Fordham International Law Journal

Volume 37, *Issue* 3 2014 *Article* 3

I Spy with My Not So Little Eye: A Comparison of Surveillance Law in the United States and New Zealand

Valerie Redmond*

*Fordham Law School

NOTE

I SPY WITH MY NOT SO LITTLE EYE: A COMPARISON OF SURVEILLANCE LAW IN THE UNITED STATES AND NEW ZEALAND

Valerie Redmond[*]

[*] J.D. Candidate, 2015, Fordham University School of Law; B.A., 2012, Government and Politics, University of Maryland. I would like to thank my parents, John and Susan, my brother, Tony, my sister, Veronica, my sister-in-law, Renae, and my friends for their support while writing this Note. I would also like to thank Professor Tracy Higgins for her guidance. Finally, I would like to express my gratitude to Maria Fufidio for her assistance, as well as the rest of the staff and Editorial Board of the *Fordham International Law Journal*.

INTRODUCTION

Imagine an action movie in which you are the target of a secret government operation. Helicopters fly overhead and sirens blare in the background. The police are ready to knock down the door and conduct a raid of your home. What is the reason for the raid? The government has covertly conducted surveillance of your every move and is preparing to arrest you for crimes based on this information.

On January 20, 2012, this was the reality for Kim Dotcom when seventy-six New Zealand police officers, some equipped with machine guns and arriving by helicopter, raided his home in connection to piracy and money-laundering allegations.[1] Dotcom is the founder of Megaupload.com, a website considered a piracy hub that allowed users to upload files illegally.[2] Prior to the raid on Dotcom's home, the New Zealand Government Communications Security Bureau ("GCSB") had illegally spied on Dotcom and his associates, all residents and

1. *See* Duncan Grieve, *Kim Dotcom: "I'm Not A Pirate, I'm an Innovator"*, GUARDIAN (U.K.) (Jan. 14, 2014, 12:34 PM), http://www.theguardian.com/technology/2014/jan/14/kim-dotcom-megaupload-pirate-innovator-dance-album-interview (providing details about the raid on Dotcom's home); *see also Kim Dotcom Raid Video Shows Helicopters, Police Vans Used in Arrest of Megaupload Founder*, HUFFINGTON POST (Aug. 9, 2012, 10:56 AM), http://www.huffingtonpost.com/2012/08/09/kim-dotcom-raid-video-megaupload_n_1758317.html (describing the night of Kim Dotcom's arrest).

2. *See* Erich Schwartzel, *U.S. Lays Out Case Against Megaupload, Kim Dotcom,* WALL ST. J. (Dec. 20, 2013, 7:05 PM), http://online.wsj.com/news/articles/SB10001424052702304773104579270710061412756 (describing what Megaupload is and the charges against Kim Dotcom); *see also* Grieve, *supra* note 1 (describing Megaupload as a piracy hub).

citizens of New Zealand.[3] As a result of this scandal, New Zealand enacted amendments to the Government Communications Security Bureau Act, which overtly regulates how the GSCB may conduct surveillance of New Zealand citizens.[4]

New Zealand is not the only country that is experiencing backlash due to its surveillance efforts.[5] In the United States, government officials have faced similar scrutiny in the wake of Edward Snowden's public revelations regarding national security and international surveillance as they implicate privacy rights.[6] On June 5, 2013, Snowden, a former worker for the US National Security Agency ("NSA"), provided the *Guardian* with classified documents about the NSA's abilities, such as the ability to target individuals ranging from "you or your accountant, to a federal judge, to even the President."[7] These documents sparked heated

---

3. *See* Bruce Zagaris, *U.S. Extradition for Mr. Dotcom in N. Zealand Caught in Controversies,* 28 INT'L ENFORCEMENT L. REP. 450 (2012) (explaining that the New Zealand Government Communications Security Bureau ("GCSB") illegally spied on Mr. Dotcom); *see also New Zealand Extends Domestic Spying Powers*, BBC (Aug. 21, 2013, 6:49 PM), http://www.bbc.co.uk/news/world-asia-23769206 (describing the allegations made against Kim Dotcom and his associates); Rebecca Quilliam, *GCSB Spying Illegal, but No Charges Laid*, N.Z. HERALD (Aug. 29, 2013, 6:49 PM), http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11116460) (stating that no charges were pursued against the GCSB because criminal intent did not exist).

4. *See New Zealand Spying Law Passes Allowing Surveillance on Citizens*, AGENCE FR. PRESSE (Aug. 21, 2013, 9:50 AM), *available at* http://www.huffingtonpost.com/2013/08/21/new-zealand-spying-law_n_3789041.html (describing the passage of the new surveillance law following this scandal); *see also* Government Communications Security Bureau Amendment Act 2013 (N.Z.) (describing the newest version of the GCSB Act's additions including the specific mention of citizenship).

5. *See* Brett Logiurato, *Edward Snowden Is in the Process of Destroying Any Support and Sympathy He Has Built Up,* BUS. INSIDER (June 17, 2013, 12:57 PM), http://www.businessinsider.com/edward-snowden-backlash-nsa-spying-china-2013-6 (stating that since former NSA worker Edward Snowden's disclosures, there has been a steady backlash against the United States); *see also* Michael Shepard, *Obama Plans to Name Navy Vice Admiral Rogers as Next NSA Chief*, BUS. WK. (Jan. 31, 2014), http://www.businessweek.com/news/2014-01-31/obama-plans-to-name-navy-vice-admiral-rogers-as-next-nsa-chief (noting the international backlash that the United States is facing).

6. *See* Loguirato, *supra* note 5; Shepard, *supra* note 5 (describing the actions of Edward Snowden and the resulting backlash).

7. *See* Glenn Greenwald et al., *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, GUARDIAN (London), June 9, 2013, http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (describing who Edward Snowden is and what he did); *see also* Carol D. Leonnig et al., *Tracking Edward Snowden, from a Maryland Classroom to a Hong Kong Hotel*,

debate in the United States about the protection of the right to privacy.[8] Today, the balance between the right to privacy and the power of government to engage in surveillance is at the heart of this important debate.[9]

In the aftermath of the September 11th attacks in the United States, the London subway bombings in the United Kingdom, and other atrocities, democratic states across the world have invested heavily in surveillance technologies.[10] Concerns relating to privacy violations, however, are at some of the highest levels in history.[11] Commentators on the state of surveillance law have stated that if members of the public understood the magnitude of surveillance, they would believe

---

WASH. POST, June 15, 2013, http://www.washingtonpost.com/world/national-security/tracking-edward-snowden-from-a-maryland-classroom-to-a-hong-kong-hotel/2013/06/15/420aedd8-d44d-11e2-b05f-3ea3f0e7bb5a_story.html (providing a short biography of Edward Snowden's life and actions); Joe Weisenthal & Paul Szoldra, *29-Year Old NSA Whistleblower Makes Mindblowing Claims About the Power He Had*, BUS. WK. (June 9, 2013, 3:14 PM), http://www.businessinsider.com/edward-snowden-nsa-2013-6#ixzz2sTqpQ894 (recounting the exact revelations made by Snowden).

8. *See* Christopher Swift, *Privacy Protections and the Surveillance State: Bridging the Transatlantic Divide*, 19 INT'L TRADE L. & REG. 75 (2013) (noting Edward Snowden disclosed information about classified programs to the *Guardian*); *see also* Frank Jordans & Raphael Satter, *Growing Backlash to Government Surveillance*, N.Z. HERALD (Oct. 13, 2013), http://www.nzherald.co.nz/world/news/article.cfm?c_id=2&objectid=11139434 (discussing the idea that before Edward Snowden's revelation this past summer that many people did not know what the NSA was doing or what it was).

9. *See* Darla W. Jackson, *Protection of Privacy in the Search and Seizure of E-Mail: Is the United States Doomed to an Orwellian Future?*, 17 TEMP. ENVTL. L. & TECH. J. 97 (1999) (noting the delicate balance between individual rights and the need for information); *see also* Alex Conte, *A Clash of Wills: Counter-Terrorism and Human Rights*, 20 N.Z. U. L. REV. 338, 339 (2003) (describing the debate surrounding counterterrorism and the protection of individual rights).

10. *See* Neil Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1938 (2013) (describing what has occurred in surveillance law as a result of these events); *see also* Kevin J. Lawner, *Post-Sept. 11th International Surveillance Activity—A Failure of Intelligence: The Echelon Interception System & the Fundamental Right to Privacy in Europe*, 14 PACE INT'L L. REV. 435, 439 (2002) (discussing how experts agree that surveillance is necessary in the post-9/11 era).

11. *See* David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 J. MARSHALL J. COMPUTER & INFO. L. 1, 4 (1999) (noting that surveys show an increasing concern for privacy); *see also Poll: American Public's Concerns over Surveillance Programs and Privacy Erosion*, FOX NEWS (Sept. 10, 2013), http://www.foxnews.com/us/2013/09/10/poll-american-public-concerns-rise-over-surveillance-programs-and-privacy/ (reviewing the poll results and concluding that Americans do not think that their privacy is protected).

that these actions infringe upon their privacy rights.[12] With the Kim Dotcom scandal and the Edward Snowden revelations, citizens of the New Zealand and the United States, and the international population at large, have become more aware of the potential privacy violations posed by state surveillance efforts.[13]

While the potential privacy violations are at the forefront of public discussion in both the United States and New Zealand, the two countries regulate the surveillance of citizens differently.[14] The United States cannot obtain warrants to conduct surveillance on individuals; however, loopholes in current surveillance law indicate that this requirement can be circumvented.[15] Alternatively, New Zealand's amendments to the Government Communications Security Bureau Act (the "GCSB Act") reveal that the country publicly admits to conducting surveillance of its citizens.[16] The question is whether either approach effectively strikes the appropriate balance between privacy and national security.

This Note compares the surveillance laws in the United States and New Zealand in order to demonstrate that a warrant requirement is not sufficient to protect the right to privacy and curb government spying. Part I of this Note will discuss the history of privacy and surveillance law in the United States and in New Zealand. Part I will also review the right to privacy internationally and the breadth of international surveillance agencies. Part II will compare surveillance law in the United States with the recently enacted amendments to New Zealand

---

12. *See* Erin L. Brown, *Echelon: The National Security Agency's Compliance with Applicable Legal Guidelines in Light of the Need for Tighter National Security*, 11 COMMLAW CONSPECTUS 185, 198 (2003) (stating that if people were aware of the scope of surveillance their thoughts would change about the state of their privacy rights). *See generally Poll: American Public's Concerns over Surveillance Programs and Privacy Erosion*, *supra* note 11 (describing how Americans felt about surveillance after the scope of American spying was publicly revealed by Edward Snowden).

13. *See supra* notes 4–5 and accompanying text (surveying the problems that New Zealand and the United States have faced because of the Kim Dotcom and Edward Snowden scandals).

14. *See infra* Part 1.B–.C (describing how the United States and New Zealand have developed their surveillance and privacy law).

15. *See infra* Part I.B.3 (outlining the provisions of Foreign Intelligence Surveillance Act ("FISA") that prohibit the Government from spying on US citizens).

16. *See infra* Part I.C.3 (providing an overview of the GCSB Act amendments that allow New Zealand to spy on its citizens).

law. Part II will also analyze the impact of New Zealand's new law on its citizens. Finally, Part III will provide an overview of proposed solutions for the international surveillance landscape. Part III will also argue that despite their different articulations of surveillance policy, the United States and New Zealand have similar problems with their surveillance laws that are not easily fixed.

I. *PRIVACY LAW IN THE UNITED STATES AND NEW ZEALAND*

Part I provides background information on the concept of the right to privacy generally, as well as how this right is treated in the United States and in New Zealand. Part 1.A. gives a general introduction to the right to privacy. Part 1.A.1 narrows this introduction, providing an overview of the right to privacy internationally. Part I.B outlines the extensive background of the right to privacy and surveillance law in the United States. Part I.C explains the development of privacy and surveillance law in New Zealand. Lastly, Part I.D provides an overview of Echelon, an NSA-operated secret international surveillance program changing the face of international surveillance.[17]

A. *The Right to Privacy*

Though privacy is central to many contemporary concerns, it remains an elusive concept.[18] The modern concept of privacy grew out of the idea that there is a difference between how people present themselves in public and what they do in their private lives, a difference that allows for a certain level of

17. Brown, *supra* note 12, at 185 (describing Echelon as NSA-operated); Lawner, *supra* note 10, at 352 (stating that Echelon is implemented by NSA). *See generally* Matt Bedan, *Echelon's Effect: The Obsolescence of the U.S. Foreign Intelligence Legal Regime*, 59 FED. COMM. L.J. 425 (2007) (providing an extensive review of Echelon); Lawrence D. Sloan, *Echelon and the Legal Restraints on Signals Intelligence: A Need for Reevaluation*, 50 DUKE L.J. 1467 (2001) (outlining the background of Echelon).

