not inhibited communication about relevant antiterrorism efforts, there would have been several opportunities to learn of the hijackers' plans.[153] The Patriot Act amendment to FISA sought to fix the problem by changing the "primary purpose" requirement to a "significant purpose" requirement.[154]

II. ANALYSIS

As of now, Congress has not passed a comprehensive statutory framework regulating the use of foreign intelligence information in criminal investigations. What limitations do exist are restricted in application and have several ambiguities that make it unclear what exactly is allowed, and under what circumstances. The lack of clear legislation leaves the IC in a "zone of twilight" when attempting to determine whether information can be shared with law enforcement. History has shown that such uncertainty may be improperly utilized in the event of some future emergency, or alternately could prevent important communication from taking place that otherwise should have. Thus, this article recommends that Congress adopt a tripartite framework applicable to information gathered under any foreign intelligence authority.

A. Current Statutory Authorizations do not Adequately Address the Potential Use of Foreign Intelligence Information in Criminal Investigations

Although the United States intelligence community utilizes a wide variety of investigative methods supporting the HUMINT, SIGINT, GEOINT, and MASINT initiatives, statutory use restrictions are fairly limited.[155] The National Security Act allows the IC to collect information for law enforcement agencies upon

---

REPORT, xv (2004), https://www.gpo.gov/fdsys/pkg/GPO-911REPORT/pdf/GPO-911REPORT.pdf.

[152] Richard Henry Seamon & William Dylan Gardner, *The Patriot Act and the Wall between Foreign Intelligence and Law Enforcement*, 28 HARV. J. L. & PUB. POL'Y 319, 373–75 (2005).

[153] *See id.* at 375 (summarizing several "missed opportunities" detailed in the 9/11 COMMISSION REPORT).

[154] *Id.* at 378.

[155] *See* DYCUS, *supra* note 30, at 130–31 (discussing intelligence investigation methods); *supra* Part II.A.3 (describing FISA and the National Security Act).

request, so long as the information is obtained outside of the United States and is in relation to a non-U.S. person.[156] However, it provides no direct language governing the use of foreign intelligence information by law enforcement.

FISA provides a more extensive framework for making decisions, but only in relation to electronic surveillance or physical searches conducted under FISA. It allows retention and dissemination of any foreign intelligence information suggesting a crime was committed if the person implicated was non-U.S. person.[157] For United States persons, dissemination of some kinds of information is limited to situations where either a court order is obtained or the Attorney General determines that the information suggests there is a threat of death or serious bodily harm.[158]

The framework regulating dissemination is far from comprehensive, yet even those provisions that do exist have ambiguities that leave open the potential for unconstitutional use of the information. The term "dissemination" is not further defined in the statute. As it is used, it could be understood to allow for the information to be shared with anyone from the President, other intelligence agencies, or local law enforcement.[159] But dissemination in the form of the President's Daily Brief, or other disseminations to the President, should not be subject to the same level of required procedures as would apply for use in a criminal investigation.[160] True, FISA requires that information collected under its authorities can only be used in a criminal prosecution after receiving prior approval from the Attorney General.[161] But

---

156 50 U.S.C. § 3039(a) (2012).

157 50 U.S.C. § 1801(h)(3) (2012) (electronic surveillance); *Id.* § 1821(4)(C) (physical searches). Note that the type of crime implicated is not a factor in allowing the retention and dissemination. *Id.*

158 50 U.S.C. § 1801(h)(4) (2012) (limiting dissemination of the content of communications gathered via electronic surveillance); *Id.* § 1821(4)(D) (limiting the dissemination of "information, material, or property" obtained through physical searches).

159 *Id.* § 1801 (h)(1) (requiring minimization procedures that are "reasonably designed in light of the purpose" of the surveillance and "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence"). As described, *supra* Part II.A.1, one legitimate use of foreign intelligence information is to stop the detrimental activity, such as espionage or terrorism, through criminal prosecution.

160 *See* WALSH, *supra* note 20 (listing the President's Daily Brief as one standard method of providing analyzed foreign intelligence information to policymakers in response to stated policy concerns).

