NOTE

THINKING INTELLIGENTLY ABOUT INTELLIGENCE:
A MODEL GLOBAL FRAMEWORK
PROTECTING PRIVACY

Chantal Khalil*

I. INTRODUCTION

According to confidential government documents leaked by for-
mer-National Security Agency Contractor Edward Snowden, the
United States' National Security Agency (NSA) has been monitor-
ing the electronic communications of at least tens of millions of
individuals abroad, as well as the private communications of thirty-
five world leaders, since as early as 2002.1

In a speech before the United Nations, Brazil’s President Rous-
seff reprimanded the NSA’s clandestine actions as “a breach of
international law,” an affront of the basic principles that guide rela-
tions among friendly, sovereign nations, and a violation of “fundamental
human rights of citizens of another country.”2 In the same
vein, Brazilian Justice Minister Jose Eduardo Cardozo referred to
the surveillance as “an attack on our country’s sovereignty.”3

Snowden’s initial revelations regarding the NSA’s intelligence
collection practices documented the agency’s practice of spying on
embassies, European Union offices, and diplomatic missions within
the United Nations in its New York headquarters and in remote
offices.4 Months later it was revealed that the NSA had collected

1. James Bell, NSA Monitored Calls of 35 World Leaders After US Official Handed Over
Contacts, GUARDIAN (Oct. 25, 2013, 2:50 PM), http://www.theguardian.com/world/2013/
Oct/24/nsa-surveillance-world-leaders-calls; Kevin Rawlinson, NSA Surveillance: Merkel's
Phone May Have Been Monitored For Over 10 Years; GUARDIAN (Oct 26, 2013, 3:20 PM),
http://www.theguardian.com/world/2013/oct/26/nsa-surveillance-brazil-germany-un-
resolution.
2. Julian Borger, Brazilian President: US Surveillance a Breach of International Law,
GUARDIAN (Sept. 24, 2013, 12:27 PM), http://www.theguardian.com/world/2013/sep/24/
brazil-president-un-speech-nsa-surveillance.
3. NSA ‘Spied on Brazil and Mexico’—Brazilian TV Report, BBC NEWS (Sept. 2, 2013),
4. Laura Poitras et al., How the NSA Targets Germany and Europe, SPIEGEL ONLINE (July
1, 2013, 11:11 AM), http://www.spiegel.de/international/world/secret-documents-nsa-tar-
geted-germany-and-eu-buildings-a908609.html.
approximately seventy million recordings of private French phone conversations and messages, over sixty million recordings of private Spanish phone conversations over the course of a month,\(^5\) intercepted Brazilian President Rousseff and German Chancellor Merkel’s phone calls,\(^6\) and hacked into the Mexican President Nieto’s email account.\(^7\) According to a document consulted by *Le Monde*, the NSA collected 124.8 billion pieces of telephone data and 97.1 billion pieces of digital data worldwide between February 8 and March 8, 2013.\(^8\) In addition, a European Parliament Committee draft report on the NSA’s surveillance states that it has “compelling evidence” that the communication and location data and metadata are not only being collected on an “unprecedented scale,” but that the collection is “indiscriminate and non-suspicion-based.”\(^9\)

Amid outrage over the United States’ expansive international surveillance program, German Chancellor Merkel and Brazilian President Rousseff, with the support of many other foreign leaders, demanded that the General Assembly adopt a resolution to end excessive spying and invasions of privacy.\(^10\) On November 2, 2013, the two nations presented a draft resolution that, in part, calls on member states to “take measures to put an end to violations of these rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies


\(^8\) Follorou & Greenwald, *supra* note 5.


with their obligations under international human rights law.” In an interesting twist of events, two days later, newspaper Folha de São Paulo revealed a report, which was subsequently confirmed by Brazil’s government, describing how Brazil’s intelligence agency, Abin, has spied on diplomats from countries including the United States, Iran, and Russia.

The issue of international law and extraterritorial intelligence collection undoubtedly impacts all nations, and thus extends beyond the current outcry over Snowden’s declassifications. While there may not be similar leaks detailing the intelligence activities of all other countries, it would be naïve to think that other nations are not engaged in similar espionage practices, though it would seem that the United States’ capacity to collect data may be unparalleled. Former French Foreign Minister Bernard Kouchner openly admitted on French radio that he was shocked by the magnitude of the eavesdropping, and went on to say: “Let’s be honest, we eavesdrop too. Everyone is listening to everyone else,” the difference is that “we don’t have the same means as the United States—which makes us jealous.”

Despite the prevalence of peacetime espionage, and the fact that intelligence practices are essentially accepted as inherent operations of the modern state, the law pertaining to peacetime espionage is virtually unstated. While individual states may attempt to regulate internal intelligence activities through legislation, there are no significant international treaties or conventions in existence.

11. NSA Spying: Germany and Brazil Produce Draft UN Resolution, GUARDIAN (Nov. 2, 2013), http://www.theguardian.com/world/2013/nov/02/nsa-germany-brazil-un-resolution.


13. See Nick Hopkins & Matthew Taylor, Trade in Spy Systems Must Be Reviewed, Says Committee Chair, GUARDIAN (Nov. 19, 2013, 2:25 PM), http://www.theguardian.com/world/2013/nov/19/trade-spy-systems-surveillance-john-stanley (describing a database revealing that several private companies are selling newly-developed mass surveillance technologies and software to “democratic and non-democratic countries”).


16. The United States’ Central Intelligence Agency, for example, is prevented from engaging in “internal security functions.” See, e.g., 50 U.S.C. § 403-4a(d)(1) (2012) (“[T]he . . . Agency shall have no police, subpoena, or law enforcement powers or internal security functions . . . .”); see also Exec. Order No. 12,333, 46 Fed. Reg. 59941, 59945 (Dec. 8, 1981) (“[T]he CIA shall . . . [c]onduct counterintelligence activities outside the United States and, without assuming or performing any internal security functions . . . .”).
that establish principles regulating international intelligence activities. Customary international law similarly fails to provide the international community with a set a rules governing espionage on foreign states and individuals. Technological advances of the modern age and the shortcomings of the current international legal framework pertaining to privacy rights between allies during peacetime make it difficult to maintain trust and security in diplomatic relations in the future. As a result, the international community must develop a convention that addresses these inadequacies and regulates intelligence gathering—of both leaders and individuals—between allies during peacetime.

This Note examines the international law pertaining to peacetime espionage among nations and recommends a framework to resolve current international conflicts. Part II defines “espionage” and related terminology. It then discusses the modern methods and dangers of mass surveillance, and assesses the current legal framework surrounding peacetime espionage on allies, focusing on sovereignty rules, human rights principles, and customary international law. Part III applies the framework to the current allegations to assess the legality of modern surveillance practices, and highlights significant issues that cannot be resolved under existing legal norms. Part III recommends developing a clear and comprehensive framework through an international convention that addresses society’s technological advances, and proposes fundamental principles extrapolated from the current framework that should be included in the new convention. The section then poses potential problems with any framework seeking to address spying between allies during peacetime. Part IV addresses the broader implications of the proposed framework and its beneficial impact on the international community.