18. *See* Lisa Tat, *Plaintiff Culpability and the New Zealand Tort of Invasion of Privacy*, 39 VICT. U. WELLINGTON L. REV. 365 (2008) (noting that there is no universally accepted definition of privacy); David Lindsay, *An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law*, 29 MELB. U. L. REV. 131, 135 (2005) (noting that privacy is an "elusive" concept and cannot be defined in a satisfactory manner).

autonomy in the private setting.[19] Although the concept of privacy is well known, throughout legal literature there is almost a "complete absence" of agreement as to the correct definition of privacy, as well as to the values that should be emphasized in its protection.[20] The concept of privacy may be so "complex and value-laden" that arguments about it cannot be easily resolved.[21]

1. Right to Privacy: Brief International Perspective

The United Nations formally declared privacy a fundamental right in Article 12 of the Universal Declaration of Human Rights.[22] Further, Article 17 of the 1966 International Covenant on Civil and Political Rights ("ICCPR") protects the right to privacy against arbitrary or unlawful interference, and considers it a vital international civil right.[23] The ICCPR has an Optional Protocol, which allows the Human Rights Committee established in the ICCPR to review allegations of privacy rights

---

19. *See* Megan Vettoretti & Gehan Gunasekara, *Ministerial Free Speech and the Privacy Act*, 17 N.Z. BUS. L.Q. 284, 287 (2011) (explaining the private and public divide creating the necessity for privacy); *see also* Zablocki v. Redhail, 434 U.S. 374, 397 (1978) (discussing the fact that the US Supreme Court's decisions have recognized a guarantee to privacy and autonomy); Henry F. Fradella et al., *Quantifying* Katz*: Empirically Measuring "Reasonable Expectations of Privacy" in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289, 295, 319 (2011) (describing the relation of the right to privacy and autonomy or the right to be left alone).

20. *See* Lindsay, *supra* note 18, at 135 (reviewing the "daunting literature" surrounding the debate on privacy); *see also* Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1094 (2002) (noting that the "horde" of literature has produced many conceptions of privacy).

21. *See* Lindsay, *supra* note 18, at 137 (noting that the definition of privacy is contested and debates cannot be rationally resolved); *see also* Solove, *supra* note 20, at 1089 (stating that privacy is a complex value).

22. Universal Declaration of Human Rights, G.A. Res. 217 (III) A, art. 12, U.N. Doc. A/RES/217(III) (Dec. 10, 1948) (stating formally a right to privacy); *see* Ariel E. Wade, *A New Age of Privacy Protection: A Proposal for an International Personal Data Privacy Treaty*, 42 GEO. WASH. INT'L L. REV. 659, 660 (2010) (describing the United Nations' affirmative declaration of a right to privacy).

23. *See* International Covenant on Article of Civil and Political Rights art. 17, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976) [hereinafter ICCPR] (providing all members a right to privacy against arbitrary intrusion); *see also* Lawner, *supra* note 10, at 465 (discussing the right to privacy established in this convention); Lauren H. Rakower, *Blurred Line: Zooming in on Google Street View and the Global Right to Privacy*, 37 BROOK. J. INT'L L. 317, 337 (2011) (noting that the right to privacy is found in Article 17 of the International Covenant on Civil and Political Rights ("ICCPR")).

violations in signatory countries.[24] Although the US Senate approved the treaty for ratification in 1992, the United States has neither signed nor ratified the Optional Protocol, meaning that US citizens cannot appeal under the protections of this convention if privacy rights have been breached.[25] New Zealand, on the other hand, has not only ratified the ICCPR, but also ratified the Optional Protocol on May 26, 1989.[26]

In addition to the United Nations, the European Union has also recognized privacy as a fundamental right.[27] Article 7 of the Charter of Fundamental Rights of the European Union protects the privacy of the home and family, and Article 8 provides for protection of personal data.[28] Furthermore, the Telecommunications Directive and the Data Protection Directive set guidelines for privacy protection by reinforcing data protection laws and establishing a range of new privacy rights.[29] Specifically, the Telecommunications Directive provides

---

24. *See* Optional Protocol to the International Covenant on Civil and Political Rights, Introduction, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976) (stating that this Optional Protocol establishes a means to appeal to the Human Rights Committee established by the ICCPR); *see also* Lawner, *supra* note 10, at 465 (discussing the ICCPR provisions pertaining to the right to privacy); David Sloss, *Using International Law to Enhance Democracy*, 47 VA. J. INT'L L. 1, 19 n.83 (2006) (mentioning the existence of the Optional Protocol).

25. *See* Optional Protocol to the International Covenant on Civil and Political Rights, *supra* note 24 (failing to list the United States as a signatory); *see also* Lawner, *supra* note 10, at 465 (noting that the Optional Protocol has not been signed by the United States); Sloss, *supra* note 24, at 19 n.83 (explaining that a US citizen may not file a complaint because the United States has not signed the Optional Protocol).

26. *See* ICCPR, *supra* note 23 (identifying the date when New Zealand ratified the Optional Protocol); *see also* Optional Protocol to the International Covenant on Civil and Political Rights, *supra* note 24 (indicating the ratification date for New Zealand).

27. *See* Charter of Fundamental Rights of the European Union, 2012 O.J. C 326/391 [hereinafter Charter of Rights] (granting all members the protection of privacy in the home, life and communications); *see also* Lawner, *supra* note 10, at 461 (describing EU initiatives to protect privacy); Banisar & Davies, *supra* note 11, at 12 (explaining EU directives that provide for data protection).

28. *See* Charter of Rights, *supra* note 27 (stating the specific rights protected under this Charter); *see also* Lawner, *supra* note 10, at 465 (describing the privacy protections implicit in this Charter).

29. *See* Directive 97/66/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the telecommunications sector art 1, 1998 O.J. L 24/1 [hereinafter Telecommunications Directive 97/66] (protecting the right to privacy in the telecommunications sector); Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. L 281/31 [hereinafter Data Protection Directive 95/46]

protections for telephone, mobile, and other telecommunication networks.[30] The Data Protection Directive provides guidelines for the processing of personal data.[31]

Furthermore, the Treaty of the European Union ensures that the European Convention on Human Rights ("ECHR") protects European Union members.[32] Article 8 of the ECHR provides for the right to privacy in the home and family life.[33] The European Court of Human Rights has construed this right broadly when used to protect the collection of information related to the private life.[34] The European Court of Human Rights reviews Member States' laws and can impose sanctions for the failure to regulate wiretapping or other modes of surveillance.[35]

B. *Privacy and Surveillance in the United States*

Overall, the United States does not have an overarching privacy law and instead uses a "piecemeal" approach, relying on

---

(providing protection of all personal information); Banisar & Davies, *supra* note 11, at 13 (describing how these directives operate to protect private information); Jennifer Morris, *Big Success or "Big Brother?": Great Britain's National Identification Scheme Before the European Court of Human Rights*, 36 GA. J. INT'L & COMP. L. 443, 453 (2008) (discussing the parameters of this data protection directive).

30. *See* Telecommunications Directive 97/66, *supra* note 29, art. 2 (explaining that the act exempts radio and television); Banisar & Davies, *supra* note 11, at 12 (explaining the purpose of the Telecommunications Directive).

31. *See* Data Protection Directive 95/46, *supra* note 29, art. 7 (describing criteria to legitimatize data processing); Banisar & Davies, *supra* note 11, at 12 (describing the role of the Data Protection Directive).

32. *See* Consolidated Version of the Treaty of the European Union art. 6, 2012 O.J. C 326/13, at 19 (stating that the European Union accedes to the ECHR); Lawner, *supra* note 10, at 461 (declaring that the ECHR is binding on Member States).

33. Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter ECHR] (granting the right to privacy in the home and family life); Lawner, *supra* note 10, at 467 (describing the rights and freedoms granted in the European Convention of Human Rights ("ECHR")); *see* Wade, *supra* note 22, at 667 (explaining the ECHR and what rights the EU protects).

34. *See* Morris, *supra* note 29, at 460 (stating that the right has been construed broadly); Banisar & Davies, *supra* note 11, at 9 (noting that Article 8 has been read broadly to protect private life).

35. *See, e.g.*, *Klass and Others v. Federal Republic of Germany*, 2 Eur. Ct. H.R. (ser. A) at 214 (1979-80) (reviewing West Germany's laws about wiretapping); Banisar & Davies, *supra* note 11, at 9 (citing situations in which the European Court of Human Rights imposed sanctions); Jackson, *supra* note 9, at 110–11 (noting the cases where the European Court of Human Rights reviewed wiretapping instances and imposed sanctions).

the US Constitution, judicial decisions, legislation, and regulations.[36] Privacy concerns in the United States were notably posed in a seminal 1890 article written by Samuel Warren and Louis Brandeis.[37] Warren and Brandeis have been labeled the "inventors" of the right to privacy in the United States.[38] Their article called for legal limits on surveillance conducted by private parties and called for a legal recognition of the "right to be left alone."[39] It highlighted the importance of the right to privacy, which developed over time in the United States with advances in technology.[40]

In Part I.B.1., this Note will discuss the constitutional protections provided in US law. Part I.B.2 discusses seminal US Supreme Court cases reviewing the Fourth Amendment right to privacy as related to surveillance. Part I.B.3 provides an extensive overview of the Foreign Intelligence Surveillance Act ("FISA") and the Foreign Intelligence Surveillance Court ("FISC"). Lastly, Part I.B.4 briefly discusses the NSA.

---

36. *See* Richards, *supra* note 10, at 1942 (determining that the "law governing surveillance is piecemeal"); Wade, *supra* note 22, at 663 (acknowledging that the United States does not have an "overarching privacy law" and relies on a piece by piece method).

37. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 197 (1890) (exploring whether there is a right to privacy in the United States and whether the law protected that right); Lindsay, *supra* note 18, at 140 (noting that the right to privacy evolved out of "public disclosure of private matters").

38. *See* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality,* 96 GEO. L.J. 123, 125 (2007) (stating that Warren and Brandeis have been hailed as the "inventors" of privacy); Irwin R. Kramer, *The Birth of Privacy Law: A Century Since Warren and Brandeis*, 39 CATH. U. L. REV. 703, 703 (1990) (labeling Warren and Brandeis as the inventors of privacy law).

39. *See* Warren & Brandeis, *supra* note 37, at 193 (arguing that the legal rights have been broadened to the right to be left alone); Lindsay, *supra* note 18, at 140 (describing how Warren and Brandeis discussed what legal limits were needed for surveillance conducted by private parties, not the state); Richards & Solove, *supra* note 38, at 128 (noting that Warren and Brandeis were concerned with the press "'overstepping' their bounds").

40. *See* Lindsay, *supra* note 18, at 140 (arguing that privacy law develops with technology and Warren and Brandeis' article directly related to this idea); Warren & Brandeis, *supra* note 37, at 195 (determining that advances like instantaneous photographs and newspapers have invaded the sacred precincts of private and domestic life).

1. Constitutional Protections: The Fourth Amendment

There is no explicit constitutional right to privacy in the United States.[41] The US Supreme Court, however, has held that there is a limited constitutional right to privacy based on provisions within the US Bill of Rights such as the First, Third, Fourth, and Fifth Amendments.[42] Notably, in *Griswold v. Connecticut*, the Supreme Court held that there was an implied right to privacy based on the "penumbras, formed by emanations from the Bill of Rights' guarantees."[43] The Court has found this right within the Fourth Amendment's protection against unlawful searches and seizures.[44] The Fourth Amendment also applies to federal government searches to obtain foreign intelligence and surveillance.[45]

2. US Supreme Court Cases Reviewing the Right to Privacy and the Fourth Amendment

The privacy principle of the Fourth Amendment, and its application to surveillance, has been examined in three main US

---

41. *See* U.S. CONST. amends. I–X (affirming many rights, but absent a grant of any explicit privacy right); Wade, *supra* note 22, at 662 (explaining that there is no explicit constitutional right but that the Court has found the right to be implicit in the Constitution); Kevin C. McAdam & John R. Webb, *Privacy: A Common Law and Constitutional Crossroads*, 40 COLO. LAW. 55, 56 (2011) (stating that there is no express right to privacy).

42. *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (reviewing amendments where the right to privacy is implicit); Banisar & Davies, *supra* note 11, at 108 (referring to the number of provisions within the US Constitution in which the Supreme Court has found a right to privacy); Wade, *supra* note 22, at 662 (listing provisions of the US Constitution where a right to privacy may be inferred).

43. S*ee Griswold*, 381 U.S. at 484 (discussing the implied right to privacy found in the US Constitution); Wade, *supra* note 22, at 662 (explaining how the Court determined that there is an implied right to privacy).

44. *See* Katz v. United States, 389 U.S. 347 (1967) (finding a right to privacy based on the Fourth Amendment "wherever a man may be"); Brown, *supra* note 12, at 196 (citing the Fourth Amendment and its relevance in the US surveillance system); Jack Wade Nowlin, *The Warren Court's House Built on Sand: From Security in Persons, Houses, Papers, and Effects to Mere Reasonableness in Fourth Amendment Doctrine*, 81 MISS. L.J. 1017, 1023 (2012) (discussing the reasonable expectation of privacy under the Fourth Amendment).

45. *See* U.S. CONST. amend. IV (granting the right to be free from unreasonable search and seizure); United States v. Butenko, 494 F.2d 593, 602–03 (3d Cir. 1974) (applying the Fourth Amendment to the federal government's actions); Sloan, *supra* note 17, at 1492 (explaining that the Fourth Amendment is a fundamental limitation on intelligence gathering and its application to the federal government).