161 *E.g.*, 50 U.S.C. § 1806(b) (2012). *But see id.* § 1861(h) (not requiring prior approval of the Attorney General for use in a criminal prosecution of business

information can be used in a criminal investigation without necessarily being used in the eventual prosecutorial proceedings. Thus, FISA leaves virtually unfettered the use of information suggesting a criminal act has or will occur if it is related to a non-U.S. person.[162] Likewise, information related to a United States person that is neither the content of an electronic communication or the fruits of a physical search is largely unconstrained.[163]

Additionally, though there are many different methods used to collect foreign intelligence information, FISA primarily regulates SIGINT activities, with a limited number of other activities being regulated in specific circumstances.[164] Thus, many intelligence activities, such as GEOINT or HUMINT conducted outside of the United States, are left unregulated by statute.

Executive-based restrictions do exist, but do not adequately address dissemination procedures. EO 12,333 provides some guidance for collection and dissemination of information gathered through methods of foreign intelligence collection not otherwise regulated by statute.[165] But, it too allows for retention and dissemination of information that could indicate a crime was committed, without providing further description of when, how, or to whom that dissemination can occur.[166] Even if the Order did provide more detailed instructions for use of foreign intelligence information in criminal investigations, it would not be sufficient to clear the ambiguity of existing legislation because the President defines its terms. EO 12,333 was promulgated by the President and can be changed at any time by issuance of another Executive

---

records gathered under FISA).

[162] PPD-28 does provide that the same dissemination procedures must be utilized for non-U.S. persons. Presidential Policy Directive 28 § 4(a)(i) (Jan. 17, 2014), http://www.whitehouse.gov/ the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities. However, that requirement was promulgated by a President and can thus ben changed by a future President at any time. *See infra* note 165 and accompanying text (arguing that limitations put in place through Executive actions are insufficient because they can be changed at any time by the President).

[163] *See supra* note 159 and accompanying text (describing the circumstances where required minimization procedures do not allow for retention or dissemination).

[164] *Supra* part I.A.2.

[165] *See* Exec. Order No. 12,333 § 2.3, *reprinted as amended in* 50 U.S.C. § 3001 (2012) (requiring dissemination procedures to be created by the head of an IC element for information pertaining to U.S. persons and listing types of information that can be retained and disseminated).

[166] *Id.* at § 2.3 (i).

Order, without any requirement for input from Congress.[167]

A. Congress Should Legislate to Occupy the Field Because It Would Both Act as a Check on Executive Discretion and Encourage Sharing in Appropriate Circumstances

Under *Youngstown*, consideration for whether Congressional authorization exists for a given action by the Executive branch is integral to determining whether that action was Constitutional.[168] Currently, use of foreign intelligence information in criminal investigations would fall under Jackson's second category because Congress has not provided direct approval or denial.[169] Even for information gathered under FISA authorities, the ambiguity of the statutory language and the ability for the Executive branch to define the contours of the utilized minimization procedures makes it unclear what exactly Congress has authorized regarding the use of information after collection.[170] Thus, as the situation currently exists, the Executive branch is left in a "zone of twilight," required to use its best guess as to when foreign intelligence information

---

[167] *See FAQ's About Executive Orders*, NATIONAL ARCHIVES, http://www.archives.gov/federal-register/executive-orders/about.html#orders (explaining that executive orders are the method by which the President "manages the operations of the Federal Government"). This concern is not merely theoretical. Just days before the inauguration of President Donald Trump, President Obama disseminated a new procedure for implementing EO 12333 that allowed the NSA to "disseminate 'raw signals intelligence information.'" Jane Chong, *Obama Administration Releases Long Awaited New E.O. 12333 Rules on Sharing of Raw Signals Intelligence Information Within IC*, LAWFARE (Jan. 12, 2017, 12:38 PM), https://www.lawfareblog.com/obama-administration-releases-long-awaited-new-eo-12333-rules-sharing-raw-signals-intelligence. Since being sworn in, President Trump has not shied away from issuing and modifying executive orders either. *See* Rebecca Harrington, *Trump has already signed 66 executive actions — here's what each one does*, BUSINESS INSIDER (Apr. 19, 2017, 10:10 AM), http://www.businessinsider.com/trump-executive-orders-memorandum-proclamations-presidential-action-guide-2017-1 (detailing the executive actions taken by President Trump in his first few months in office).