18. Id.
II. BACKGROUND

A. What Is Spying?

Interestingly, there is no internationally agreed-upon definition for “espionage.” A 2001 European Commission report on foreign intelligence defines espionage as “simply the organised theft of information,” traditionally targeting military and government secrets.20 Black’s Law Dictionary defines espionage as “[t]he activity of using spies to collect information about what another government or company is doing or plans to do.”21 Similarly, the Oxford English Dictionary defines “espionage” as “[t]he practice of playing the spy, or of employing spies,”22 and “to spy” as “[t]o watch (a person, etc.) in a secret or stealthy manner; to keep under observation with hostile intent . . . .”23 However, these broad definitions only capture a particular form of intelligence gathering—that conducted by individuals—and fails to account for modern intelligence gathering, whereby information is collected by technological means.24

Intelligence, or the information collected by espionage, can be divided into two sub-categories: foreign intelligence and counter-intelligence.25 Foreign intelligence is “information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.”26 Counterintelligence is “information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.”27


22. A spy is defined as “a secret agent whose business it is to keep a person, place, etc., under close observation; esp. one employed by a government in order to obtain information relating to the military or naval affairs of other countries, or to collect intelligence of any kind.” OXFORD ENGLISH DICTIONARY (online version Oct. 2014).

23. Id.

24. Id.


26. Id. § 401a(2).

27. Id. § 401a(3).
Intelligence collection is performed by people in the form of human intelligence (HUMINT), by machines as geospatial intelligence (GEOINT), signals intelligence (SIGINT), and measurement and signatures intelligence (MASINT). HUMINT is defined as a “category of intelligence derived from information collected and provided by human sources.” The information is usually collected “from people and their associated documents and media sources to identify elements, intentions, composition, strength, dispositions, tactics, equipment, personnel, and capabilities.” SIGINT, which is mostly at issue in foreign surveillance and intelligence collection, is mainly comprised of communications intelligence (COMINT) and electronics intelligence (ELINT). COMINT consists of “foreign communications passed by radio, wire, or other electromagnetic means” and ELINT is “foreign electromagnetic radiations such as emissions from a radar system.” This Note focuses on the use of SIGINT techniques, as they have become exponentially prevalent and are at the forefront of contemporary surveillance debates.

The NSA and the British Government Communications Headquarters (GCHQ) use a variety of methods, many of which remain unknown, to gather intelligence on individuals throughout the world. For instance, several of the disclosures have revealed confidential programs whereby the NSA demands metadata and content data from telecom providers, has direct access to the servers of

28. See ECHELON Report, supra note 20, § 2.4.
32. See ECHELON Report, supra note 20, § 2 (stating that SIGINT intelligence operations make up a large part of services’ interception capacity).
internet giants such as Google, Facebook, and Apple,\textsuperscript{34} intercepts huge fiber-optic communications cables,\textsuperscript{35} and implants software in devices such as phones and computers either by intercepting packages or remote installation for remote access to the devices’ data.\textsuperscript{36} It has also been revealed that the United Kingdom’s GCHQ spy agency is engaging in practices similar to those of the NSA, at times cooperating with the NSA,\textsuperscript{37} and is itself operating a mass-interception network by tapping fiber-optic cables to secretly gain access to the network of cables which carry the world’s telephone calls and internet traffic.\textsuperscript{38}

**B. Intelligence in a Modern World**

The Internet and technological communications have made remarkable advances over the past decade, such that technology permeates nearly every aspect of most individuals’ lives on a daily basis.\textsuperscript{39} While these advances have the potential to improve the human condition globally, the same technology makes states and individuals increasingly vulnerable to espionage, allegedly for the sake of economic and national security.\textsuperscript{40} Similarly, the global dependency on cyberspace makes it easier for intelligence agencies to shift away from targeted surveillance, and to instead engage in


\textsuperscript{39} OECD Guidelines, supra note 19, at 19–20.

mass surveillance.\textsuperscript{41} The ability to procure information remotely is another significant innovation that distinguishes cyberspace from traditional espionage.\textsuperscript{42} Intelligence agencies, even those without the most robust capabilities, no longer need to be physically located near the source of their desired information; rather, the ubiquity of technology and new methods of interception mean that they could access essentially any information from anywhere in the world.\textsuperscript{43} Individuals using phones, computers, the Internet, and GPS make themselves vulnerable to constant surveillance. It also seems that any attempt to increase the security of one’s personal devices will virtually always be rendered futile as a result of the inconceivable breadth of the resources and abilities available to advanced intelligence agencies.\textsuperscript{44} Technology has enabled states to gather more information on individuals globally than ever imaginable.\textsuperscript{45} Intelligence agencies with the capability of collecting, storing, and analyzing both metadata and content data can quickly build a dossier and know nearly everything about any person, without his knowledge.\textsuperscript{46}

Modern technological developments raise numerous questions about the evolving nature of intelligence collection and its place under the international legal regime. The analysis in the following subsection demonstrates that while the international law currently in force does guarantee individual privacy and state sovereignty—notions at the center of the mass surveillance debate—the laws are insufficient to address modern technological developments and must be reworked to provide adequate protections.

\textsuperscript{41} For purposes of this Note, cyberspace refers to the “global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies.” Daniel T. Kuehl, \textit{From Cyberspace to Cyberpower: Defining the Problem, in Cyberpower and National Security} 24, 26–28 (Franklin D. Kramer et al. eds., 2009).


\textsuperscript{43} ECHELON Report, supra note 20, § 3.3.1 (describing a “worldwide interception system,” wherein certain categories of cable, radio, and satellite communications may be intercepted from anywhere).

\textsuperscript{44} \textit{OECD Guidelines}, supra note 19, at 20.

\textsuperscript{45} Id. at 20.

\textsuperscript{46} Id.
C. Espionage in the Context of International Law

While many individual countries implement statutes to regulate domestic intelligence operations and to guarantee the rights of their own citizens, with the exception of a few classified agreements involving intelligence sharing among allies, there are no significant international treaties or conventions that specifically govern international intelligence activities. Furthermore, customary international law also fails to provide a clear, internationally recognized set of standards pertaining to espionage. Consequently, in order to address the legality of modern espionage practices, a survey of international law norms relating to state sovereignty and privacy as a human right must be conducted.