Supreme Court cases.[46] In *Olmstead v. United States*, the Court considered the constitutionality of the government's participation in electronic surveillance.[47] This was one of the first cases to specifically review the constitutionality of wiretapping.[48] In *Olmstead*, the Court held that the Fourth Amendment did not provide protection from electronic surveillance.[49] It construed the Fourth Amendment narrowly as only protecting against trespassory searches and seizures, and rejected the idea that the Fourth Amendment's protections could extend beyond the physical search of a limited area.[50] In Justice Brandeis's dissent, he postulated that the Fourth Amendment should not be limited to physical property, but it should extend to invasions of "personal security, personal liberty and private property."[51] This dissent aside, the US Supreme

46. *See* Olmstead v. United States, 277 U.S. 438 (1928) (stating that the issue in the case was whether wiretapping of telephones was constitutional)*; Katz*, 389 U.S. at 359 (1967) (holding that wiretapping of telephones is unconstitutional even if reached from outside the home); United States v. US District Court (*Kieth*), 407 U.S. 297 (1972) (reviewing the government's ability to conduct warrantless domestic surveillance); Rebecca A. Copeland, *War on Terrorism or War on Constitutional Rights? Blurring the Lines of Intelligence Gathering in Post-September 11 America*, 35 TEX. TECH L. REV. 1, 6 (2004) (explaining the impact of the *Olmstead*, *Katz* and *Keith* cases).

47. *See Olmstead,* 277 U.S. at 438 (discussing the constitutionality of wiretapping of private telephones); Brown, *supra* note 12, at 196 (explaining that *Olmstead* was the first time that the US Supreme Court considered this problem); Copeland, *supra* note 46, at 6 (stating that before *Olmstead* the US Supreme Court had not considered the issue of electronic surveillance).

48. *See Olmstead*, 277 U.S. at 455 (stating that the case reviews the constitutionality of wiretapping); Copeland, *supra* note 46, at 6 (noting that this was the first instance in which the US Supreme Court reviewed wiretapping).

49. *See Olmstead*, 277 U.S. at 466 ("We think, therefore, that the wire tapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment."); Brown, *supra* note 12, at 196 (discussing that the Fourth Amendment was not intended to protect against non-trespassory electronic surveillance); Sloan, *supra* note 17, at 1493 (noting the US Supreme Court's holding that the Fourth Amendment does not provide protection from electronic surveillance).

50. *See Olmstead*, 277 U.S. at 465 ("The intervening wires are not part of his house or office, any more than are the highways along which they are stretched."); Jonathan D. Forgang, *"The Right of the People": The NSA, the FISA Amendments Act of 2008, and Foreign Intelligence Surveillance of Americans Overseas*, 78 FORDHAM L. REV. 217, 227 (2009) (describing the Court's holding in *Olmstead* as limiting the Fourth Amendment's protections to physical searches of private property).

51. *See Olmstead*, 277 U.S. at 474–75 (Brandeis, J., dissenting) ("[B]ut it is the invasion of his indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited by his conviction of some public offense . . . ."); Forgang, *supra* note 50, at 227 (describing the dissent written by Justice Louis Brandeis).

Court held that the US Government did not infringe upon any constitutional right to privacy.[52]

In 1967, the Supreme Court overruled *Olmstead* in *Katz v. United States*, finding wiretapping to be restricted by the privacy protections implicit in the Fourth Amendment.[53] The Court found that the Fourth Amendment creates and protects a reasonable expectation of privacy.[54] The Court went beyond the Fourth Amendment's previously recognized protections and decided to protect those areas that are private outside the home.[55] The Court, however, did not address whether a warrant was required to conduct electronic surveillance for national security purposes.[56] This question was not answered until 1972 in *United States v. United States District Court*, popularly known as the *Keith* case.[57]

---

52. *See Olmstead*, 277 U.S. at 466 (holding that no constitutional right was infringed upon by the wiretapping); Forgang, *supra* note 50, at 228 (noting the ability of federal agencies to use warrantless wiretaps in criminal and intelligence investigations); Neal Katyal & Richard Caplan, *The Surprisingly Stronger Case for the Legality of the NSA Surveillance Program: The FDR Precedent*, 60 STAN. L. REV. 1023, 1037 (2008) (discussing how the FBI continued to use wiretapping surveillance after *Olmstead*).

53. *See* Katz v. United States, 389 U.S. 347, 359 (1967) ("The government agents here ignored the procedure of antecedent justification that is central to the Fourth Amendment, a procedure that we hold to be a constitutional precondition of the kind of electronic surveillance involved in this case.").

54. *Id.* at 351 (holding that the Fourth Amendment grants a right to privacy against governmental intrusion); *see* Sloan, *supra* note 17, at 1493 (explaining that the protections of the Fourth Amendment are not only applied to specific places, but also to people and their reasonable expectations of privacy); Brown, *supra* note 12, at 197 ("The Court relied on the reasoning that petitioner had a reasonable expectation of privacy, and therefore the use of a listening device was deemed an unconstitutional search and seizure.").

55. *See Katz*, 389 U.S. at 353 (discussing the erosion of past limitations on the application of the Fourth Amendment); Forgang, *supra* note 50, at 229 (describing the holding in *Katz*).

56. *See Katz*, 389 U.S. at 359 n.23 (indicating that this case did not address national security cases); Sloan, *supra* note 17, at 1493 ("The unresolved question of warrantless electronic surveillance for national security purposes was addressed in the 1972 case of United States v. United States District Court."); David G Barnum, *Warrantless Electronic Surveillance in National Security Cases: Lessons from America*, 5 EUR. HUM. RTS. L. REV. 633, 655 (2006) (stating that this case did not address whether prior authorization would satisfy the Fourth Amendment because it was not a question presented in this case).

57. *See* United States v. US District Court (*Kieth*), 407 U.S. 297 (1972) (holding that judicial approval is required for domestic surveillance); *see also* Forgang, *supra* note 50, at 233 (describing the *Keith* case and the Court's decision about warrants for electronic surveillance); *see also* Robert Bloom & William J. Dunn, *The Constitutional*

In the *Keith* case, the Supreme Court reviewed a petition by the US Government for a writ of mandamus to compel a US District Court judge to disclose electronically monitored telephone conversations, which had been ordered collected by the US Attorney General, to protect national security.[58] The Court restated its "deep seated uneasiness and apprehension" with the US Government's ability to conduct secret electronic surveillance, even when the goal was to prevent terrorism.[59] This case held that judicially-approved warrant procedures are necessary for the US Government to constitutionally conduct secret surveillance.[60] The case, however, did not address what would be required when the US Government collected information about foreign powers or their agents.[61] Instead, the US Supreme Court in the *Keith* case invited the US Congress to create legislation governing electronic surveillance.[62]

3. The Foreign Intelligence Surveillance Act of 1978

In 1975 after the *Keith* case, the US Congress examined intelligence collection practices.[63] Following the investigation,

---

Infirmity of Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury to the Fourth Amendment, 15 WM. & MARY BILL RTS. J. 147, 155 (2006) (describing the question of warrants reviewed in the *Keith* case).

58. *See Keith*, 407 U.S. at 300 (citing the Attorney General's affidavit in support of the government's ability to conduct the surveillance and also citing the fact that the Attorney General approved the collection); *see also* Copeland, *supra* note 46, at 10 (quoting the affidavit as stating collection was warranted, "to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the [US] Government").

59. *See Keith*, 407 U.S. at 312 (describing the feelings of the Court when making their decision); *see also* Copeland, *supra* note 46, at 10 (stating the Court's reiteration of its uneasiness and apprehension).

60. *See Keith*, 407 U.S. at 320 (describing that procedures are necessary for surveillance to be constitutional); *see also* Copeland, *supra* note 46, at 10 (affirming that the *Keith* case established that a warrant procedure with judicial approval is necessary for secret surveillance to be constitutional).

61. *See Keith*, 407 U.S. at 308–09 (indicating that this case was about a potential attack by a domestic organization and did not involve foreign powers); *see also* Forgang, *supra* note 50, at 232 (describing the Court's decision to narrow the scope of the case to domestic intelligence and not foreign intelligence).

62. *See Keith*, 407 U.S. at 322 ("Congress may wish to consider protective standards for the latter."); *see also* Copeland, *supra* note 46, at 10 (explaining that Justice Powell made the invitation to Congress to enact legislation regulating surveillance).

63. *See Church Committee Created*, U.S. SENATE, http://www.senate.gov/artandhistory/history/minute/Church_Committee_Created.htm (last visited Apr. 1, 2014) (outlining the development of the Church Committee and its investigation into

Congress drafted FISA.[64] Congress enacted FISA in 1978 for the purpose of regulating the use of electronic surveillance in the United States for foreign intelligence purposes.[65] FISA is the "primary vehicle" that allows the US Government to conduct electronic surveillance on individuals who are suspected of engaging in terrorist activities.[66] FISA defines electronic surveillance as the acquiring of a communication, through intentional targeting, that was either sent or received by a US person and if the circumstances are such that the person has a reasonable expectation of privacy.[67]

FISA provides a framework for US Government agency officials to follow when conducting electronic surveillance.[68] A "guiding principle" of FISA is its regulation of the US executive power to conduct electronic intelligence by imposing a warrant application procedure.[69] To obtain approval of a warrant from the FISC, an application must include the identity of the target, a certification that the target was a foreign power or agent of a

---

intelligence practices)*; see also* Forgang, *supra* note 50, at 233 (describing the actions Congress took to examine intelligence collection procedures); *see also* Bloom & Dunn, *supra* note 57, at 156 (noting Congress' review of the appropriate protective standards).

64. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1885(c) (2012); *see* Forgang, *supra* note 50, at 233 (describing the congressional action that culminated in the passage of FISA).

65. *See* Nathan C. Henderson, Note, *The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications*, 52 DUKE L.J. 179, 190 (2003) (discussing the legislative history of FISA); *see also* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801–1885(c)(2012)) at 3908 (1978) ("[While] [t]he Federal Government has never enacted legislation to regulate the use of electronic surveillance within the United States for foreign intelligence purposes . . . the Executive Branch and the Congress [recognize] that the statutory rule of law must prevail . . . .").

66. *See* Copeland, *supra* note 46, at 3 (describing FISA as the primary vehicle for surveillance provisions and its purpose); *see also* 50 U.S.C. § 1802(a)(1)(A)(i) (stating what surveillance may be conducted under FISA).

67. *See* 50 U.S.C. § 1801(f) (internal quotations omitted) (defining electronic surveillance allowed under FISA).

68. *See* 50 U.S.C. §§ 1801–1805 (outlining the appropriate procedures for conducting electronic surveillance); *see also* Bedan, *supra* note 17, at 429 (stating that one purpose of FISA is to establish a framework for foreign surveillance); K. A. Taipale, *The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance*, 9 YALE J. L. & TECH. 128, 139 (2007) (describing FISA as a framework for the United States to conduct surveillance).

69. *See* 50 U.S.C. § 1801 (providing the requirements for obtaining a warrant from the FISC); *see also* Forgang, *supra* note 50, at 233 (discussing the creation of FISA and the procedures within it); Copeland, *supra* note 46, at 15 (describing the warrant requirement in FISA).

foreign power, the type of surveillance to be used, and a certification that the information sought is for foreign intelligence purposes.[70]

Under the 2008 Amendments to FISA, Congress clarified the procedures for conducting surveillance on US citizens abroad.[71] Prior to these amendments, Executive Order 12,333 provided the only governance for surveillance of US citizens living outside of the United States.[72] These amendments clarified that the US Government cannot conduct surveillance on a US citizen living outside of the United States without a warrant.[73] Ultimately, the 2008 FISA amendments ensured that US citizens living in the United States and outside of the United States are protected from electronic surveillance conducted by the US Government.[74]

Warrants are not always required for electronic surveillance, however, and FISA provides procedures for the US Executive Branch to conduct warrantless surveillance for up to

---

70. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801–1885(c)(2012)) at 3943 (1978) (providing the procedures to obtain a court order); *see* Bedan, *supra* note 17, at 429–30 (detailing what was required in FISA); *cf.* 50 U.S.C. § 1804 (2012) (describing what is required for warrant approval after the 2008 Amendments).

71. *See* 50 U.S.C. § 1881 (naming additional procedures and changes to FISA); *see also* Forgang, *supra* note 50, at 237–38 (describing the changes made to FISA in 2008); Stephanie Cooper Blum, *What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform*, 18 B.U. PUB. INT. L.J. 269, 297 (2009) (discussing the 2008 FISA Amendments).

72. *See generally* Exec. Order No. 12,333, 3 C.F.R. 200 (1981), *reprinted in* 50 U.S.C. § 401 (1981) (outlining the procedures required for foreign intelligence information collection); *see also* Forgang, *supra* note 50, at 220 n.7 (stating that Executive Order 12,333 was the law concerning surveillance of Americans abroad).