[168] Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 636–37 (1952) (Jackson, J., concurring) (describing the three categories under which a President's action could fall in relation to Congressional authorization and the President's authority under each category).

[169] *See id.* at 637 (describing the second category as a "zone of twilight" in which distribution of authority between Congress and the President is unclear). *See also supra* Part III.A (discussing the limited and generally ambiguous statutory authorities controlling the use of foreign intelligence information).

[170] *See, e.g.*, 50 U.S.C. § 1804 (a)(4) (2012) (requiring an application to conduct electronic surveillance to include the proposed minimization procedures); 50 U.S.C. § 1801 (h)(1) (providing guidelines for minimization procedures but leaving the specific details to be adopted by the Attorney General).

can constitutionally be used in criminal investigations based only on the President's constitutional powers.[171]

Providing a statutory framework that fully defines under what circumstances any foreign intelligence information can be used in a criminal investigation would place Executive branch action squarely within categories one and three of the *Youngstown* analysis. When a statute authorized an action, the Executive branch would be acting under the President's maximum authority and "would be supported by the strongest of presumptions and the widest latitude of judicial interpretation."[172] Thus, if a criminal investigation utilizing foreign intelligence information ultimately resulted in a prosecution, there would be fewer legitimate challenges to the constitutionality of that information's use.[173]

If the executive branch chose to use information in a criminal investigation despite a statutory prohibition, the authority under which it acted would be at "its lowest ebb."[174] Since the Supreme Court has said that Congress should legislate procedures for conducting surveillance in the national security context,[175] the Executive branch's action would almost always be overturned upon judicial review.[176] The framework, therefore, would enable Congress to guide the Executive branch by encouraging the use of criminal proceedings in appropriate cases, and discouraging the

---

171 *Youngstown*, 343 U.S. at 637.

172 *See id.* at 637 (indicating a wide "latitude of judicial interpretation" in favor of Executive action is appropriate where "the President acts pursuant to an express or implied authorization of Congress," and that there would be a heavy "burden of persuasion" for anybody challenging the action).

173 The defendant could still, of course, challenge the constitutionality of the initial collection. As noted above, the government is required to inform a criminal defendant if evidence gathered under FISA is used against him. *See supra* note 53 and accompanying text (explaining that the Attorney General must approve use of FISA information in a criminal proceeding, likely because defendants must be notified of its use).

174 *Youngstown*, 343 U.S. at 637 (describing the President's authority as consisting of "his own constitutional powers minus any constitutional powers of Congress over the matter").

175 United States v. U.S. District Court (*Keith*), 407 U.S. 297, 321–23 (1972). Although *Keith* was decided in the context of domestic national security investigations, cases addressing the constitutionality of certain provisions of FISA assume that Congress can also legislate procedures in the foreign intelligence context. *See, e.g.*, *In re* Sealed Case No. 02-001, 310 F.3d 717, 746 (FISA Ct. Rev. 2002) (upholding a statutory provision regulating when a foreign intelligence authority could be used to collect foreign intelligence information).

176 *See Youngstown*, 343 U.S. at 640 (concluding that when a President's action falls under the third category, it can only be sustained if Congress did not have the constitutional authority to regulate the conduct in question).

sharing of information where it would be unconstitutional or otherwise inappropriate.[177]

In the fight against terrorism, there are several extrajudicial uses for foreign intelligence that have received considerable criticism. Although using drones to conduct reconnaissance missions has the potential to save pilots' lives, drone strikes' validity under international law has been challenged due to a lack of accountability, and also on due process grounds.[178] The use of military detention procedures has also proved problematic for the government. Both indefinite detention of terrorists and the use of military courts to try suspects have been the subject of legal debate.[179] As compared to these other, controversial methods of addressing terrorism threats, criminal prosecution in the civilian courts may sometimes be preferable.[180]