1. Traditional International Law

Eminent international law scholar Richard Falk’s depiction of traditional international law as “remarkably oblivious to the peacetime practice of espionage” remains accurate to this day. The prominent treatises either completely overlook espionage, or only briefly define a spy and describe “his hapless fate in the event of capture.” For example, while the Hague Convention of 1907 permits espionage as a ruse of war, it states that spies captured during an armed conflict are not entitled to prisoner of war status, and are

47. Radsan, supra note 17, at 597; Simon Chesterman, The Spy Who Came in from the Cold War: Intelligence and International Law, 27 Mich. J. Int’l L. 1071, 1072 & n.4 (2006) (noting that, aside from a handful of classified agreements involving intelligence sharing among allies, and despite its importance to the conduct of international relations, there are few, if any treaties that deal with espionage directly).
48. Radsan, supra note 17, at 597.
49. The increasing use of signals intelligence by state intelligence agencies, which is generally conducted remotely, constrains the ability of domestic laws and law enforcement to deter espionage since there are territorial limits on a state’s ability to exercise police power. See Williams, supra note 42, at 1183.
50. Richard A. Falk, Foreword to Essays on Espionage and International Law, v (Roland J. Stanger ed., 1962). As Professor Radsan has noted, “[t]hose words remain a fair assessment of the state of the literature today.” Radsan, supra note 17, at 602. The Hague Convention of 1907 limited its definition of a “spy” to the context of war, reading: “A person can only be considered a spy when, acting clandestinely or on false pretences, he obtains or endeavours to obtain information in the zone of operations of a belligerent, with the intention of communicating it to the hostile party.” Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land art. 29, Oct. 18, 1907, 36 Stat. 2277, 187 Consol. 227 [hereinafter Convention IV]. The Hague Convention’s definition and treatment of spies was subsequently reaffirmed in other rules of warfare agreements, such as in the Geneva Protocols of 1977, Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts art. 46, June 8, 1977, 1125 U.N.T.S. 609.
51. Radsan, supra note 17, at 602.
therefore not afforded any protections beyond “humane” treatment and limited trial rights under the laws of armed conflict.\textsuperscript{52} Espionage during wartime is thought to be legitimate because of the “absence of any general obligation of belligerents to respect the territory or government of the enemy state,” meaning that sovereignty is essentially suspended.\textsuperscript{53}

Nevertheless, there is no peacetime counterpart to the Hague Convention. As a result, academics have been divided on whether the lack of targeted law suggests that peacetime espionage is legal, illegal, or neither legal nor illegal.\textsuperscript{54} Regardless of its current questionable legality, peacetime espionage should be regarded as a violation of international law with respect to “territorial integrity and political independence” of other nations, as well as a violation of the inalienable rights of individuals.\textsuperscript{55}

2. State Sovereignty

The principle of state sovereignty is a cornerstone of international law, providing tentative guidance for restrictions on intelligence gathering. The international courts affirmed the norm of non-intervention as foundational in matters of sovereignty.\textsuperscript{56} As the Permanent Court of International Justice articulated in the 1927 \textit{Lotus} case, “the first and foremost restriction imposed by international law upon a State is that—failing the existence of a permissive rule to the contrary—it may not exercise its power \textit{in any form} in the territory of another State.”\textsuperscript{57}

The United Nations Charter, the constitutive document of international law, espouses the notion of sovereignty repeatedly

\begin{itemize}
\item \textsuperscript{52} Convention IV, \textit{supra} note 50, arts. 24, 30, 31. The First Additional Protocol to the Geneva Conventions reiterates that spies are not entitled to Prisoner-of-War status unless they return to their armed forces and cease espionage activities prior to being captured. Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts, art. 46(4), June 8, 1977, 1125 U.N.T.S. 3.
\item \textsuperscript{53} Quincy Wright, \textit{Espionage and the Doctrine of Non-Intervention in Internal Affairs}, in \textit{ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW}, \textit{supra} note 50, at 3, 12.
\item \textsuperscript{54} See, e.g., Demarest, \textit{supra} note 15, at 347 (arguing that although espionage is an “unfriendly act,” it does not violate international law); Wright, \textit{supra} note 53, at 12 (arguing that peacetime espionage violates a state’s duty to “respect the territorial integrity and political independence of other states”); Daniel B. Silver et al., \textit{Intelligence and Counterintelligence, in NATIONAL SECURITY LAW} 935, 965 (John Norton Moore & Robert F. Turner eds., 2d ed. 2005) (describing the legality of espionage in international law as “oxymoronic” and concluding that the ambiguity of the law results in situational rules).
\item \textsuperscript{55} Wright, \textit{supra} note 53, at 12.
\item \textsuperscript{56} S.S. “Lotus” (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 18 (Sept. 7).
\item \textsuperscript{57} \textit{Id.} (emphasis added).
\end{itemize}
throughout its articles.58 The Charter begins by stating that the United Nations is “based on the principle of the sovereign equality of all its Members.”59 Article 2(4) provides that “[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.”60 “[I]t is now widely accepted that the prohibition applies to any use of force not otherwise permitted by the terms of the Charter,” not just force against the territorial integrity or political independence of another state.61 In addition to prohibiting the threat or use of force, the article expounds a principle of non-interference in the sovereign affairs of a foreign nation.62

Similarly, Article 2(7) reinforces the notion of state sovereignty as it states, “[n]othing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state . . . .”63 Moreover, the General Assembly Declaration on Principles of International Law concerning Friendly Relations and Co-operation Among States, an influential body that reflects the status of current customary international law, maintains that “[e]very State has an inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another State” and prohibits states from intervening, directly or indirectly, for any reason, in the internal or external affairs of another state.64 The United Nations Convention on the Law of the Sea also seeks to preserve territorial integrity by prohibiting foreign ships from engaging in intelligence collection in the territorial sea of another state, which extends up to twelve nautical miles from a nation’s coast.65

58. See generally U.N. Charter.
59. Id. art. 2, ¶ 1.
60. Id. art. 2, para. 4.
62. See id. at 602 (noting that “[b]y the principle of sovereignty (and the derivative notion of territorial integrity), a state enjoys near absolute control over access to its territory”).
63. U.N. Charter art. 2, para. 7
In addition to codified international agreements, state sovereignty is also guaranteed by customary international law. In *The Case Concerning the Military and Paramilitary Activities In and Against Nicaragua*, the International Court of Justice evaluated whether the United States violated customary international law by encouraging, supporting, and aiding military and paramilitary activities in and against Nicaragua. The court decided that the United States was in breach of its obligation under customary international law not to violate the sovereignty of another state, and emphasized that, “[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations.”