73. *See* 50 U.S.C. § 1881(a) ("[The Government] may not intentionally target a United States person reasonably believed to be located outside the United States"); *see also* Forgang, *supra* note 50, at 236 (describing the changes made to FISA in the 2008 amendments); *see also* Blum, *supra* note 71, at 300 (discussing the changes for US citizens living abroad).

74. *See* 50 U.S.C. § 1881(b)(1)–(3) (providing protections for citizens inside of the United States and outside of the United States); *see also* Forgang, *supra* note 50, at 237 (determining that Congress created a procedure for protecting the privacy of all Americans subject to foreign intelligence surveillance); *see also* Blum, *supra* note 71, at 300 (describing the efforts Congress took to protect citizens through FISA's amendments).

one year.[75] The US Executive's ability to conduct warrantless surveillance is limited by numerous conditions.[76] Included in the conditions is a requirement that warrantless surveillance only be conducted for foreign intelligence information.[77] The targets of warrantless surveillance must be foreign powers or their agents.[78] In addition, there must not be a substantial likelihood that intercepted communications will involve a US citizen.[79]

Although still limited, the ability to conduct warrantless surveillance was expanded by the 2008 FISA amendments.[80] Notably, the amendments allow an agency to conduct surveillance without a warrant while an appeal of a denied warrant application is pending.[81] Therefore, FISA does have some limits on the US Executive's power to conduct electronic surveillance without a warrant.[82]

Outside of the 2008 FISA Amendments, the US Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("the USA PATRIOT ACT"), and further

---

75. *See* 50 U.S.C. § 1802 (explicitly outlining when a President can conduct surveillance without a court order); *see also* Bedan, *supra* note 17, at 430 (reviewing what is required for the President to engage in warrantless surveillance).

76. *See* 50 U.S.C. § 1802(a)(1) (explicitly defining what must be certified under oath); *see also* Bedan, *supra* note 17, at 430 (continuing to review and list out the requirements under oath).

77. *See* 50 U.S.C § 1802(a)(1)(A)(i) (stating that the surveillance can only be conducted against a foreign power); *see also* Bedan, *supra* note 17, at 430 (describing how surveillance can occur against a foreign power).

78. *See* 50 U.S.C § 1802(a)(1)(A)(i); *see also* Bedan, *supra* note 14, at 430 (reviewing the provisions for warrantless surveillance).

79. *See* 50 U.S.C § 1802(a)(1)(A)(i); *see also* Bedan, *supra* note 14, at 430.

80. *See* 50 U.S.C. § 1881(a)(c)(2) (stating, for example, that warrantless surveillance may occur if information important to national security will be lost); *see also* Forgang, *supra* note 50, at 237 (describing warrantless procedures under the amendments); Blum, *supra* note 71, at 299 (explaining the changes made for warrantless searches).

81. *See* 50 U.S.C. § 1881(a)(i)(4)(B) (stating that surveillance may continue during appeal); *see also* Forgang, *supra* note 50, at 238 (noting continuation of surveillance during an appeal if a request is denied); Blum, *supra* note 71, at 304 (indicating that surveillance will continue during appeals of warrant applications).

82. *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801–1885(c)(2012)) at 3910 (1978) ("[FISA is] designed to permit the Government to gather necessary foreign intelligence information by means of electronic surveillance but under limitations and according to procedural guidelines which will better safeguard the rights of individuals."); *see also* Henderson, *supra* note 65, at 190 (reviewing the legislative history of FISA).

expanded FISA.[83] Notably, section 218 of the USA PATRIOT ACT changed the standard under which electronic surveillance may be conducted.[84] Instead of requiring foreign intelligence to be the primary purpose of the search and surveillance, foreign intelligence simply needs to be a "significant purpose".[85] The USA PATRIOT ACT also authorizes the use of roving wiretaps, the ability to secretly surveil email communications, and the expanded duration for which a FISA warrant is valid.[86]

FISA also created the FISC, an Article III special court that reviews warrant applications for foreign electronic surveillance.[87] Originally, the FISC consisted of seven judges who served for eleven-year terms.[88] The FISC judges hail from different federal districts and are appointed by the Chief Justice of the US Supreme Court.[89] Under the USA PATRIOT ACT, changes were

---

83. *See generally* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 *(*USA PATRIOT ACT*),* Pub. L. No. 107–56*,* 115 Stat. 272 (2001) (codified in scattered titles of U.S.C.) *(*changing the requirements for surveillance); *see* Copeland, *supra* note 46, at 18 (discussing how the USA PATRIOT ACT makes significant changes to FISA procedures); Jennifer L. Sullivan, *From "Purpose" to "A 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, 381 (2005) (describing the lower threshold for surveillance approval in the USA PATRIOT ACT).

84. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT ACT), Pub. L. No. 107–56, 115 Stat. 272 (2001) (amending "purpose" to "significant purpose"); Gehan Gunasekara, *The 'Final' Privacy Frontier? Regulating Trans-Border Data Flows*, 15 INT'L J.L. & INFO. TECH. 362, 375 (2007) (noting the changes in section 218).

85. *See supra* note 84 and accompanying text (explaining the changes made to the purpose requirement of FISA).

86. *See* Uniting and Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism Act Of 2001 (USA PATRIOT ACT), Pub. L. No. 107–56, § 206, 115 Stat. 272 (2001) (establishing the use of roving surveillance); *see* Copeland, *supra* note 46, at 19–20 (discussing that roving wiretaps affect terrorists and potentially US citizens); *see also* Henderson, *supra* note 65, at 197 (noting that prior to this change roving wiretaps were only available in the law enforcement context).

87. 50 U.S.C. § 1803 (2012) (establishing the FISC and its internal workings, including the appointment of judges); *see* Henderson, *supra* note 65, at 190–91 (reviewing the creation of the FISC and its structure).

88. *See* § 1803 (noting the appointment of the FISC judges and their terms); *see also* Forgang, *supra* note 50, at 235 (explaining the creation of the FISC and the procedure for choosing judges).

89. *See* § 1803(a)(1) (granting the Chief Justice of the US Supreme Court the ability to appoint judges from different districts to the FISC); *see also* Bloom & Dunn, *supra* note 57, at 161 (describing the original composition of the FISC); *see* Sloan, *supra* note 17, at 1496 (reviewing the structure of the FISC).

made to the FISC including changing the number of the FISC judges from seven to eleven.[90]

The FISC is designed to be a check on the US Executive's power under FISA.[91] Since FISA's inception, however, the FISC has rejected very few applications for warrants.[92] The FISC has allowed applications where the US Government seeks surveillance of a US citizen, and there is probable cause that the US citizen is an agent of a foreign power and suspected of terrorism.[93] Essentially, the FISC only approves applications when the communications do not involve a US citizen, or when there is cause for conducting electronic surveillance against a US citizen.[94]

4. The National Security Agency

The NSA is the "primary" agency responsible for collecting and disseminating signals intelligence information in support of

---

90. *See* Uniting and Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism Act Of 2001 (USA PATRIOT ACT), Pub. L. No. 107–56, § 206, 115 Stat. 272 (2001) (amending provisions of FISA stating that the FISC will have seven judges to eleven judges); 50 U.S.C § 1803(a) (2010) (stating the new composition of the FISC); Copeland, *supra* note 46, at 21 (discussing the changes made to this court including the expansion of the number of judges); *see also* Henderson, *supra* note 65, at 197 (discussing the changes to the FISC after the Patriot Act).

91. *See* Copeland, *supra* note 46, at 15 (describing the procedures in FISA that serve as checks on the President, including the FISC); *see also* S. REP. NO. 95-604, pt. 1 (1977) (describing the internal and external checks on the US Executive).

92. *See* Henderson, *supra* note 65, at 193 (noting that at the time of publication of that note only two warrant applications were rejected since FISA was enacted); *see also* Sloan, *supra* note 17, at 1496 (noting that between 1978 and 1999, the FISC approved 11, 883 applications and denied none).

93. *See* 50 U.S.C. § 1805(a)(2) (requiring probable cause to believe that a person is an agent of a foreign power for a warrant to be approved); *see also* Taipale, *supra* note 68, at 134–35 (noting that surveillance of US citizens can happen when the person is suspected of terrorism); Jonathan W. Gannon, *From Executive Order to Judicial Approval: Tracing the History of Surveillance of U.S. Persons Abroad in Light of Recent Terrorism Investigations*, 6 J. NAT'L SEC. L. & POL'Y 59, 74 (2012) (reviewing FISA's procedures and the probable cause requirement).

94. *See* 50 U.S.C. § 1802(a)(1)(B) ("[T]he President, through the Attorney General, may authorize electronic surveillance without a court order . . . if . . . there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party . . . ."); *see also* Copeland, *supra* note 46, at 16–17 (explaining the express provisions of surveillance in FISA).

US military operations and foreign policy.[95] The NSA's mission is to protect US information systems by preventing access and producing foreign intelligence information.[96] Executive Order 12,333 permits the NSA to disseminate information to authorized government recipients, while prohibiting it from sharing intelligence with private corporations.[97]

When surveillance is conducted outside the United States and US citizens are not involved, then there are few restrictions on the NSA's surveillance activities.[98] That said, any NSA effort to conduct electronic surveillance involving US citizens is subject to the strictures of FISA and Executive Order 12,333.[99]

C. *Privacy and Surveillance in New Zealand*

Part I.C.1 surveys the background of privacy legislation in New Zealand before the Privacy Act of 1993. Part I.C.2 discusses the development of the New Zealand Privacy Act of 1993. Part I.C.3 outlines the history of the GCSB and what laws apply to its actions.

1. Privacy Legislation Prior to 1993

Unlike in the United States, in New Zealand, the recognition of privacy as a legally protected right is a relatively

---

95. *See* Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (1981) (to be codified at 3 C.F.R. pt. 200) ("Establishment and operation of an effective unified organization for signals intelligence activities . . ."); *see also* Bedan, *supra* note 17, at 431 (noting that the NSA was given this "primary responsibility").

96. *See Mission*, NSA http://www.nsa.gov/about/mission/index.shtml (last visited November 10, 2013) (introducing the two parts of NSA cryptology as "Information Assurance" and "Signals Intelligence"); *see also* Brown, *supra* note 12, at 186 (laying out this "twofold mission" of the NSA).

97. *See* Exec. Order No. 12,333, 46 Fed. Reg. 59,941, §2.3 (describing what information can be disseminated and retained by the NSA); *see also* Bedan, *supra* note 17, at 431 (describing the inability of the NSA to share information with private US corporations).

98. *See* Bedan, *supra* note 17, at 431 (noting that neither FISA or Executive Order 12,333 prohibits this kind of conduct); *see also* Brown, *supra* note 12, at 198, (implying that warrants are required for US citizens but that no such requirements exist for non-citizens).

99. *See* Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (regulating the NSA's actions outside of the United States); *see also* 50 U.S.C. 1801 (regulating NSA's activities inside and outside of the United States).

new concept.[100] The New Zealand Bill of Rights of 1990 does not include an express right to privacy.[101] Article 21 of the New Zealand Bill of Rights, however, does protect against unreasonable searches of people, property, and correspondence.[102] Unlike the US Constitution, the New Zealand Bill of Rights cannot be used to preempt or override other legislation.[103] Besides the New Zealand Bill of Rights, the right to privacy is recognized in search and seizure cases and in tort law.[104] Prior to the enactment of the New Zealand Privacy Act of 1993, some legislation restricted access to specific categories of personal information, such as health records.[105]

In 1982, the Official Information Act was passed and granted New Zealanders access to all publicly held information unless there is good reason to withhold.[106] While the Official Information Act was a step towards comprehensive privacy legislation, it only covers the right to access information held by

---

100. *See* Vettoretti & Gunasekara, *supra* note 19, at 287 (noting that with the adoption of the Bill of Rights privacy law is developing); *see also* Cynthia Laberge, *To What Extent Should National Security Interests Override Privacy in a Post 9/11 World?* 1, 17 (3 Victoria U. Wellington Working Paper Ser., 2010) (discussing that New Zealand law regarding privacy is recent).

101. *See generally* Bill of Rights Act 1990 (N.Z.) (listing the rights of New Zealand citizens); *see also* Vettoretti & Gunasekara, *supra* note 19, at 292 (expressing the lack of a privacy provision).

102. *See* Bill of Rights Act 1990, art. 21 (N.Z.) (granting the explicit right to be free from unreasonable search and seizure); *see also* Banisar & Davies, *supra* note 11, at 73 (explaining the rights of Article 21 and privacy of correspondence).

103. *See* Thomas Eichelbaum, *The State of the Courts in New Zealand*, 44 FED. LAW. 29, 30 (1997) (stating that the New Zealand Bill of Rights is not supreme); *see also* David Erdos, *Judicial Culture and the Politicolegal Opportunity Structure: Explaining Bill of Rights Legal Impact in New Zealand*, 34 LAW & SOC. INQUIRY 95, 99 (2009) (affirming that the New Zealand Bill of Rights is not supreme).

104. *See* Sam McMullan, *Third Party Consent Searches Following the Search and Surveillance Act*, 43 VICT. U. WELLINGTON L. REV. 447, 450 (2012) (describing where the reasonable expectation of privacy is found in New Zealand laws and legislation); *see also* Hamed & Others v. R., (2011) NZSC 101 (utilizing the right to privacy in a tort case).