Conversely, by providing an explicit framework within foreign intelligence information could be used in criminal investigations, Congress would discourage the Executive branch from utilizing ambiguity in the current statutory framework to push the boundaries of the constitution. In the 1970's, a Congressional investigation infamously found that the IC had systematically acted unconstitutionally in terms of both its methods and targets of investigation.[181] Though some activities were done in contravention of existing law, the Committee found it a contributing factor that there was an "absence of laws and lack of clarity in those that [do] exist."[182] More recently, a willingness to

---

[177] That Congressional prohibition should discourage certain Executive actions is logical—if the action would not be upheld in court, then there is little incentive to act in the first place. What is less certain is to what extent a grant of approval would encourage action in appropriate circumstances. Because secrecy is a key aspect of foreign intelligence collection, LOWENTHAL, *supra* note 7, a decision to pursue criminal charges will always require careful consideration. Removing the risk of having use of the information overturned at trial, however, at least addresses one element that discourages the use of civilian courts.

[178] Pilkington, *supra* note 147 (noting concern over the ability to hold countries responsible when drones are used in secret and the lack of consensus over when lethal force is justified).

[179] *See supra* notes 149–51 and accompanying text (describing criticisms of indefinite detention, military trials, and allegations that detainees have been tortured).

[180] Kris, *supra* note 26, at 74 (providing a terrorist who is a U.S. citizen and located in the United States as an example of when criminal prosecutions are the most constitutionally feasible option).

[181] *See supra* notes 138–41 and accompanying text (summarizing the Church Committee report findings detailing unconstitutional conduct by the IC during the Cold War).

[182] S. REP. NO. 94-755, Book II, IX-X (1976). The Committee's

act without Congressional authorization was demonstrated through the Terrorist Surveillance Program, in response to the 9/11 attacks.[183] In the current international climate, it is not hard to imagine that a future national security emergency could prompt the Executive branch to use any statutory ambiguity available to further its goal of protecting the country. While the goal may be honorable, past examples suggest that the ends will not always justify the means.

B. The Fourth Amendment Reasonableness Requirement Allows Use of Foreign Intelligence Information in Three Types of Criminal Investigations

The Supreme Court has, at a minimum, provided that Congress can legislate less protective procedures for surveillance conducted for national security investigations than are required for ordinary criminal investigations under Title III.[184] Although the Court required a reasonable substitution for the warrant requirement to include prior judicial review for domestic national security cases, it suggested without deciding that such a requirement for judicial review would not be necessary in foreign intelligence investigations.[185] Since then, a number of circuit courts have held that a foreign intelligence exception to the warrant requirement does exist, and that foreign intelligence surveillance must meet only the reasonableness requirement of the Fourth Amendment.[186]

---

recommendation to enact oversight legislation to prevent future violations was fulfilled with FISA's enactment in 1978. *See id.* (recommending that Congress "devise the legal framework within which intelligence agencies can, in the future, be guided [and] checked[.]"); Beryl A. Howell & Dana J. Lesemann, *FISA's Fruits in Criminal Cases: An Opportunity for Improved Accountability*, 12 UCLA J. INT'L L. & FOREIGN AFF. 145, 149 (2007) (recognizing that FISA was passed in response to the Church Committee findings).

183 *See supra* notes 142–44 and accompanying text (explaining that the NSA instituted a program to allow collection where communications took place between individuals with one party in the United States and another located abroad, which was not accounted for in FISA).

184 United States v. U.S. District Court (*Keith*), 407 U.S. 297, 322 (1972).

185 *Id.* at 321–22.