These international principles affect local jurisprudence within states. For example, a recent federal court decision in Canada ruled on the issue of collecting covert intelligence abroad, and relied on customary international law principles of territorial sovereignty and non-intervention. The court, in *Re Canadian Security Intelligence Service Act* (CSIS case), held that Canada’s chief security intelligence agency—the Canadian Security Intelligence Service (CSIS)—could not legally engage in electronic surveillance and gather intelligence in a foreign state as per international law and various domestic statutes. Specifically, the Canadian court found that “the warrant [sought by CSIS] would therefore be authorizing activities that are inconsistent with and likely to breach the binding customary principles of territorial sovereign equality and non-intervention, by the comity of nations. These prohibitive rules of international law . . . have evolved to protect the sovereignty of nation states against interference from other states.”

3. Human Rights Law

Along with state sovereignty, individual privacy rights are deeply ingrained in the notion of international human rights. Many of the international agreements guaranteeing the right to privacy go so far as to specifically protect communications.
there is a strong argument that clandestine surveillance inherently violates individual human rights.

The Universal Declaration of Human Rights (UDHR)\textsuperscript{74} is one of the formative international human rights documents.\textsuperscript{75} Following World War II, world leaders came together to establish a new commitment to ensuring respect for the inherent dignity and inalienable rights of all persons.\textsuperscript{76} The UDHR and the International Covenant on Civil and Political Rights (ICCPR), guarantee privacy protections, declaring that no individuals may be subject to arbitrary or unlawful “interference with his privacy, family, home or correspondence. Everyone has the right to the protection of the law against such interference or attacks.”\textsuperscript{77} While neither agreement actually defines “privacy,” they do suggest that everyone has the right to be free from arbitrary or unlawful interference of “correspondence,” demarcating correspondence as a protected realm.\textsuperscript{78} The Human Rights Committee, set up pursuant to Article 41 of the Covenant, later elaborated on the meaning of Article 17 of the ICCPR, opining that interferences must be authorized under the law on a case-by-case basis, ensuring that any interference is essential to society’s interests and in accordance with the provisions and objectives of the Covenant.\textsuperscript{79} The Committee further expounded on its meaning of “correspondence”: “Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.”\textsuperscript{80} In addition,
the Committee describes safeguards, prescribing states to ensure that effective measures are taken to secure any personal information gathered and stored by its authorities, and also granting private individuals the right to request the rectification or elimination of information unlawfully collected or used.81

The International Telecommunication Convention of 1973 similarly emphasizes the importance of privacy, and provides that all members must take “all possible measures” to ensure the secrecy of international correspondence.82 Several years later, the Organization for Economic Cooperation and Development created its Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, which contains several provisions meant to minimize infringements on privacy rights and potential abuses of power.83 It requires that even exceptions to the guidelines related to national security should be “as few as possible,” and “made known to the public.”84 Further, the collection of personal data should be limited, obtained by lawful and fair means, and, when possible, with the knowledge or consent of the individual being surveilled.85 The reason for collecting personal data must be specified by the time of its collection, and the data must then be used exclusively for a specified purpose.86 Finally, the personal data may not be disclosed without either the consent of the data subject or by law.87

The Vienna Convention on Diplomatic Relations establishes a clear framework regarding the rules for spying on a diplomatic mission.88 The convention declares that diplomats, 89 the premises of a diplomatic mission, 90 the “archives and documents of the mission,” 91 and the “official correspondence of the mission” 92 shall be inviolable. The convention defines “official correspondence” as “all correspondence relating to the mission and its functions.”93

81. Id. ¶ 10.
83. See generally OECD Guidelines, supra note 19.
84. Id. at 14.
85. Id.
86. Id.
87. Id.
89. Id. art. 29.
90. Id. art. 22.
91. Id. art. 24.
92. Id. art. 27.
93. Id.
Global Framework Protecting Privacy

Not only is the receiving state prohibited from entering the premises of the mission, but the receiving state is also “under a special duty to take all appropriate steps to protect the premises of the mission against any intrusion or damage and to prevent any disturbance of the peace of the mission or impairment of its dignity.”94 Further, the premises are immune “from search, requisition, attachment or execution.”95 Consequentially, intercepting the communications of diplomats or those of diplomatic missions, and otherwise spying on a diplomatic mission, violate the convention. While narrow in scope, the Vienna Convention on Diplomatic Relations similarly underlines privacy as fundamental to relations between states.

4. Customary International Law

In addition to binding international law, nations also have customary international law obligations to the international community.96 Article 38 of the Statute of the International Court of Justice defines international custom as a “general practice accepted as law.”97 Generally, a customary international law is a rule “created and sustained by the constant and uniform practice of States... in circumstances which give rise to a legitimate expectation of similar conduct in the future.”98 It is generally accepted that for a practice to become customary international law two elements must exist: state practice and opinio juris.99

To constitute state practice, the conduct in question must be “both extensive and virtually uniform,” such that it is performed consistently by a widespread and representative number of states.100 In addition, the practice must occur in a manner that demonstrates “a general recognition that a rule or legal obligation

94. Id. art. 22.
95. Id.
96. Statute of the International Court of Justice art. 38, June 26, 1945, 3 Bevans 1179 [hereinafter ICJ Statute]. As is the case with most law, there are many caveats and specifics in relation to the formation of customarily international law. This Note does not go into depth regarding these considerations, as they are irrelevant to the analysis.
97. See id.
99. Continental Shelf (Libya v. Malta), Judgment, 1985 I.C.J. 13, ¶ 27 (June 3) (“It is of course axiomatic that the material of customary international law is to be looked for primarily in the actual practice and opinio juris of States.”).
100. North Sea Continental Shelf (Ger./Den.; Ger./Neth.), Judgment, 1969 I.C.J 1, ¶ 74 (Feb. 20).
is involved,” implying that the practice must be public.\textsuperscript{101} \textit{Opinio juris}, the second requirement for the existence of custom, requires evidence that states felt “legally compelled” to act in accordance with the norm in question.\textsuperscript{102}

Customary international law could plausibly support both sides of the surveillance debate. On one hand, proponents of surveillance can argue that foreign surveillance has become so prevalent, albeit in different forms, that it has the character of customary international law. On the other hand, privacy advocates may argue that individual privacy protections and state sovereignty either independently constitute customary international law, or have become part of customary international law by way of the treaties that espouse those principles.