105. *See* Health Act 1956, pt 1 sec 22(C) (N.Z.) (outlining disclosure procedures notably referencing the Privacy Act today); *see also* John M. Howells, *The Privacy Act of 1993: A New Zealand Perspective*, 17 COMP. LAB L.J. 107 (1995) (describing existing legislation before the New Zealand Privacy Act).

106. *See* Official Information Act 1982, pt 1 sec 4 (N.Z.) (granting the right to access of information); *see also* Howells, *supra* note 105, at 108 (outlining the implementation of the Official Information Act).

public organizations.[107] After years of debate, the Privacy Act of 1993 was enacted, providing comprehensive legislation to cover all forms of privacy.[108]

2. New Zealand Privacy Act of 1993

The New Zealand Privacy Act of 1993 codifies the general rules that govern privacy issues in New Zealand.[109] The Privacy Act contains the basic principles relating to the information that is held by public and private registers.[110] In addition, it sets guidelines and procedures for the matching programs run by agencies.[111] A matching program compares the personal information of certain individuals to that of another group of individuals in order to verify information that may be used against an individual.[112]

This Act is structured around twelve privacy principles.[113] The twelve principles are: (1) purpose of collection of personal information; (2) source of personal information; (3) collection of information; (4) manner of collection; (5) storage and security of personal information; (6) access to personal information; (7) correction of personal information; (8)

---

107. *See* Official Information Act 1982, pt 1 sec 2 (N.Z.) (defining official information that can be obtained under the Act); *see also* Howells, *supra* note 105, at 112 (indicating that the Official Information Act only pertained to the public sector).

108. *See* Privacy Act 1993 (N.Z.) (covering all forms of personal information within its regulations).

109. *See* European Commission, Article 29 Data Protection Working Party. 00665/11/EN. WP 182, Adopted on April 4, 2011 (stating that the Privacy Act of 1993 is the main data protection legislation in New Zealand); *see also* Howells, *supra* note 105, at 107 (discussing the background and development of the Privacy Act of 1993).

110. *See* Privacy Act 1993, pt 7 sec 63 (N.Z.) (describing the practice of public registers); *see also* Banisar & Davies, *supra* note 11, at 74 (listing the fact that the Act provides principles relating to information held on public registers).

111. *See* Banisar & Davies, *supra* note 11, at 74 (describing the privacy principles as part of the Act); *see also* Howells, *supra* note 105, at 112 (stating the purpose of the Act and then listing the principles).

112. *See* Privacy Act 1993, pt 10 sec 97 (N.Z.) (defining an information matching program); *see also* Howells, *supra* note 105, at 119 (describing what a matching program is).

113. *See* Privacy Act 1993, pt 1 (N.Z.) (defining the privacy principles in detail); *see also* Gehan Gunasekara & Erin Dillon, *Data Protection Litigation in New Zealand: Processes and Outcomes*, 39 VICT. U. WELLINGTON L. REV. 457, 458 (2008) (mentioning that New Zealand uses twelve principles as well as some comparable States' legislation); Howells, *supra* note 105, at 112 (outlining the twelve principles without explicitly stating that there are twelve).

accuracy of personal information; (9) length of time information can be held; (10) limits on use; (11) limits on disclosure; and (12) unique identifiers.[114] These principles are based on the 1980 Organization for Economic Cooperation and Development ("OECD") guidelines and the information privacy principles in Australia's Privacy Act of 1988.[115] These privacy principles form the core of the New Zealand Privacy Act (the "Privacy Act").[116]

All forms of personal information are protected in the Privacy Act, irrespective of the form that the information is in, or how it was collected.[117] Further, when a foreign agency wants to conduct surveillance in New Zealand, the Privacy Act will apply.[118] Overall, the Privacy Act is about data protection and the collection of personal information.[119]

The Privacy Act also provides for the appointment of a Privacy Commissioner.[120] The Office of the Privacy Commissioner ("the Office") was created in 1991, prior to the enactment of the Privacy Act, which later codified the duties and

---

114. *See supra* note 113 and accompanying text (providing details about the privacy principles and their contents).

115. *See OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,* OECD (2013), http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (suggesting several principles for national application); *see also Privacy Act 1988* (cth.) pt 3 div 2 (Austl.) (outlining the information principles that must be followed for information collection); Banisar & Davies, *supra* note 11, at 73 (discussing the development of the privacy principles); Gunasekara, *supra* note 84, at 367 (discussing the OECD guidelines and stating that New Zealand has similar principles).

116. *See* Vettoretti & Gunasekara, *supra* note 19, at 288 (describing the information privacy principles as the essence of the Privacy Act); *see also* Howells, *supra* note 105, at 113 (noting that the purpose of the Act was to create guidelines and that these principles act as those guidelines).

117. *See* Privacy Act 1993, pt 2 (N.Z.) (stating that, with few exceptions, no personal information may be collected); *see also* Gunasekara, *supra* note 84, at 368–69 (describing the protection of all forms of personal information in New Zealand).

118. *See* Alan Toy, *Cross-Border and Extraterritorial Application of New Zealand Data Protection Laws to Online Activity*, 24 N.Z. U. L. REV. 222, 224 (2010) (noting that an agency in a foreign jurisdiction collecting information on New Zealand citizens still falls under the Privacy Act); *see also* Gunasekara, *supra* note 84, at 383 (explaining the applicability of these provisions to varying situations).

119. *See* Privacy Act 1993, pt 11A s 114A (N.Z.) (indicating that the full title mentions protection of personal data); *see also* Gunasekara & Dillon, *supra* note 113, at 458 (noting that New Zealand's data protection statute is the Privacy Act).

120. *See* Privacy Act 1993, pt 3 ss 12–14 (N.Z.) (identifying the role and functions of the Privacy Commissioner); *see also* Vettoretti & Gunasekara, *supra* note 19, at 287 (discussing the Privacy Commissioner appointment).

appointment of the position.[121] The functions of the Office include promoting the objectives of the Privacy Act and monitoring proposed legislation and government policies.[122] The Office must deal with privacy complaints in the first instance, and approve and issue codes of practice.[123] Additionally, the Office must authorize special exemptions from the information privacy principles, and review public sector information-matching programs.[124]

The Privacy Act also sets up a means of dispute resolution that is outside of the New Zealand court system.[125] A complaint citing a violation of a privacy right protected under the Privacy Act can be filed with the Privacy Commissioner.[126] It is within the discretion of the Privacy Commissioner to investigate the violation once the complaint is filed.[127] Even if an investigation is not undertaken, the Privacy Commissioner can attempt to seek settlement between the parties.[128] The vast majority of privacy disputes are settled this way, avoiding the traditional court system.[129] That said, disputes may be appealed to the New

---

121. *See* Privacy Act 1993, pt 3 s 12 (N.Z.) (codifying the position of the Privacy Commissioner in the Privacy Act)*; see also* Banisar & Davies, *supra* note 11, at 74 (noting that the position was created in a separate act); Howells, *supra* note 105, at 112 (noting the existence of the Privacy Commissioner Act).

122. *See* Banisar & Davies, *supra* note 11, at 74 (explaining the functions of the Privacy Commissioner); *see also* Privacy Act 1993, pt 3 s 13 (N.Z.) (defining the duties and functions of the Privacy Commissioner).

123. *See* Banisar & Davies*, supra* note 11, at 74 (stating that the role of the position involves reviewing complaints and issuing "codes of practice"); Howells, *supra* note 105, at 118 (describing the process for complaint review).

124. *See* Privacy Act 1993, pt 3 sec 13 (N.Z.) (defining the duties and functions of the commissioner); *see also* Banisar & Davies, *supra* note 11, at 75 (explaining the functions of the Privacy Commissioner).

125. *See* Gunasekara & Dillon, *supra* note 113, at 460 (describing the dispute resolution system and procedures); *see* Howells, *supra* note 105, at 116–18 (describing the complaint procedures).

126. *See* Privacy Act 1993, pt 8 s 67 (N.Z.) (stating that complaints may be made to the Privacy Commissioner).

127. *See* Privacy Act 1993, pt 8 ss 70–71 (N.Z.) (granting the Privacy Commissioner the ability to decide to investigate or not to investigate).

128. *See* Privacy Act 1993, pt 8 s 74 (N.Z.) (providing that a settlement can be reached without an investigation).

129. *See* Gunasekara & Dillon, *supra* note 113, at 462 (demonstrating by a review of annual reports that many claims are settled); *see also* Banisar & Davies, *supra* note 11, at 74 (giving an example of the number of complaints received in 1998 and noting the small amount actually getting a final disposition).

Zealand courts, though these courts rarely find that a violation of privacy rights has occurred.[130]

Lastly, the Privacy Act allows for the sharing of information by certain government agencies.[131] The Privacy Act allows for certain agencies in New Zealand to share information amongst them, but places limitations on information transferred outside of New Zealand.[132] The Privacy Commissioner is granted the right to determine whether the transfer of information outside of New Zealand would violate any of the privacy principles.[133]

One agency regulated by the Privacy Act is the New Zealand Security Intelligence Service ("NZSIS"), which is permitted to carry out electronic interceptions of information under the New Zealand Security Intelligence Act of 1969.[134] Founded in 1956, NZSIS is an advisory organization that is charged with "obtaining, correlating, and evaluating" information relevant to New Zealand's national security.[135] The NZSIS is a civilian government agency that primarily collects information within New Zealand.[136] The NZSIS does rely on warrants granted by the Minister to conduct surveillance, but may not obtain a warrant for conducting surveillance on a New Zealand citizen.[137] While

---

130. *See* Privacy Act 1993, pt 83 (N.Z.) (granting individuals the right to bring proceedings before the Human Rights Tribunal); *see also* Gunasekara & Dillon, *supra* note 113, at 463 (stating that some claims are appealed and noting the Tribunal's willingness in only a few instances to find an interference occurred); *see also* Howells, *supra* note 105, at 118 (describing the complaint procedures).

131. *See* Banisar & Davies, *supra* note 11, at 74 (describing the ability of certain agencies to share information); *see also* Privacy Act 1993, pt 9A s 96D (N.Z.) (stating that information agreements may be entered into by approved agencies).

132. *See* Privacy Act 1993, pts 9A 11A (N.Z.) (describing the process for information sharing inside and outside of New Zealand).

133. *See* Privacy Act 1993, pt 11A (N.Z.) (giving the Privacy Commissioner the right to make sure a determination).

134. *See* Banisar & Davies, *supra* note 11, at 75 (describing what the NZSIS may do); *see also NZSIS History*, N.Z. SECRET INTELLIGENCE SERV., http://www.security.govt.nz/about-us/nzsis-history/ (last visited Nov. 9, 2013) (discussing the history of the NZSIS). *See generally* Intelligence Services Act 1969 (N.Z.) (providing for the regulation of the NZSIS).

135. *See* David Collins, *Spies Like Them: The Canadian Security Intelligence Service and Its Place in World Intelligence*, 24 SYDNEY L. REV. 505, 517–19 (2002) (recounting the role of the NZSIS); *see also NZSIS History*, *supra* note 134 (listing the duties of the NZSIS).

136. *See* Collins, *supra* note 135, at 517 (describing the NZSIS as a civilian agency); *see also* Banisar & Davies, *supra* note 11, at 75 (explaining the role of the NZSIS as an intelligence agency).

137. *See* Security Intelligence Services Act 1969, s 4A (N.Z.) (outlining the warrant procedures).

the NZSIS operates as a relatively transparent body, New Zealand operates another intelligence agency, the Government Communications Security Bureau ("GCSB") that has recently come under scrutiny for its activities.[138]

3. The Government Communications Security Bureau

The GCSB created in 1977, is New Zealand's intelligence organization responsible for intercepting foreign communications.[139] The GCSB is subject to New Zealand law; however, specific exemption provisions are contained in legislation, such as the Privacy Act, the Public Finance Act, and the Radio Communications Act.[140] Therefore, the GCSB, unlike the NZSIS, does not have to comply with provisions of the Privacy Act.[141]

In early 2000, the first statutory framework was developed to govern the GCSB's activities, the GCSB Act.[142] In April 2003, the first version of the GCSB Act took effect.[143] The GCSB Act defines the functions of the GCSB—and makes provisions for its administration and the conduct of its operational activities.[144] The original GCSB Act did have a warrant requirement for

---

138. *See supra* notes 3–4 and accompanying text (discussing the backlash that the GCSB has faced); *see also* Collins, *supra* note 135, at 519 & n.85 (comparing the GCSB and the NZSIS, and noting the GCSB's efforts to become less secret since at least 2001).

139. *See* Collins, *supra* note 135, at 519 (describing the role of the GCSB, its location, and creation date); *see also* Banisar & Davies, *supra* note 11, at 75 (noting the location of GCSB stations).

140. *See* GOV'T COMM. SEC. BUREAU, http://www.gcsb.govt.nz [hereinafter GCSB website] (noting the applicability of privacy laws to GCSB); *see also* Privacy Act 1993, pt 6 s 57 (N.Z.) (exempting GCSB from its provisions).

141. *See supra* notes 134, 140 and accompanying text (noting the application of the Privacy Act to the NZSIS but not GCSB).