186 *See In re* Directives, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008) (holding that the foreign intelligence exception exists "when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States"); United States v. Truong, 629 F.2d 908, 916 (4th Cir. 1980) (upholding the validity of foreign intelligence surveillance conducted pursuant to approval by the Attorney General under a foreign intelligence exception); United States v. Butenko, 494 F.2d 593, 605 (3d Cir. 1974) (holding that the warrant

Because foreign intelligence authorizations do not comply with the traditional criminal procedures required under Title III,[187] a reasonableness analysis should look at restrictions placed on collection and use of the information.[188] This article assumes that the relevant foreign intelligence information was constitutionally acquired, and looks instead to determine how that information can be used after collection. Foreign intelligence information can be immediately separated into two categories: (1) information relevant to foreign intelligence crimes, and (2) information incidentally collected but relevant to crimes other than foreign intelligence crimes.

For constitutional purposes, the requirements for allowing use of information in these two categories should differ. In *In re Sealed Case*, the FISA Court of Review acknowledged that foreign intelligence information would often inherently constitute evidence of a foreign intelligence crime.[189] It also acknowledged that although information could not be collected for the purpose of investigating ordinary crimes, under the terms of the statute, incidental collection of information related to ordinary crimes need not be destroyed.[190] Though the opinion impliedly upheld the validity of the provision allowing retention of incidentally collected information, recall that FISA's electronic surveillance minimization procedures impose restrictions on dissemination of that information as it relates to United States persons.[191] Additionally, the FISA Court of Review has stated that the reasonableness of procedures should be determined by using a totality of the circumstances test.[192] Thus, the reasonableness of

---

requirement does not apply to surveillance conducted solely to collect foreign intelligence information).

[187] *See, e.g.*, *In re* Application of the FBI, No. BR-13-109, 2013 WL 5741573, at *4–5 (FISA Ct. Aug. 29, 2013) (comparing and contrasting the Section 215 procedures with 18 U.S.C. § 2703(d), which authorizes collection of similar information in ordinary criminal investigations).

[188] *In re Directives*, 551 F.3d at 1013 (noting both targeting and minimization procedures as important to its totality of the circumstances test when determining that collection was reasonable under the Fourth Amendment).

[189] *In re* Sealed Case No. 02-001, 310 F.3d 717, 724 (FISA Ct. Rev. 2002) (accepting under its constitutional analysis that use foreign intelligence information as evidence of a crime is reasonable because the information "can include evidence of certain crimes relating to sabotage, international terrorism, or clandestine intelligence activities").

[190] *Id.* at 731.

[191] *See supra* notes 54–56 and accompanying text (discussing FISA minimization procedures).

[192] *In re Directives*, 551 F.3d at 1012 (explaining that the totality of the

using incidentally collected information will vary based on the level of government interest in the type of crime. The totality of the circumstances test allows for greater governmental intrusion based on the level of government interest,[193] and there are two logical categories of crimes for which its use is reasonably justified—domestic national security crimes,[194] and ordinary crimes causing loss of life or serious bodily harm.[195]

There is some foreign intelligence information that could be of use in criminal investigations, but would not ordinarily be subject to the Fourth Amendment—for instance if it was collected outside of the United States in relation to a non-U.S. person.[196] One could argue that adopting a framework applicable to information not subject to Fourth Amendment protections would be incompatible with separation of powers principles. However, the Court acknowledged in *Verdugo-Urquidez* that Congress could place restrictions on searches of non-U.S. persons conducted outside of the United States.[197] Thus, although it is not a Constitutional requirement, Congress would be within its authority to impose restrictions for policy reasons, such as to promote consistency and

---

circumstances analysis "takes into account the nature of the government intrusion and how the intrusion is implemented").

193 *Id.*

> If the protections that are in place for individual privacy interests are sufficient in light of the governmental interest at stake, the constitutional scales will tilt in favor of upholding the government's actions. If, however, those protections are insufficient to alleviate the risks of government error and abuse, the scales will tip toward a finding of unconstitutionality.

Id.

194 *See* United States v. U.S. District Court (*Keith*), 407 U.S. 297, 313, 322 (1972) (recognizing that the Executive has a stronger "investigative duty" for domestic national security investigations and that the goal may be to prevent a crisis or emergency).