5. The Self-Defense Exception

Following World War II, the international community drafted the United Nations Charter, which includes a prohibition on the use of force,\textsuperscript{103} and, together with related customary international laws,\textsuperscript{104} governs how and when force may be used by states.\textsuperscript{105} Article 51 of the United Nations Charter arguably serves as a justification available to intelligence agencies within the current framework of applicable international law.\textsuperscript{106} Article 51 states, “Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.”\textsuperscript{107} The categorical assertion that “nothing” may impair the right to self-defense provides for the sole exception in the United Nations Charter for one state to violate another state’s sovereignty and independence.\textsuperscript{108}

Although the text of the provision seems to indicate that the right to use self-defense is limited to responses to armed attacks

\textsuperscript{101.} \textit{Id.; accord} ILA \textit{Report, supra note 98, §§ 1, 5.} Performance may entail either physical or verbal acts or omissions. ILA \textit{Report, supra note 98, § 4.}

\textsuperscript{102.} \textit{See} North Sea Continental Shelf, 1969 I.C.J. ¶ 77; ILA \textit{Report, supra note 98, § 2} (defining state act(s), conduct, behavior, or usage as neutral to whether they are positive or negative, meaning that the norm may require, prohibit, or allow the practice at issue).

\textsuperscript{103.} U.N. Charter art. 2, para. 4.

\textsuperscript{104.} For a further discussion of customary international law, see \textit{supra} notes 96–102 and accompanying text.

\textsuperscript{105.} \textit{See, e.g.,} U.N. Charter arts. 39, 51.

\textsuperscript{106.} \textit{See id.} art. 51.

\textsuperscript{107.} \textit{Id.} art. 51.

\textsuperscript{108.} U.N. Charter.
Global Framework Protecting Privacy

once they have already occurred, most international legal scholars interpret a broader reading of the right.109 Among those whom support a broader construction of the text, the most common interpretation arises from an incident referred to as the Caroline case.110 The resolution of the dispute in the Caroline case set forth the principles that (1) self-defense is justified where there is “a necessity of self-defense, instant, overwhelming, leaving no choice of means, and no moment for deliberation” and (2) the response was not “unreasonable or excessive; since the act, justified by the necessity of self-defense, must be limited by that necessity, and kept clearly within it.”111 The International Military Tribunal at Nuremberg acknowledged and implemented the criteria for self-defense articulated in the Caroline case over a century later, and legitimized the right to self-defense in cases of imminent attack.112 Consequently, it is now widely accepted that a state may engage in defensive actions if an armed attack is imminent or has occurred.113 Lastly, Article 51’s final clause requires that a state exercising its right to self-defense immediately report its actions to the Security Council, and must discontinue its defensive actions once the Security Council has acted.114


110. The Caroline case was resolved by diplomatic correspondence, rather than judicial process. Samuel R. Maizel, Intervention in Grenada, 35 Naval L. Rev. 47, 72 n.136 (1986). The incident concerned an American ship, the Caroline, which supplied weapons to American volunteers and Canadian rebel forces fighting against the British for independence. In response, British forces seized the Caroline, set it on fire, and set it adrift over Niagara Falls. R.Y. Jennings, The Caroline and McLeod Cases, 32 Am. J. Int’l L. 82, 83–84 (1938). For more information about the Caroline case, see generally Jennings, supra.

111. Letter from Lord Ashburton to Mr. Webster (July 28, 1842), reprinted in 30 British and Foreign State Papers, 195, 195–96 (1841–42) (accepting the terms suggested by Daniel Webster, the United States Secretary of State, to Mr. Fox, the British Minister in Washington); see also Letter from Mr. Webster to Mr. Fox (Apr. 24, 1841), reprinted in 29 British and Foreign State Papers 1129, 1137–38 (1840–41).

112. Judicial Decisions Involving Questions of International Law—International Military Tribunal (Nuremberg), Judgment and Sentences, 41 Amer. J. Int’l L. 172, 205 (1947) [hereinafter Nuremberg Judgment] (“It must be remembered that preventive action in foreign territory is justified only in case of ‘an instant and overwhelming necessity for self-defense, leaving no choice of means, and no moment of deliberation.’”).

113. See Lewis, supra note 109, at 3:6.

III. Analysis

A. Piecing Together the Current Framework & Assessing Its Deficiencies

While the foregoing survey of international law delineates fairly clear notions of state sovereignty and individual privacy rights, it only provides spotty rules in relation to peacetime espionage, prohibiting spying on certain actors in certain places, while leaving many issues unresolved.

1. State Sovereignty

The Vienna Convention on Diplomatic Relations’ requirement that diplomats, the premises of a diplomatic mission, the “archives and documents of the mission,” and the “official correspondence of the mission” shall be inviolable, in conjunction with the responsibility of the receiving state to protect the premises of the mission from intrusion or impairment of its dignity, makes surveilling diplomatic missions clearly unlawful. On the other hand, the Vienna Convention on Diplomatic Relations, along with various other agreements, also presents a deficiency in the applicable law. The convention often renders domestic laws prohibiting surveillance useless, as diplomats, presumably including those conducting espionage on behalf of a foreign state, are immune from civil and criminal prosecution by the host state.

Beyond the walls of diplomatic missions, the ambiguities of the current framework make its application in the context of modern surveillance capabilities nearly impossible. For instance, it is questionable whether intercepting emails and phone calls of foreign leaders and citizens actually violates the territorial integrity or political independence of the state under surveillance guaranteed by the United Nations Charter, or, more generally, “the first and foremost restriction imposed by international law upon a State [:] that . . . it may not exercise its power in any form in the territory of another State.”

These ideas lead to other inquiries such as: does intercepting electronic communications constitute a physical intru-

---

115. VCDR, supra note 88, art. 29.
116. Id. at 22.
117. Id. at 24.
118. Id. at 27.
119. See, e.g., id. at 31. Nonetheless, the sending state may waive a diplomat’s immunity. Id. at 32. Few states have prosecuted foreign “diplomats” for espionage; rather, it is more likely that the diplomat would be declared personae non grata by the receiving country and expelled. Radsan, supra note 17, at 620–21.
120. See U.N. Charter art. 2, para. 4.
tion; are the politics of the surveilled state directly impacted through monitoring and collection; and is surveillance an exercise of power?

From a broad perspective, surveillance on foreign heads of state does seem to violate the principle of non-interference in the sovereign affairs of a foreign nation.122 Moreover, to complicate matters, even foreign-to-foreign telephonic and electronic communications signals are often routed through another state or through satellites in outer space, such that the communications may be intercepted without physically entering the states where the communications begin and end.123 These complex factors lead to further ambiguities such as: (1) would intercepting signals traveling through the collecting state, or intercepting signals as they travel to or from satellites in outer space constitute violations of state sovereignty?;124 and (2) would intercepting and tampering with physical products traveling to a state, but doing so prior to their arrival in such state, constitute a violation of the current framework?

Further, while the Law of the Sea Convention extends a nation’s territory to its territorial sea and prohibits foreign ships from engaging in surveillance from that area, foreign ships are not prohibited from collecting such information on the high seas, where they could access fiber-optic cables.125 This raises issues similar to those mentioned above, namely, are the communications traveling through cables, beyond the physical boundaries in which the state is sovereign, considered a state’s “territory?”