142. *See* GCSB website, *supra* note 140 (explaining that a statutory footing was needed for the GCSB); *see also* Laberge, *supra* note 100, at 111 (affirming that although the GCSB came into existence in 1977, a statutory framework was not created until 2003).

143. *See* GCSB website, *supra* note 140 (noting the date of enactment for the original version of the GCSB Act); *see also* Government Communications Security Bureau Act 2003 (N.Z.) (listing the date of assent as April 1, 2003).

144. *See* GCSB website, *supra* note 140 (describing the key provisions of the GCSB Act and the functions of the GCSB); *see also* Government Communications Security Bureau Act 2003, pt 1 sec 3 (N.Z.) (describing the general purposes of the GCSB Act).

surveillance; however, the requirement made no mention of New Zealand citizenship as a restriction on surveillance.[145]

The GCSB Act also has provisions that regulate warrantless surveillance.[146] This portion of the Act does not allow for warrantless surveillance to be conducted on New Zealand citizens or residents, allowing this surveillance when a warrant is obtained.[147] However, the GCSB Act does not place restrictions on the warrantless surveillance of non-New Zealanders.[148]

4. Government Communications Security Bureau Act Amendments

In 2013, the New Zealand legislature amended the GCSB Act and clarified the GCSB's limitations, specifically clarifying that warrants are required to conduct surveillance on New Zealand citizens.[149] The GCSB amendments added language that related to the surveillance of New Zealand citizens.[150] Under the amendments, the GCSB can conduct surveillance on a New Zealand citizen or permanent resident, as defined in the GCSB Act with a warrant.[151] Contrary to US laws, these New Zealand

---

145. *See* Government Communications Security Bureau Act 2003, pt 3 sec 15 (N.Z.) (describing the times when a warrant is required without mentioning citizenship); *see also* Government Communications Security Bureau Amendment Act 2013 (N.Z.) (describing the newest version of the GCSB Act's additions including the specific mention of citizenship).

146. *See* Government Communications Security Bureau Act 2003, pt 3 sec 16 (N.Z.) (regulating warrantless surveillance conducted by the GCSB).

147. *See* Government Communications Security Bureau Act 2003, pt 3 sec 15 (N.Z.) (requiring that the GCSB always have a warrant for conducting surveillance on a citizen or resident of New Zealand).

148. *See* Government Communications Security Bureau Act 2003, pt 3 sec 16 (N.Z.) (making no mention of non-citizens in the prohibition of warrantless surveillance section).

149. *See* Government Communications Security Bureau Amendment Act 2013, pt 3 sec 15A–F (N.Z.) (describing the new warrant procedures). *See generally* Telecommunications (Interceptions Capability and Security) Bill 2013 (N.Z.), *available at* http://www.legislation.govt.nz/bill/government/2013/0108/5.0/DLM5177923.html (introducing other legislation at the same time as the new GCSB Act to change the surveillance law landscape in New Zealand).

150. *Cf.* Government Communications Security Bureau Amendment Act 2013, pt 3 sec 15B–C (N.Z) (describing the exceptions for New Zealand citizens), *with* Government Communications Security Bureau Act 2003, pt 3 sec 15 (N.Z.) (citing language that does not create exceptions for New Zealand citizens).

151. *See* § 15B (N.Z.) Government Communications Security Bureau Amendment Act 2013, pt 3 (describing the requirements for surveillance to be conducted on New Zealand citizens).

laws explicitly allow New Zealand authorities to conduct surveillance on New Zealand citizens in prescribed circumstances with a warrant.[152] Although this seems to provide less privacy protection, the ability to conduct surveillance on New Zealand citizens, coupled with the required warrant application process, arguably affords New Zealand citizens better privacy protection than the United States affords its citizens.[153]

Under the GCSB amendments, applications for warrants are made to the New Zealand Minister of Foreign Affairs and the New Zealand Commissioner of Security.[154] The application may be approved if the proposed interception complies with one of GCSB's named functions, the outcome justifies the interception, the outcome is not likely to be achieved by other means, satisfactory arrangements are in place to ensure that nothing beyond what is necessary is done and satisfactory arrangements are in place that the surveillance is reasonable.[155] The Minister can issue a warrant or an authorization subject to conditions that protect the public interest.[156]

Under the New GCSB Act, the New Zealand Government may not intercept the private communications of a New Zealand citizen or permanent resident without a warrant.[157] Just as in the previous version, a warrant is not necessary for the surveillance

---

152. *Compare* Forgang, *supra* note 50, at 224 (noting that surveillance on US citizens is prohibited without a warrant unless the person is an agent of a foreign power), *with* Government Communications Security Bureau Amendment Act 2013, sec 15 (N.Z.) (describing the procedure for obtaining a warrant for surveillance of a New Zealand citizen).

153. *See* Audrey Young, *Key Pledges to Restrict Spy Agency's Probe Rights*, N.Z. HERALD (Aug. 16, 2013 5:30 AM), http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10913063 (describing the Prime Minister's statements that he will restrict warrants); *see also* Audrey Young, *GCSB Bill Passes After Final Reading*, N.Z. HERALD (Aug. 21, 2013 7:49 PM), http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11112152 [hereinafter Young, *GCSB Bill Passes*] (noting that the Prime Minister reiterated that the warrant process has two steps and is about protection).

154. *See* Government Communications Security Bureau Act 2013, pt 3 sec 15E(3) (N.Z.) (stating that an application must be made to the Minister of Foreign Affairs).

155. *See id.*, pt 3 sec 15A(2) (describing the components of an approvable warrant application).

156. *See* i*d.*, pt 3 sec 15A(4) (noting that the Minister may approve any application subject to conditions that are in his view desirable to the public interest).

157. *See id.*, pt 3 sec 16 (noting the requirements for a surveillance to occur without a warrant).

of foreign individuals, with certain limitations.[158] The intercepted communication must be to a foreign person or agency and must contain, or be expected to contain, foreign intelligence.[159]

Further, the GCSB amendments contain a provision that regulates the warrant application and authorization process in urgent situations.[160] This provision applies when the Minister is unavailable to assess a warrant application.[161] The circumstances must make it absolutely necessary for a warrant to be immediately issued.[162] Further, there must be a minimization of effects and reasonable efforts must be taken to prevent the interception of irrelevant communications.[163]

These amendments also clarify the functions of the GCSB.[164] The three main functions of the GCSB are information assurance and cyber security, gathering intelligence related to foreign persons and organizations, and assisting other New Zealand agencies such as the NZSIS.[165] Previously, the goals were stated more broadly without separate subsections and only included gathering intelligence and assisting other agencies.[166]

---

158. *See id.* (describing the limitations for surveillance on foreign individuals).

159. *See* Government Communications Security Bureau Act 2003, pt 3 sec 16 (N.Z.) (providing that the surveillance may occur without a warrant, but "does not authorize anything to be done for the purpose of intercepting the private communications of a New Zealand citizen or permanent resident of New Zealand"); *see also* Government Communications Security Bureau Amendment Act 2013, pt 3 sec 16 (N.Z.) (keeping intact the original provisions relating to warrantless surveillance).

160. *See* Government Communications Security Bureau Amendment Act 2013, pt 3 sec 19A (N.Z.) (describing the process for urgent warrant applications and approval).

161. *See id.* (describing that the Attorney General, Minister of Defense or Minister of Foreign Affairs may then issue a warrant).

162. *See id.* (noting that circumstances must be present such that the approval cannot wait until the Minister returns).

163. *See id.* (noting that practical steps must be taken to ensure a minimization of effects); *see also* Government Communications Security Bureau Act 2003, pt 3 sec 24 (N.Z.) (describing what minimization is required).

164. *See* Government Communications Security Bureau Amendment Act 2013, sec 7 (N.Z.) (noting a complete repeal of sections 7 and 8, and redefines the functions of the GCSB); *see also* Young, *GSCB Bill Passes*, *supra* note 153 (describing the bill and the changes that it makes).

165. *See* Government Communications Security Bureau Amendment Act 2013, sec 7 (N.Z.) (noting the three functions of the GCSB); *see also* Young, *GSCB Bill Passes*, *supra* note 153 (describing the redefined functions of the GCSB).

166. *See* Government Communications Security Bureau Act 2003, pt 2 sec 7 (N.Z.) (describing the major functions of the GCSB).

D. *ECHELON: States Working Together*

While having separate intelligence agencies within their boundaries, the United States and New Zealand also work together when engaging in surveillance, as members of Echelon.[167] Following World War II, the United States and the United Kingdom entered into the UKUSA Agreement, which created a cooperative alliance for international intelligence agencies.[168] In the past, the term Echelon may have been used as a code word to describe the network of computers that processed communications after they were intercepted.[169] Today, Echelon is used generically to describe the system that the UKUSA members use to intercept and share intelligence.[170] The United States originally refused to acknowledge the existence of Echelon, but its existence has been confirmed in certain documents released by the NSA.[171] The European Parliament has similarly released reports confirming Echelon's existence.[172]

---

167. *See* Brown, *supra* note 12, at 187 (listing the five countries that are known members of Echelon); Bedan, *supra* note 17, at 435 (mentioning the countries that are members of Echelon).

168. *See* Early Papers Concerning UK-USA Agreement, 1940–1944, at 1, 7, *available at* http://www.nsa.gov/public_info/_files/ukusa/early_papers_1940-1944.pdf (presenting a clear affirmation that the British Government sought to enter into an information exchange agreement); Lawner, *supra* note 10, at 444 (recognizing that the United States and United Kingdom entered into the agreement following World War II); *see also* Bedan, *supra* note 17, at 435 (noting the formation of the agreement after World War II).

169. *See* Bedan, *supra* note 17, at 436 (suggesting that some evidence points to the idea that Echelon was used as a code word); *see also* Sloan, *supra* note 17, at 1468 (noting that Echelon was a code word for the agreement).

170. *See* Bedan, *supra* note 17, at 436–37 (noting the use of Echelon "generically" to describe the system of computers, satellites and cables that collect intelligence); *see also* Sloan, *supra* note 17, at 1471 (stating that Echelon refers to a system of intelligence collection involving telephones, email and fax).

171. *See* Nat'l Sec. Agency, *UKUSA Agreement Release 1940–1956*, http://www.nsa.gov/public_info/declass/ukusa.shtml (last visited Apr. 2, 2014) (providing access to early drafts of the agreement); *see* Bedan, *supra* note 17, at 436 (stating that the United States has never publicly acknowledged the existence of Echelon although there is "overwhelming evidence" that it exists).

172. *See* European Parliament Report, A5-0264/2001 (reporting on the existence of Echelon and its capabilities); *see also* Lawner, *supra* note 10, at 452–53 (noting that the European Parliament released an official report acknowledging Echelon's existence); Brown, *supra* note 12, at 190 (describing reports that have been released by the European Parliament).

Although the exact numbers are unknown, this global surveillance organization is capable of collecting a vast amount of information.[173] It is a common belief that Echelon intercepts and analyzes nearly three billion communications every day.[174] The exact capabilities of Echelon are unknown, however, because of the classified nature of the program.[175] The system is believed to intercept email, fax, and telephone communications.[176] It links supercomputers throughout the world to accomplish this feat.[177]

In the United States, there is a concern that Echelon allows the NSA to circumvent FISA and other laws to spy on US citizens.[178] This system allows US agencies to receive the information from foreign agencies without questioning, or being involved in, how the information was obtained.[179] On its face, the agreement appears completely legal by US constitutional and statutory standards because information sharing among countries is not regulated.[180] US individuals,

---

173. *See* Bedan, *supra* note 17, at 437 (noting that Echelon's exact "scope of capabilities" is unknown); *see also* Brown, *supra* note 12, at 190 (noting that reports suggest Echelon's ability to collect an "indiscriminately" large amount of information).

174. *See* Bedan, *supra* note 17, at 437 (noting that it is a belief among researchers that Echelon can collect three billion communications a day); *see also* David Alan Jordan, *Decrypting the Fourth Amendment: Warrantless NSA Surveillance and the Enhanced Expectation of Privacy Provided by Encrypted Voice Over Internet Protocol*, 47 B.C. L. REV. 505, 512 (2006) (describing how Echelon collects three billion communications every day).

175. *See* Bedan, *supra* note 17, at 437 (noting that the exact capabilities are unknown); *see also* Jordan, *supra* note 174, at 512 (noting that Echelon is only rumored to collect three billion communications per day).

176. *See* Brown, *supra* note 12, at 185 (listing the types of telecommunications Echelon intercepts); *see also* Elizabeth Sepper, *Democracy, Human Rights, and Intelligence Sharing*, 46 TEX. INT'L L.J. 151, 173 (2011) (noting the types of communications collected).

177. *See* Lawner, *supra* note 10, at 453 (describing the network of linked computers); *see also* Bedan, *supra* note 17, at 438 (noting that supercomputers are linked at around twenty bases throughout the world).

178. *See* Bedan, *supra* note 17, at 439 (noting the possibility of using NSA resources for Echelon's use); *cf.* Brown, *supra* note 12, at 200 (stating that Echelon may appear to act illegally but actually works within a legal framework).