195 Recognition of the government's interest in investigation or preventing crimes related to death or serious bodily harm is already recognized in FISA. *See* 50 U.S.C. § 1801(h)(4) (2012) (providing for dissemination of the contents of intercepted communications involving U.S. persons only if it relates to the potential death or serious bodily harm). This standard is used elsewhere in federal law as a justification for authorizing a variance from ordinary procedures. *E.g.*, 42 U.S.C. § 290dd-2(b)(2)(C) (2012) (permitting disclosure of otherwise confidential medical information upon a showing that it is needed "to avert a substantial risk of death or serious bodily harm").

196 *See* United States v. Verdugo-Urquidez, 494 U.S. 259 (1990) (holding that the Fourth Amendment does not apply to non-U.S. persons located outside of the United States).

197 *See id.* at 275 (providing that the political branches could enact restrictions not required by the Constitution).

transparency.

III. RECOMMENDATIONS

The Fourth Amendment reasonableness requirement would be satisfied by a tripartite framework, providing progressively more stringent requirements for sharing related to (1) foreign intelligence crimes, (2) domestic national security crimes, and (3) a limited number of serious ordinary crimes. Although it could be argued that instituting restrictions on the use of foreign intelligence information would resurrect the negative consequences associated with "the wall," this framework is different both because it does not restrict collection by imposing a standard on the purpose of collection, and because it allows for information related to foreign intelligence crimes to be freely shared between the IC and law enforcement.[198]

A. Congress Should Enact a Tripartite Framework Regulating the Use of Any Foreign Intelligence Information in Criminal Investigations

1. Evidence of Foreign Intelligence Crimes Should Be Shared with Law Enforcement Subject to Internal Executive Branch Procedural Requirements

Under a totality of the circumstances test, foreign intelligence information should be allowed in a criminal investigation for foreign intelligence crimes without any additional required approval.[199] First, foreign intelligence crimes are of great

---

[198] *See supra* Part I(C)(4) (describing how the primary purpose doctrine limited communication between the intelligence community and law enforcement, thus contributing to the intelligence failures resulting in the 9/11 attacks).

[199] Based on definitions of foreign intelligence in FISA and the National Security Act, foreign intelligence crimes would include: treason, terrorism, proliferation of weapons of mass destruction, espionage, sabotage, narcotics trafficking, assassination, or organized crime. *See* 18 U.S.C. § 2381 (2012) (defining treason as levying war against the United States or giving aid to its enemies); 50 U.S.C. §§ 1801(b)–(e) (2012) (describing activities of interest for foreign intelligence investigations); 50 U.S.C. § 3003(3) (2012) (describing counterintelligence activities, including espionage and sabotage); 50 U.S.C. § 3021(i)(5) (2012) (defining "transnational threats" to the national security, including narcotics trafficking and proliferation of weapons of mass destruction). Although treason is not listed in the National Security Act or FISA, it is commonly accepted as a national security crime and it has elements requiring foreign

government interest to resolve because of the risk they present to the national security.[200] Second, the level of added government intrusion is minimal because foreign intelligence investigations will inherently reveal information relevant to foreign intelligence crimes.[201] Congress should therefore enact a law allowing the government to utilize foreign intelligence information in criminal investigations of foreign intelligence crimes, subject to internal agency procedures.[202]

2. Evidence of Domestic National Security Crimes Should be Shared with Law Enforcement Only Upon Approval of the President or Attorney General

Information related to domestic national security crimes can only constitutionally be acquired based on foreign intelligence authorizations if the information was incidentally collected—i.e., if the investigation was being conducted in relation to a foreign power or agent of a foreign power,[203] but information happened to surface related to a wholly domestic national security crime.[204]

---

involvement. Erin Creegan, *National Security Crime*, 3 HARV. NAT'L SEC. J. 373, 373 (2012) (listing treason with espionage, sabotage, and terrorism).

200 *See In re* Directives, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008) (recognizing the government interest in utilizing foreign intelligence investigations to protect the national security as being "of the highest order of magnitude"). *See also* Haig v. Agee, 453 U.S. 280, 307 (1981) ("It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation." (quoting Aptheker v. Sec'y of State, 378 U.S. 500, 509 (1964))).