122. See U.N. Charter art. 2, para. 4.
123. Communications transmitted over the internet are often routed through switches, which are often located in the United States or in London, and at which point the communications may be intercepted. Radio communications are transmitted through waves, many forms of which may be intercepted using radio transmitters. Communications transmitted to and from satellites use microwave signals, which can travel long distances, and therefore may be intercepted using relatively few listening stations in particular regions across the world or by SIGINT satellites (also known as spy satellites). Electric cables may be tapped between the terminals of a connection electromagnetically, thus without creating a direct connection. Underwater electric cables can also be tapped in this way from submarines, as the United States has done in the past. New fiber-optic cables can be intercepted using erbium lasers, which transform the signal into an electric signal for transmission. ECHELON Report, supra note 20, § 3.
124. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies art. 2, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205 ("Outer space, including the moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means.").
125. LOSC, supra note 65, arts. 3, 19(2)(c).
In addition, despite addressing a nation’s inherent right to self-defense in response to an actual or imminent armed attack, the United Nation Charter leaves ambiguous whether a state not faced with an armed attack can exert force that does not rise to the level of violating the territorial integrity or political independence of another state. This ambiguity is particularly relevant in determining the legality of espionage because it is questionable whether modern surveillance techniques rise to the level of a violation of territorial integrity or political independence.

2. Human Rights Law

International principles pertaining to human rights and privacy rights similarly fail to provide definitive protections against espionage. Although both the UDHR and ICCPR guarantee all individuals privacy over their communications, the protection is only from arbitrary or unlawful intrusions. While mass surveillance seems arbitrary in its failure to distinguish innocent and potentially suspicious individuals that may pose a threat to national security or the like, it remains unclear what actually constitutes an arbitrary or unlawful intrusion.

Additionally, while the Organization for Economic Cooperation and Development’s Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data restrict the instances in which communications may be intercepted and establish stringent rules for when exceptions apply to protect privacy rights, the national security exception may be interpreted broadly and does not help to narrow the scope of “unlawful” surveillance.

3. Customary International Law

The arguments for customary international law on both sides of the surveillance debate, though compelling, seem to fall short of establishing binding international norms. Although many nations have implemented domestic legislation protecting the privacy rights of their own citizens from unwarranted surveillance by their own intelligence agencies, there are no significant international agreements protecting individual privacy rights from modern for-

126. U.N. Charter art. 2, para. 4, art. 51.
128. UDHR, G.A. Res. 217 (III) A, supra note 76, art. 12; ICCPR, supra note 77, art. 17.
129. See OECD Guidelines, supra note 19, at 14.
eign intelligence collection, thereby being insufficient to meet the state practice prong of becoming part of international custom. Moreover, the ubiquity of transnational espionage by state intelligence agencies demonstrates that the alleged practices of respecting privacy and state sovereignty are not followed in such a way as to show a general recognition that the rule is a legal obligation, thus failing to satisfy \textit{opinio juris}.

While international intelligence collection by state intelligence agencies of foreign heads of state and millions of individuals is becoming increasingly prevalent as a result of modern advances in surveillance technology, it is unlikely that the practice can be defended as a form of customary international law. Even presuming, \textit{arguendo}, that international espionage during peacetime is and has been a prevalent practice by many states, there remains a glaring disconnect between a state’s propensity to spy and public condemnations of surveillance as a transgression of sovereignty rights. The clandestine nature of espionage, a state’s corresponding unwillingness to acknowledge spying, and the general perception of espionage as international delinquency undoubtedly frustrate both the state practice and the \textit{opinio juris} elements necessary to establish custom. While both physical and verbal acts can demonstrate state practice and thus contribute to the formation of custom, such acts do not contribute if they are conducted in secrecy and not communicated to other states, as is the case with spying on allies. Therefore, little can be said to support the legality of peacetime espionage as customary international law.

The most significant hindrance for satisfying the elements of customary international law for both camps is the intrinsic covert nature of foreign espionage. Because intelligence agencies do not publicly reveal their methods for or the extent of their surveillance, it is practically impossible to surmise whether there exists an extensive and virtually uniform state practice of respecting individual privacy rights and non-interference in sovereign states, or of the

\textsuperscript{130} Chesterman, supra note 47, at 1072; ICJ Statute, supra note 96, art. 38; see, e.g., Exec. Order 12,333, supra note 16 and accompanying text.

\textsuperscript{131} See Hopkins & Taylor, supra note 13.

\textsuperscript{132} Chesterman, supra note 47; accord Romero, supra note 12, and accompanying text.

\textsuperscript{133} See Wright, supra note 53, at 17; ILA Report, supra note 98, § 5.

\textsuperscript{134} The committee expressly states that a secret physical act, such as secretly spying on a diplomatic premises, likely does not qualify as state practice, unless the spying is discovered and made public and the state attempts to assert that its conduct was legally justified. ILA Report, supra note 98, § 5.
opposite practice of indiscriminate data collection. The clandestine nature of espionage similarly makes it essentially impossible to determine the subjective *opinio juris* inquiry—whether states feel legally compelled to act in accordance with the practice. For instance, the ICCPR, which enjoys the support of 167 out of 193 countries, declares that no individual can be subject to arbitrary or unlawful inference of his privacy or correspondence. Despite the extensive and virtually uniform ratification of the ICCPR, the absence of evidence of actual consistent state practice in conformity with the Covenant’s principles, and an unclear *opinio juris* on the scope of the privacy right (e.g., what exactly constitutes unlawful or arbitrary interference) will likely prevent the ICCPR’s privacy provision from being adopted as custom. Thus, customary international law should not be relied upon to regulate espionage, as its inherent qualities seem to be incompatible with what is needed to form binding norms.

4. The Self-Defense Exception

A state attempting to justify its foreign intelligence activities may try to evade international law’s state sovereignty protections by contending that its actions are in the name of national security and self-defense, thereby invoking Article 51 of the United Nations Charter. However, because this Note examines peacetime surveillance between allies, the context *ipso facto* precludes situations in which there has been an attack or one is impending. The provision’s text is clear regarding the narrow circumstances under which self-defense may be asserted. It does not provide states with carte blanche to act before they are aware of a potential attack, as this would upend the charter’s guarantees of state sovereignty and territorial integrity. As a result, this exception does not excuse violations of a nation’s territorial integrity and political independence under the circumstances presented.

Another factor precluding intelligence agencies from having recourse to Article 51 is the article’s reporting requirement.