179. *See* Bedan, *supra* note 17, at 439 (noting that US law allows for agencies to accept information from foreign agencies regardless of how it was obtained); *cf.* Brown, *supra* note 12, at 192 (arguing that once the information is in the United States it must comply with established law).

180. *Compare* Brown, *supra* note 12, at 200 (reviewing applicable legal standards and concluding that Echelon meets those standards), *with* Lawner, *supra* note 10, at 480 (stating that Echelon infringes on rights).

therefore, have less privacy when information is transferred among countries.[181]

II. *AMBIGUITIES, NEW LEGISLATION, AND SOLUTIONS*

In Part II, this Note will compare the changes in surveillance law in New Zealand and the United States, as well as each country's recognition of Echelon. Part II.A will review the loopholes in current US surveillance law, with particular emphasis on the loopholes created by FISA. Part II.B will compare the current state of US law to the recent amendments to New Zealand's GCSB Act. Specifically, Part II.B analyzes the Government Communications Security Bureau Act Amendments. Thus, this Part of the Note identifies and compares the problems in today's surveillance law in two countries with storied histories of surveillance.

A. *The United States under FISA and Its Drawbacks*

In the United States, the current state of surveillance law is a product of FISA, its amendments, and its strictures. An evaluation of US surveillance law proves that inherent loopholes undercut FISA's protections, which allows the US Government to circumvent privacy protections.[182] The main problems are the insufficient definition of surveillance, the ability to spy on agents of foreign powers, the lack of protection against third party surveillance, and the ability to collect incidental information.[183]

First, a significant loophole arises in the interpretation of the term "surveillance."[184] In order for information collection to

---

181. *See* Toy, *supra* note 118, at 234 (noting that individuals have a harder time exercising privacy rights when information is transferred abroad). *See generally* Bedan, *supra* note 17 (arguing that Echelon does not protect rights).

182. *See* Bedan, *supra* note 17, at 433 (reviewing the ambiguities and loopholes in FISA); *see also FISA: A Law with Many Loopholes*, WALL ST. J., June 7, 2013, http://blogs.wsj.com/law/2013/06/07/fisa-a-law-with-many-loopholes/ (describing the main loopholes of FISA).

183. *See infra* notes 184, 188, 191, 195, 196 and accompanying text (outlining separate problems with FISA).

184. *See* Bedan, *supra* note 17, at 433 (describing the definition of surveillance as falling into FISA's loopholes); William F. Brown & Americo R. Cinquegrana, *Warrantless Physical Searches for Foreign Intelligence Purposes: Executive Order 12,333 and the Fourth Amendment*, 35 CATH. U. L. REV. 97, 157, 164 (1985) (describing definitions to be key in FISA).

be regulated by FISA, it must fall under FISA's definition of surveillance.[185] This definition does not apply to certain National Security Letters, which are secret authorizations for the Federal Bureau of Investigation ("FBI") to obtain records from telephone companies, credit agencies, and other organizations if they merely certify that the information is relevant to an international terrorism investigation.[186] National Security Letters are regularly used to circumvent FISA's warrant procedures.[187]

Additionally, FISA's definition of surveillance is antiquated because it distinguishes between data acquired inside of the United States and outside of the United States.[188] This distinction allows the NSA to process surveillance that is received from other countries irrespective of whether the target is a US citizen.[189] Therefore, the NSA is unrestrained when a communication is not physically intercepted within the United States.[190]

Second, an issue arises when US citizens are construed to be agents of foreign powers under FISA because a warrant can be issued to engage in surveillance against them.[191] According to

---

185. *See* Bedan, *supra* note 17, at 433 (noting that if FISA is not implicated then the government may conduct surveillance in whatever way it wishes); *see also* Bloom & Dunn, *supra* note 57, at 164 (reviewing the definition of "agent" and how someone can fall within that definition).

186. *See* Richards, *supra* note 10, at 1942 (clarifying the nature of National Security Letters); *see also* Bedan, *supra* note 17, at 433 (noting the exclusion of certain letters from FISA); *see also* Andrew P. MacArthur, *The NSA Phone Call Database: The Problematic Acquisition and Mining of Call Records in the United States, Canada, the United Kingdom, and Australia*, 17 DUKE J. COMP. & INT'L L. 441, 449–50 (2007) (defining National Security Letters and what information can be obtained as an alternative to FISA).

187. *See supra* note 186 and accompanying text (describing how National Security Letters are used to get around FISA's provisions).

188. *See* Bedan, *supra* note 17, at 434 (noting the distinction between surveillance conducted inside the United States versus outside); *see also* Sloan, *supra* note 17, at 1501 (noting that FISA does not apply when surveillance is conducted outside of the United States).

189. *See* Brown, *supra* note 12, at 199 (describing how the NSA may receive information from other Echelon members); *see also* Sepper, *supra* note 176, at 173 (stating that reports suggest that Echelon members use the system to exchange information about their citizens).

190. *See* Bedan, *supra* note 17, at 434 (describing the situations that are not protected by FISA). *See generally* Forgang, *supra* note 50 (debating whether there is real protection for US citizens living abroad and FISA's shortcomings).

191. *See* Copeland, *supra* note 46, at 18 (labeling the definition of an agent of a foreign power as a "subtle exception" to FISA's procedures); *see also* Blum, *supra* note

FISA's procedures, the only way to spy on a US citizen is when they can be considered to be an agent of a foreign power, or engaged in information gathering, aiding, or abetting a foreign power.[192] However, this limitation does not result in total privacy protection because it only requires probable cause that a person is an agent of a foreign power, not that a crime is being committed.[193] The effect of this ability is that the US Government can conduct surveillance on a US citizen with no ties to terrorism such as a suburban mother telling her friend that her son "bombed" a school play.[194]

Furthermore, FISA is limited to protecting against surveillance by the US Government; it does not create a reasonable expectation of privacy for individuals from surveillance by a third party.[195] This rule is exploited by the United States' participation in Echelon.[196] Because US law generally does not regulate information sharing, the United States essentially violates the privacy rights of US citizens by accepting information from foreign intelligence agencies about potential threats involving US citizens.[197] Thus, the lack of

---

71, at 276 (describing what is required for a person to be considered to be an agent of a foreign power).

192. *See* 50 U.S.C. § 1801 (2012) (defining an agent of a foreign power); *see also* Brown, *supra* note 12, at 198 (describing when surveillance can be conducted on a United States citizen).

193. *See* Blum, *supra* note 71, at 291 (analyzing the probable cause requirement for determining when a citizen is an agent of a foreign power); *see also* Copeland, *supra* note 46, at, 27 (noting that the definition of agent of a foreign power combined with other factors creates the ability for average citizens to be spied on).

194. *See* 50 U.S.C. § 1801(b)(2) (defining an agent of a foreign power in a way that that allows for the inclusion of a US citizen within the definition); *see* Copeland, *supra* note 46, at 27 (noting that through the ambiguities in the definition of an agent of foreign power and the fact that the definition does not always rule out the US citizens from the definition, surveillance can occur on them); *see also Ex-Snoop Confirms Echelon Network*, CBS NEWS, Feb. 24, 2000, http://www.cbsnews.com/news/ex-snoop-confirms-echelon-network (retelling a story from a former spy about a mother who was listed as a possible terrorist because she said her son "bombed" a school play over the phone).

195. *See* United States v. Miller, 425 U.S. 435, 440–42 (1976) (deciding that there is no reasonable expectation of privacy for information revealed to a third party); *see also* Bedan, *supra* note 17, at 433 (reviewing the problems created by the lack of protection from surveillance by third parties).

196. *See supra* note 168 and accompanying text (demonstrating the United States' participation in Echelon).

197. *See* Bedan, *supra* note 17, at 439, 444 (describing how a country can spy on US citizens and once a threat is discovered can give the United States that information

privacy rights when US citizens are spied on by agencies outside of the United States creates a loophole for spying on US citizens without the government restrictions created by existing law.[198]

Lastly, US law allows for the collection of incidental information.[199] It is predicted that Echelon collects nearly all communications, many of which can be considered incidental.[200] Therefore, the fact that FISA allows for the collection of incidental information suggests that privacy rights can be violated by its involvement in Echelon.[201]

B. *New Zealand: Impact of Recent Legislation*

In New Zealand, the government defends the GCSB amendments, amid criticism that it promotes the "wholesale spying" on citizens.[202] Opponents of these amendments argue that they are merely the product of major events in the international community, namely the surveillance practices in the United States.[203] A recent poll has found that the majority of

---

without FISA being implicated); *see also* Richards, *supra* note 10, at 1959 (stating that democratic societies should not allow secret surveillance).

198. *See* Sloan, *supra* note 17, at 1505 (stating that the concept of incidental information should be reevaluated to determine whether it is still limited); *see also* Bedan, *supra* note 17, at 434 (noting the problems faced when information is held by third parties).

199. *See* United States v. Bin Laden, 126 F. Supp. 2d 264, 279 (S.D.N.Y. 2000), *aff'd sub nom*, In re Terrorist Bombings of U.S. Embassies in E. Africa, 552 F.3d 157 (2d Cir. 2008) (allowing for the incidental collection of information of a person who was not a target of surveillance); *see also* Brown, *supra* note 12, at 192 (noting that incidental information about US citizens "may be retained and disseminated if the communication is in regard to foreign intelligence or counterintelligence").

200. *See* Sloan, *supra* note 17, at 1503 (discussing the incidental acquisition of information by Echelon); *see also* Brown, *supra* note 12, at 192.

201. *See* Sloan, *supra* note 17, at 1505 (stating that the concept of incidental information should be reevaluated to determine whether it is still limited); *see also* Bedan, *supra* note 17, at 434 (noting the problems faced when information is held by third parties).

202. *See New Zealand Extends Domestic Spying Power,* BBC ASIA (Aug. 21, 2013 6:49 PM), http://www.bbc.co.uk/news/world-asia-23769206 (quoting the Prime Minister as stating that the law is not about wholesale spying); *see also New Zealand Passes Law Allowing Domestic Spying*, AGENCE FR. PRESSE (Aug. 22, 2013), *available at* http://www.abc.net.au/news/2013-08-21/new-zealand-passes-spy-bill/4903500 (citing the Prime Ministers statements that the bill is not about wholesale spying).

203. *See* Lee Jae-Won, *New Zealand Rights Group Blasts New Law Extending surveillance powers*, REUTERS (Aug. 22, 2013, 3:48 AM), http://www.reuters.com/article/2013/08/22/us-newzealand-security-idUSBRE97L09S20130822 (stating that New Zealand is buying into the surveillance society being created); *see also* Rodney

New Zealanders are concerned about this new law because it looks like a means for unrestricted spying inside and outside of New Zealand.[204] The Prime Minister in New Zealand, however, has publically lauded the amendments for creating a technically stricter and more proactive oversight regime than that in place prior to the Kim Dotcom scandal.[205] Further, supporters suggest that the GCSB is undertaking important activities to protect the safety of this country despite the potential overreach of these amendments.[206] The amendments make it clear that no surveillance may occur on citizens without a warrant.[207]

Similar to the NSA in the United States, the GCSB is not restricted from engaging in information sharing.[208] The GCSB is free to give information to agencies outside of New Zealand with no repercussion.[209] Although New Zealand has a warrant requirement in place to conduct surveillance on citizens, the GCSB can get information from other agencies.[210]

Even with the new amendments, New Zealand also remains a member of Echelon.[211] New Zealand directly acknowledges a

---

Harrison, *Wholesale Spy Power is Precisely What GCSB Bill Means for Kiwis,* N.Z. HERALD (Aug. 17, 2013, 5:30 AM), http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10913479 (describing the new bill as creating a total surveillance state).

204. *See New Zealand Passes Law Allowing Domestic Spying, supra* note 202 (noting a poll in which the majority of those polled were concerned about the changes); *see also* Isaac Davidson, *Three-quarters of Kiwis Concerned about GCSB Bill,* N.Z. HERALD (Aug. 21, 2013, 1:54 PM), http://www.nzherald.co.nz/nz/news/article. cfm?c_id=1&objectid=11112107 (describing that a majority of those polled were at least somewhat concerned about the new law).

205. *See* Quilliam, *supra* note 3 (noting when the law was passed); *New Zealand Spying Law Passes Allowing Surveillance on Citizens*, AGENCE FR. PRESSE, Aug. 21, 2013, *available at* http://www.huffingtonpost.com/2013/08/21/new-zealand-spying-law_n_3789041.html (describing the illegal government spying on Kim Dotcom).

206. *See New Zealand Passes Law Allowing Domestic Spying, supra* note 2032 (noting that the Prime Minister thinks that the law is necessary because of the real and ever present threats to New Zealand); *see also GCSB Bill Becomes Law,* 3 NEWS (Aug. 21, 2013), http://www.3news.co.nz/GCSB-Bill-becomes-law/tabid/1607/articleID/310009/.aspx (describing the necessity of the law because the Prime Minister has encountered numerous risks to New Zealand's security).

207. *See* Government Communications Security Bureau Amendment Act 2013, sec 16 (N.Z.) (stating that no surveillance may occur on a citizen without a warrant).