201 *See In re* Sealed Case No. 02-001, 310 F.3d 717, 726 (FISA Ct. Rev. 2002) ("'International terrorism,' by definition, requires the investigation of activities that constitute crimes. That the government may later choose to prosecute is irrelevant." (citing United States v. Sarkissian, 841 F.2d 959, 964 (9th Cir. 1988))). *See also* United States v. Truong, 629 F.2d 908, 915 (4th Cir. 1980) (recognizing that foreign intelligence investigations could not be required to be conducted "solely" for foreign policy reasons because "almost all foreign intelligence investigations are in part criminal investigations").

202 This requirement essentially mimics requirements provided for by EO 12, 333. Exec. Order 12, 333 § 2.3, reprinted as amended in 50 U.S.C. § 3001 (2012).

> Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General . . . after consultation with the Director.

Id.

203 *See supra* notes 13–16 and accompanying text (defining foreign intelligence under the National Security Act and FISA).

204 National security crimes would include any fully domestic versions of the

Because the Court has recognized that national security investigations allow for different procedures than required for normal crimes due to their sensitive nature, the government's interest is heightened above that of ordinary crime.[205] However, because the government interest in investigating a national security crime represents a different interest than that which initially justified the search (a foreign intelligence interest), due consideration should be given to whether its use is appropriate.[206] This is especially true because the potential for government intrusion into individual privacy interests is heightened in domestic national security cases.[207] Accordingly, some additional level of approval should be required outside of the intelligence agency prior to its use in a criminal investigation. Cases have accepted that review by the President or Attorney General is a sufficient compromise between the investigatory needs of sensitive cases and the need to check agent discretion where the national security is implicated.[208] Congress should therefore enact a law requiring the approval of the President or Attorney General prior to use of foreign intelligence information in a criminal investigation for domestic national security crimes.

3. Evidence of Normal Crimes Should be Shared with Law Enforcement Only for a Small Subset of Crimes and Only Upon Judicial Authorization

Incidental collection of information related to ordinary crimes is constitutionally permissible under otherwise constitutional

---

foreign intelligence crimes listed *supra* note 199.

[205] *See* United States v. U.S. District Court (*Keith*), 407 U.S. 297, 313, 322 (1972) (accepting that the government has a stronger investigative duty in national security cases).

[206] In essence, the interest of the government in using the foreign intelligence information should be tempered for purposes of the balancing test in order to help protect against foreign intelligence authorities being used as an "end run" around traditional requirements. *See* Hall, *supra* note 26, at 101–03 (explaining the concern that prosecutors might inappropriately use foreign intelligence authorities if it is too easy to do so).

[207] *See Keith*, 407 U.S. at 313 (noting that there is often a "convergence of First and Fourth Amendment values" in national security cases).

[208] *See In re* Sealed Case No. 02-001, 310 F.3d 717, 739 (FISA Ct. Rev. 2002) (recognizing as constitutionally significant the approval of certifications by the Attorney General for applications under FISA). *See also* United States v. Ehrlichman, 546 F.2d 910, 926 (D.C. Cir. 1976) (holding that involvement of the Attorney General prior to surveillance in domestic national security cases helped affix accountability and was thus integral for Fourth Amendment purposes).

foreign intelligence surveillance authorizations.[209] Additionally, government interest in utilizing the foreign intelligence information is somewhat heighted in relation to attempts to prevent and investigate death and serious bodily harm.[210] However, the weight given to the government interest should be tempered for purposes of the balancing test because the government's initial interest in gathering foreign intelligence information is significantly removed from its interest in using the information to prosecute an ordinary crime.[211]

Utilizing procedures mimicking those required under Title III for ordinary criminal surveillance can help to ensure the Fourth Amendment reasonableness requirement is met by balancing the government and public interests.[212] Because prior judicial review is recognized as a fundamental aspect of Fourth Amendment reasonableness for ordinary crimes, prior judicial review should be required to use foreign intelligence information in an applicable criminal investigation.[213] Congress should therefore enact a law limiting the use of foreign intelligence information for ordinary crimes to only crimes involving death or serious bodily harm, and only after prior judicial review determining that the foreign intelligence information establishes probable cause that a crime has been committed.[214]

---

[209] *See In re Sealed Case No. 02-001*, 310 F.3d at 731 (recognizing that statutory minimization requirements later found to support the constitutionality of a FISA amendment allowed for retention of incidentally collected evidence of crime).