---

136. See *Continental Shelf* (Libya v. Malta), Judgment, 1985 I.C.J. 13, § 81 (June 3); *ILA Report*, supra note 98, § 2.
137. ICCPR, supra note 77, art. 17.
139. A state may only act in self-defense when an attack is imminent and there is no time for the Security Council to deliberate regarding a course of action. See id.
140. See id. art. 2, para. 4., art. 51.
141. *Id.* art. 51.
The article authorizes the unilateral use of force as a measure for safeguarding that state’s integrity, but also obligates states acting in self-defense to report their actions to the Security Council.\textsuperscript{142} Once it reports its actions, the Council reacts as it deems necessary, at which point the defensive state is no longer authorized to use force.\textsuperscript{143} Based on the lack of information indicating otherwise, intelligence agencies engaging in mass surveillance have repeatedly failed to report their allegedly defensive actions to the Security Council and also lack evidence of specific anticipated attacks coming from the nations under surveillance. These issues will make it difficult, if not impossible, for states engaging in indiscriminate intelligence collection to invoke the right of self-defense to prove the legality of their actions.

Furthermore, the principles of self-defense delineated in the Caroline case and endorsed by the International Military Tribunal at Nuremberg stated that the response to an imminent or recent armed attack may not be “unreasonable or excessive,” but rather must be limited to the necessity that justified the self-defense.\textsuperscript{144} While it is admittedly difficult to balance a state’s national security interest with respect to an allegedly specific but unknown attack against potential harm to individual privacy rights, the NSA’s indiscriminate and non-suspicion-based collection of 124.8 billion pieces of telephone data and 97.1 billion pieces of digital data worldwide over the course of one month would seem to raise a red flag with regard to excess.\textsuperscript{145}

5. Moving Forward

Unfortunately, the existing international legal norms do not offer a clear and comprehensive framework to address today’s surveillance issues. In order to meet the modern-day needs of the international community and fill what seems to be a lacuna in international law, the international community must create a new convention using prevailing legal concepts. In creating such a convention, the nations involved should outline the process, methods, boundaries, and oversight mechanisms universally acceptable in conducting intelligence activities both domestically and abroad.

\textsuperscript{142} Id.

\textsuperscript{143} Id.

\textsuperscript{144} See Letter from Lord Ashburn to Mr. Webster, supra note 111, at 196; Letter from Mr. Webster to Mr. Fox, supra note 111, at 1137–38; Nuremberg Judgment, supra note 112, at 205.

\textsuperscript{145} Follorou & Greenwald, supra note 5; European Parliament Draft Report, supra note 9, at 36.
While this Note does not attempt to design such a convention, it does delineate certain protections that may be extrapolated from existing international law principles and should be included in any modern international framework.\footnote{146}

B. Creating a Convention

First and foremost, it is crucial that the process for establishing the elements of a new convention include rigorous public debate regarding the scale and purpose of surveillance in society.\footnote{147} All nations share common interests in protecting privacy, as well as in promoting national security.\footnote{148} Fundamentally, the international community must decide the extent to which it is willing to relinquish individual privacy rights in exchange for national security.\footnote{149}

Overall, a proper legal framework should condemn the vast, systematic, indiscriminate, blanket collection of personal data of innocent people, as this method of collection violates international norms prohibiting the arbitrary interference with any individual’s privacy or communications.\footnote{150} The practice of collecting and storing such intimate information about individuals can have serious ramifications as it breaks down the foundation of democratic societies by infringing upon inalienable rights, “notably freedom of expression, of the press, of thought, of conscience, of religion and of association, private life, data protection, as well as the right to an effective remedy, the presumption of innocence and the right to a fair trial and non-discrimination.”\footnote{151} The marketplace of ideas is essential to a democratic society, and mass surveillance will almost inevitably hinder an open and free society.\footnote{152}

\footnote{146. It should be noted that I am in no way suggesting that the tension between espionage and international law should be resolved by simply eradicating espionage. Espionage has existed for thousands of years, and certainly has its benefits. However, the recent revelations revealing the unfathomable extent of the practice certainly prompt a need to establish boundaries that protect national security while, at the same time, respect the international traditions of state sovereignty and individual privacy rights.}
\footnote{147. See European Parliament Draft Report, supra note 9, at 36.}
\footnote{148. Id.}
\footnote{149. Id.}
\footnote{150. See, e.g., UDHR, supra note 76, art. 12; ICCPR, supra note 77, art. 17 (prohibiting arbitrary or unlawful interference in an individual’s privacy or correspondence).}
\footnote{151. See European Parliament Draft Report, supra note 9, at 9.}
\footnote{152. While not all nations are democracies, and therefore may not agree with these ideals, it is assumed that this covenant is targeted at the many countries that are signatories to the UDHR and the ICCPR, which espouse similar democratic notions and are most likely to agree to an international mechanism for regulation of privacy rights.}
Thus, the convention should establish clear and precise, legally binding principles regarding whose data may be collected.\footnote{Such principles are meant to both define what constitutes unlawful intrusions of an individual’s privacy and also prevent arbitrary intrusions. \textit{See}, e.g., UDHR, \textit{supra} note 76; ICCPR, \textit{supra} note 77.} It should require individualized requests for targeted surveillance, which should be examined on a case-by-case basis by an independent committee. Furthermore, the purpose of the collection should be specified prior to its collection, and the information’s subsequent use should be limited to its original purpose.

The guidelines should incorporate the principles of necessity and proportionality, and multiple evidentiary standards of suspicion based on the degree of desired privacy infringement. Necessity and proportionality would dictate a rule demanding that the interest of the nation in protecting its national security must outweigh the gravity of the invasion of an individual’s privacy in order to permit data collection.\footnote{As noted above, necessity and proportionality are conditions that must be met for a nation to exercise its right to self-defense. \textit{See}, e.g., Military and Paramilitary Activities In and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. ¶ 176 (June 27) (referring to a rule “whereby self-defence would warrant only measures which are proportional to the armed attack and necessary to respond to it” as “a rule well established in customary international law.”). Despite their origins in the use of force context, the terms have come to be defined more broadly and operate in other contexts. Necessity is generally characterized as measures that are indispensable for securing a legitimate aim. Proportionality requires that the measures be the least intrusive among those available to achieve the designed result, and that they outweigh the interest being protected. For additional information, see Judith Gardam, \textit{Necessity, Proportionality and the Use of Force by States} (2009), available at \url{http://ebooks.cambridge.org/ebook.jsf?bid=CBO9780511494178}.} Moreover, not only must the derogation from privacy rights be absolutely necessary to achieve the anticipated objective (protecting national security), but proportionality would also require that the invasiveness of information collection does not extend beyond what is necessary to achieve justifiable ends. Further, a possible evidentiary standard for a national security threat that may be extrapolated from existing law would require present, clear, articulable threats, such that the intelligence collection would be justified as a practice essential to the right to self-defense.\footnote{See \textit{supra} notes 111–112 and accompanying text.} Due to the secretive nature of intelligence collection, and the sensitivity of balancing interests, it is particularly important to establish an independent, stringent monitoring system, likely in the form of a committee, to ensure legitimate purpose (protecting national security) and use of data. This would include ex ante authorization and ex post verification.
One consequence of the current ambiguous status of peacetime espionage under international law is that there is no explicit international forum, sanctions, or remedy for punishing unlawful acts of espionage.\textsuperscript{156} In addition to the oversight mechanisms already mentioned, the Covenant should also guarantee access to efficient administrative and judicial redress, to be conducted through an adversarial process. The Covenant must create remedies available to individuals harmed by misconduct to ensure public accountability for those who egregiously violate the principle set forth by the Covenant. One option that would avoid the need to construct an entirely new international tribunal to hear these disputes is to require all signatories to the convention to sign the Additional Protocol to the ICCPR, whose tribunal allows for individuals to submit complaints.\textsuperscript{157}