208. *See* Privacy Act 1993, secs 11A, X (N.Z.) (prohibiting certain agencies from engaging in information sharing and exempting the GCSB).

209. *See id.* (expressing no limitation on the GCSB for sharing information).

210. *See id.* (lacking a prohibition on this type of activity).

211. *See* Nathan Smith, *The World of Signals Intelligence and GCSB in Context,* NAT'L BUS. REV., http://www.nbr.co.nz/article/world-signals-intelligence-and-gcsb-context-ns-

relationship with its UKUSA allies on its GCSB website.[212] In addition to the website, a 1996 book written by a New Zealand investigative journalist provided extensive details about Echelon and New Zealand's involvement in the program.[213] The new law makes no mention or change to New Zealand's ability to participate in Echelon or its effect on foreign and domestic surveillance in this country.[214]

Therefore, the United States and New Zealand each have ambiguities and loopholes in their surveillance law. The United States and New Zealand are both members of Echelon and can circumvent their laws by sharing information with other countries. The question turns to whether these problems can be fixed.

III. *PROPOSED RESOLUTIONS AND THEIR POTENTIAL EFFICACY*

Part III reviews and critiques solutions proposed to resolve some of the issues surrounding surveillance law. This Part argues that as long as secret surveillance programs exist, new warrant requirements are simply not enough to protect the rights of citizens. Part III.A explores the various proposals for controlling international surveillance. The solutions are also analyzed for their viability. Part III.B argues that both the United States and New Zealand surveillance law systems are problematic. Overall, Part III demonstrates that irrespective of how the surveillance policy is framed, be it through public acknowledgement or public denial of a surveillance program, the violations to public policy that are created by membership in secret international programs create problems that cannot be easily solved by

---

129503 (last visited Apr. 2, 2014) (describing the ability of Echelon members to exchange information). *See generally* Government Communications Security Bureau Amendment Act 2013 (N.Z.) (making no mention of the GCSB's involvement with Echelon).

212. *See* GCSB website, *supra* note 140 (describing GCSB's relationship with the UKUSA allies under the "About Us" tab).

213. *See* NICKY HAGER, SECRET POWER, NEW ZEALAND'S ROLE IN THE INTERNATIONAL SPY NETWORK (1996); Bedan, *supra* note 17, at 436 (noting that the book exposed New Zealand's involvement and Echelon generally); *see also* Sepper, *supra* note 176, at 162 (describing Nicky Hager's book).

214. *See supra* notes 211–13 and accompanying text (describing New Zealand's involvement in Echelon).

adhering to either the United States' or New Zealand's methodology.

A. *Proposed Solutions to Control the Threats Posed by Surveillance and Why They Will Not Work*

Various solutions have been proposed to quell the debate surrounding surveillance and better protect privacy rights.[215] First, an international treaty that creates cross-border oversight of electronic surveillance could be implemented.[216] Second, the proposed eradication of secret agencies would allow courts to review agency actions and reduce fear of surreptitious spying.[217] These potential solutions will not strike the appropriate balance between privacy and national security in the international community, specifically in the United States and New Zealand.[218]

It is possible that a binding international treaty could be formed to protect information privacy.[219] The European Directives regulating privacy could be used as guidance, notably the requirement that third parties have adequate protection before receiving or sending information.[220] An opt-in provision has been proposed for an international treaty that would ensure that individuals know that their information is collected before action is taken.[221]

---

215. *See* Gunasekara, *supra* note 84, at 391 (reviewing potential international solutions); *see also* Sepper, *supra* note 176, at 202 (suggesting implementation of a better law enforcement network); *see also* Henderson, *supra* note 65, at 208 (describing how the courts could act as a better check on the executive's power in the United States).

216. *See* Gunasekara, supra note 84, at 392 (describing an international solution); *see also* Wade, *supra* note 22, at 676 (proposing a treaty for data protection).

217. *See* Richards, *supra* note 10, at 1959 (stating the problems with secret surveillance). *But see* Sloan, *supra* note 17, at 1510 (stating that systems like Echelon are necessary to protect against threats).

218. *See infra* Part III.B (describing the problems with New Zealand and the United States' surveillance systems).

219. *See supra* note 216 and accompanying text (explaining that there is no reason to believe that an international treaty could not be implemented).

220. *See supra* notes 30–31 and accompanying text (discussing EU directives and the ability to regulate third parties).

221. *See* Wade, *supra* note 22, at 679 (discussing a potential opt-in provision for individuals); *see also* Steven R. Salbu, *Regulation of Borderless High-Technology Economies: Managing Spillover Effects*, 3 CHI. J. INT'L L. 137, 137 (2002) (stating that opt-in rules can create a default presumption of data privacy).

There are notable problems with the implementation of an international treaty. Before a treaty could be agreed upon, agreement about how the right to privacy is recognized would need to occur.[222] There are many definitions of privacy and finding a universally agreed upon definition may prove impossible.[223] Different States protect these rights in quite distinct ways.[224] An international treaty, furthermore, must account for the different ways that surveillance is conducted in countries in order for a treaty to be applicable to each state.[225] The creation of an international treaty, in other words, requires not merely an agreement upon one definitive interpretation of privacy, but also necessitates determining what the appropriate level of surveillance is, such that privacy is maintained while national security interests are protected.[226] The viability of an international privacy treaty will turn on whether or not it can be enforced, an action that will prove difficult because there is no overarching system to enforce treaties.[227]

Regarding the United States and New Zealand, past experiences with international conventions regarding privacy rights demonstrates that the United States is reluctant to join the international community in achieving this balance.[228] Notably, the United States has never ratified the Optional Protocol to the ICCPR, which is an attempt by the international community to enforce privacy law, and New Zealand waited over

---

222. *See supra* note 20 and accompanying text (explaining the lack of one agreed upon definition for privacy).

223. *See supra* note 21 and accompanying text (stating that privacy is a complex value and it may not be possible to resolve debates around its definition).

224. *See supra* Part I (reviewing the United Nations' understanding of an explicit right to privacy, the United States' implicit right to privacy, and New Zealand's Bill of Rights establishing a right to privacy).

225. *See supra* Part I.B–.C (explaining the ways that the United States and New Zealand protect privacy in clearly different ways); *see also* Wade, *supra* note 22, at 679 (explaining that the goal a privacy protection treaty should be to balance interests).

226. *See supra* note 20 and accompanying text (describing the lack of a universal definition of privacy).

227. *See UN 2010 Treaty Event, Towards Universal Participation and Implementation* (2010), https://treaties.un.org/doc/source/events/2010/Press_kit/fact_sheet_5_english.pdf ("There is no over-arching compulsory judicial system or coercive penal system to address breaches of the provisions set out in treaties or to settle disputes.").

228. *See supra* note 25 and accompanying text (declaring that the United States has not signed the Optional Protocol to the ICCPR).

twenty years after it came into force to ratify it.[229] Furthermore, an international treaty cannot regulate agencies that are not known to the public.[230]

A second proposed solution would eliminate the ability for countries to run secret agencies.[231] When programs are public or known, a court can review the legality of their plans without question.[232] The opacity and deniability under which these networks operate insulate each intelligence agency from criticism and oversight.[233] Agencies have worked together for a long time, sharing information and coordinating operations to address surveillance problems.[234] When nations work together, there is a danger that the interests of one or more states may be detrimentally affected because not all state interests are adequately protected.[235] Any attempt to completely eradicate secret surveillance agencies would be significantly challenging.[236] It is exceptionally difficult to eliminate a program whose existence is unknown.[237] Sanctions could be imposed on countries that violate privacy rights, but is that enough to deter a

---

229. *See supra* notes 25–26 and accompanying text (discussing the United States and New Zealand's treatment of the Optional Protocol).

230. *See supra* notes 175–77 and accompanying text (explaining that, due to the covert nature of Echelon, its capabilities are unknown); *see also* Richards, *supra* note 10, at 1934 (describing how a secret program cannot be reviewed until made public).

231. *See supra* note 217 and accompanying text (introducing the idea that secret programs must not be allowed).

232. *See* Richards, *supra* note 10, at 1959 (stating that only when something is public can the court review it); *see also* Sepper, *supra* note 176, at 169 (describing the lack of democratic oversight for the secrete programs).

233. *See* Sepper, *supra* note 176, at 168 (identifying the ease of the agencies to deny their actions); *see also* Bedan, *supra* note 17, at 440 (noting the claim that Echelon is used to spy on citizens and the NSA may not control all information that is disseminated).

234. *See supra* note 168 and accompanying text (explaining that Echelon was founded after World War II which ended almost seventy years before the time this Note was written).

235. *See* Sepper, *supra* note 177, at 172 (noting that liberties of some nations are detrimentally affected by countries sharing information); *cf.* Brown, *supra* note 12, at 199 (describing how a secret agency like Echelon can fall within legal bounds because the participants do not conduct surveillance on their own citizens).

236. *See supra* note 227 and accompanying text (describing the difficulty inherent in implementing treaties).

237. *See supra* note 232 and accompanying text (stating how difficult it is to review agencies whose existence is unknown).

country from trying to protect its national security interests?[238] If countries were forced to eliminate these programs, they would have to handle even more court review of, public inquiry into, and international scrutiny concerning their surveillance programs than already occurs, threatening their efforts to maintain security within their borders.[239]

B. *Why the US and New Zealand Surveillance Systems are Problematic*

The surveillance laws currently in force in the United States and New Zealand are riddled with ambiguous language and various loopholes enabling exploitation of intended protections.[240] To some extent, each country allows its surveillance agencies to spy on its citizens.[241] The main difference between the two countries is that the United States publically denies that the US Government conducts surveillance of its citizens, denying warrants for surveillance against these individuals though they may be spied on regardless of this pronouncement.[242] Contrarily, New Zealand blatantly allows warrants to be obtained for surveillance against citizens.[243] These seemingly opposite structures have the same result—citizens of each country are the object of government surveillance and privacy intrusions.[244]

The United States and New Zealand are also known members of Echelon, the secret surveillance program created after World War II.[245] Echelon provides a loophole through

---

238. *See supra* note 35 and accompanying text (stating that the European Court of Human Rights places sanctions on states that violate their laws).

239. *See supra* notes 4, 5, 9 and accompanying text (explaining the international scrutiny that the United States and New Zealand currently face as well as an example of a Court review of surveillance).

240. *See supra* Part II.A–.B (reviewing the potential ambiguities and loopholes in US and New Zealand law).

241. *See* Part II.A–.B (discussing the ability of each country to collect information on their citizens).

242. *See supra* Part I.B–.C (describing the surveillance law in New Zealand and the United States).

243. *See* Part I.B–.C (noting that the United States does not allow warrants to be approved for surveillance on citizens, whereas New Zealand does).

244. *See supra* Introduction (showing evidence that the United States and New Zealand spy on their citizens).

245. *See supra* note 168 and accompanying text (recognizing when the agreement was formed).

which each country can avert its own surveillance law framework, specifically the warrant requirement.[246] Further, the warrant requirement in each nation is undercut by the ability to engage in information sharing.[247] Neither the NSA nor the GSCB is prohibited from sharing information with or receiving information from outside agencies.[248] Therefore, even strict warrant requirements for surveillance on citizens will not prevent an agency from getting information about citizens.[249]

The above distinction further highlights the similar problems that these two countries face even while on the surface their surveillance structures may appear quite dissimilar.[250] Echelon allows the United States, whose law does not allow for approval of warrants to conduct surveillance on its citizens, to work with other countries to gain information.[251] Further, the recent amendments in New Zealand to the GCSB were enacted with the intention of enhancing transparency of the GCSB's actions.[252] By maintaining a membership in Echelon, New Zealand is diminishing its transparency by engaging in secret intelligence gathering with other countries.[253] As threats of international terrorism continue to prevail, it is unlikely that either country will willingly abstain from participating in this international surveillance agency.[254]

---

246. *See supra* Part II (outlining the problems caused by Echelon in the United States and New Zealand).

247. *See supra* notes 180, 227 and accompanying text (noting that the NSA and GCSB are allowed to engage in information sharing).

248. *See supra* notes 180, 227 and accompanying text.

249. *See supra* notes 180, 227 and accompanying text (describing how information sharing works outside of the established surveillance system).

250. *See supra* Part I.B–.C (recognizing the differences between the United States and New Zealand).

251. *See supra* note 179 (establishing that Echelon allows the United States' Government to circumvent established procedures).

252. *See supra* note 204 and accompanying text (noting that the Prime Minister has lauded the amendments as creating a more proactive structure).

253. *See supra* notes 211–13 and accompanying text (describing New Zealand's relationship with Echelon).

254. *See supra note* 167 and accompanying text (listed New Zealand and the United States).

CONCLUSION

The United States and New Zealand have comprehensive legislation concerning privacy and surveillance. Although the scope of surveillance deemed legal differs between the countries, both require warrants to protect their citizens against unwarranted searches. Despite these protections, each country's laws are effectively circumvented at times through information obtained from international surveillance affiliates, and other legal loopholes. Both the United States and New Zealand are members of Echelon, and, thus, may circumvent their domestic laws. Therefore, overarching international protection of these rights—the systems in place in the United States and New Zealand—although different, offer the same amount of protection to citizens from surveillance: little to none.