[210] *See supra* note 195 (providing existing examples of the threat of death or serious bodily harm receiving exceptions to statutory requirements).

[211] *See supra* note 206 and accompanying text (explaining why a difference in government interest is significant).

[212] *Cf. In re Sealed Case No. 02-001*, 310 F.3d at 737 ("[I]n asking whether FISA procedures can be regarded as reasonable under the Fourth Amendment, we think it is instructive to compare those procedures and requirements with their Title III counterparts. Obviously, the closer those FISA procedures are to Title III procedures, the lesser are our constitutional concerns.").

[213] United States v. U.S. District Court (*Keith*), 407 U.S. 297, 323 (1972) (allowing procedures different from those under Title III for national security investigations, but requiring an element of prior judicial review to satisfy the warrant requirement and, by extension, the reasonableness requirement). Note that judicial review would be required for dissemination to law enforcement. Collection authorities would remain the same.

[214] The law should clarify, however, that information related to ordinary crimes may be used in criminal investigations if the information obtained under foreign intelligence authorities also provides evidence of a foreign intelligence or domestic national security crime. *See In re Sealed Case No. 02-001*, 310 F.3d at 736.

> That is not to deny that ordinary crimes might be inextricably

CONCLUSION

Foreign intelligence information can be gathered through several different methods, some of which have extensive statutory procedural requirements, but many of which do not. Additionally, foreign intelligence information is utilized for a wide variety of purposes, including informing decisions by policy makers, influencing military tactics, and use in criminal investigations. Congress, however, has not clearly defined under which circumstances information gathered under each type of foreign intelligence collection method can be utilized in criminal investigations. In order to prevent the potential for the Executive branch to push the boundaries of constitutionality in the future, and to encourage the use of foreign intelligence information in criminal investigations when appropriate, Congress should enact a framework governing the use of foreign intelligence information obtained under all foreign intelligence authorities.

Under Fourth Amendment jurisprudence, foreign intelligence surveillance does not have to meet traditional warrant requirements, but it does still have to meet the reasonableness requirement. Reasonableness in the context of foreign intelligence tends to look at restraints placed on the collection and use of information. For the purposes of this article, it is assumed that the collection of any relevant foreign intelligence information was both legal and constitutional. The question, therefore, is whether and when foreign intelligence information can be constitutionally utilized in criminal investigations. The answer must be determined by applying a totality of the circumstances test, which balances the weight of the government interest against the weight of public privacy interests.

Under the totality of the circumstances test, Congress' framework should delineate three categories of crimes for which foreign intelligence information can be used. First, the use of foreign intelligence information should be allowed in investigations of foreign intelligence crimes without any additional

---

> intertwined with foreign intelligence crimes. For example, if a group of international terrorists were to engage in bank robberies in order to finance the manufacture of a bomb, evidence of the bank robbery should be treated just as evidence of the terrorist act itself.

Id.

Congressional requirements. Second, the use of foreign intelligence information should be allowed in investigations of wholly domestic national security crimes only upon the approval of the President or Attorney General. Finally, the use of foreign intelligence information should be allowed in investigation of ordinary crimes only if the information indicates a substantial risk of death or serious bodily harm, and only after judicial review to determine that the foreign intelligence information establishes probable cause that a crime has been committed.

How would this framework apply to the hypothetical posed in the introduction of this article? Because the crime to be investigated, international narcotics trafficking, would constitute a foreign intelligence crime, it would fall under the first category within the framework. The information gained was directly relevant to the legally conducted foreign intelligence investigation, and its applicability as evidence of a crime is directly related to the purpose of the investigation. The government could therefore choose to use the information in a criminal investigation of the narcotics operation, subject to its own internal procedures.