The Covenant must also design safeguards for government authorities and their contractors to ensure the security of the data collected and stored. Such personal data must be protected against unauthorized access, modification, and loss. These issues may be addressed through a variety of practices. For instance, there should be adequate minimization procedures applicable to the retention and dissemination of any information collected. Moreover, only a small number of vetted individuals should have access to the information gathered, and the information should be secured through encryption.

Snowden’s revelations and subsequent media reporting demonstrate the invaluable role of free press as an additional oversight mechanism, ensuring that state governments are held accountable to their constituents and do not abuse their power.\textsuperscript{158} Despite their crucial role in exposing the NSA’s nefarious practices, Snowden and his entrusted journalists, such as Laura Poitras and Glenn Greenwald,\textsuperscript{159} are being sought by authorities from various countries for releasing classified documents.\textsuperscript{160} This backlash

\textsuperscript{156} Williams, supra note 42, at 1180.

\textsuperscript{157} Optional Protocol to the ICCPR, supra note 79, art. 1; see also European Parliament Draft Report, supra note 9, at 20 (recommending calling on the US to provide for the redress of EU citizens by signing the Additional Protocol to allow complaints under the International Covenant on Civil and Political Rights).


\textsuperscript{159} Both journalists for The Guardian.

2015] \hspace{1cm} \textit{Global Framework Protecting Privacy} \hspace{1cm} 945

against Snowden and his confidants exemplifies the need for stronger whistleblower and press protections.\textsuperscript{161} While not all leakers should be immune from prosecution, there should be a legitimate process in place with independent arbiters responsible for making determinations as to the lawfulness of disclosures.\textsuperscript{162}

C. \textit{Possible Limitations of An International Espionage Framework}

Espionage in response to threat or use of force or in preparation for armed attack may be sanctioned by the United Nations Charter and customary international law as a form of self-defense.\textsuperscript{163} In a speech addressing the recent revelations regarding the NSA’s surveillance programs, NSA Director General Keith Alexander defended the programs as necessary to protect the United States and to save lives: “What we’re doing is for foreign intelligence purposes to go after counterterrorism, counterproliferation, cyberattacks.”\textsuperscript{164} However, as discussed earlier, international law seems to dictate that for a state to invoke self-defense, it must be able to articulate a clear and imminent threat, such that otherwise prohibited anticipatory measures are necessary and proportionate to protect against attack.\textsuperscript{165} Furthermore, many of the countries being surveilled by the United States counter any national security defenses by noting that there is no evidence of terrorists within their borders.\textsuperscript{166} Brazilian President Roussef, in particular, responded to the claim of surveillance to monitor terrorist activities stating, “Brazil knows how to protect itself. We reject, fight and do not harbour terrorist groups.”\textsuperscript{167} Without evidence of terrorist activity, the United States and other nations engaged in similar mass intelligence collection techniques could hardly justify its mass international surveillance programs by merely asserting national security.


\textsuperscript{162} See id.

\textsuperscript{163} U.N. Charter art. 51.


\textsuperscript{165} \textit{Supra} notes 109–113.

\textsuperscript{166} E.g., Thalif Deen, Address to the General Debate of the 68th Session of the General Assembly, Breaking U.N. Protocol, Brazil Lambastes U.S. Spying (Sept. 24, 2013).

\textsuperscript{167} \textit{Id.}
Nevertheless, the precise scope of the right to undertake preemptive self-defense is ambiguous, and has become increasingly contentious with the emergence of new security threats posed by technological advances. While Article 51 definitively refers to “armed attack[s],” it is also phrased in a way that suggests that the provision simply incorporates an \textit{a priori} or “inherent” right to self-defense for every state, necessary for self-preservation. If Article 51 does in fact incorporate customary law that existed prior to the United Nations Charter, the interpretation of what constitutes the “inherent right” may extend substantially beyond “armed attacks,” particularly with modern technological capabilities that provide numerous ways in which a state can attack another state that would be even more destructive than traditional armed attacks. For example, in the case of nuclear attacks and cyber attacks, both could stealthily inflict catastrophic harm on a nation’s physical territory or on governmental activities and the economy, respectively.

Furthermore, some legal scholars contend that international law recognizes the ability of a nation to lawfully take action to defend itself without having to first suffer an attack. Considering modern methods of attack, the amount of time available between “imminent threat” and the damage being done is arguably insufficient to permit the defensive state to take requisite action for its

---

168. See generally Schmitt, supra note 61, at 571, 600; Lewis, supra note 109, at 3:5.


170. The International Military Tribunal at Nuremburg’s judgment reflected the court’s willingness to extend the scope of the right to self-defense beyond the text, which suggests that a response is only permissible once an armed attack has occurred, to include imminent armed attacks. See Nuremberg Judgment, supra note 112.


own preservation. Consequently, some law scholars contend that the international community must reevaluate its understandings of anticipatory defensive actions and adapt the concept of imminent threat to the modern potential for instantaneous and devastating attacks, even if the precise time and place of attack is uncertain. This broad interpretation of the law could potentially be used to warrant widespread intelligence gathering, even on allies during peacetime, so as to detect a threat before it is too late.

IV. CONCLUSION

The legal analysis set forth above of existing, relevant international norms reveals an abundance of fault lines that leave the state of the law unsettled (at best) with regard to peacetime espionage. In light of recent and ongoing technological advances—in the ubiquity of technology in daily life, as well as in surveillance capabilities—all individuals are left increasingly vulnerable to arbitrary intrusions that pervade every aspect of their privacy lives. In order to address this important gap in international law, the international community should convene to openly discuss and create a convention that establishes a process for intelligence collection, and also provides safeguards and oversight mechanisms to protect privacy interests. By creating such convention, foreign leaders may begin to resolve current tensions arising out of overly intrusive transnational intelligence practices, and individuals may begin to regain faith in the sanctity of their fundamental right to privacy.

175. See id.
176. See, e.g., Goldsmith, supra note 40.