

THE CORRELATION BETWEEN WIRETAPPING AND TERRORISM: A COMPARATIVE ANALYSIS OF AMERICAN AND EUROPEAN SOCIETAL VIEWS ON GOVERNMENT SURVEILLANCE

Lora A. Esau^{*}

I.	INTRODUCTION.....	55
II.	LAWS AND EVENTS IN DIFFERENT COUNTRIES.....	56
	<i>A. The United States</i>	56
	<i>B. European Countries</i>	62
	1. Russia.....	62
	2. Italy.....	64
	3. France.....	66
III.	COMPARATIVE ANALYSIS OF LAW.....	68
	<i>A. Differences</i>	68
	<i>B. Similarities</i>	69
IV.	SOCIETY’S VIEW AROUND THE GLOBE.....	70
	<i>A. The United States</i>	70
	<i>B. European Countries</i>	72
	<i>C. Comparison of Views</i>	73
V.	CONCLUSION.....	74

I. INTRODUCTION

As the former Federal Bureau of Investigation (FBI) Director Louis Freeh once said, “[a]sk the American public if they want an FBI wiretap and they’ll say, ‘No’. If you ask them do they want a feature on their phone that helps the FBI find their missing child they’ll say, ‘Yes’.”¹ According to reports, 2014 was the deadliest year of the twenty-first century as it pertained to deaths from a direct result of terrorism with a total of 32,658 deaths; an increase of eighty percent from 2013.² Wiretapping is defined as, “a form of electronic eavesdropping accomplished by seizing or

^{*} Lora Esau is a second year law student at Nova Southeastern University Shepard Broad College of Law. Lora graduated in 2014 from Florida Atlantic University where she received her Bachelor of Arts in Criminal Justice.

1. *Quote from Louis Freeh*, LIBERTY-TREE.CA, http://quotes.liberty-tree.ca/quote_blog/Louis.Freeh.Quote.4006 (last visited on Sept. 23, 2016) [hereinafter *Louis Freeh*].

2. Daniel Costa-Roberts, *4 surprising facts from the 2015 Global Terrorism Index*, PBS.ORG (Nov. 23, 2015, 2:30 PM), <http://www.pbs.org/newshour/rundown/4-surprising-facts-from-the-2015-global-terrorism-index/>.

overhearing communications by means of a concealed recording or listening device connected to the transmission line.”³ Wiretapping is one of the many tools used to conduct surveillance. This surveillance is conducted domestically, as well as internationally; therefore, a citizen of a specific country is not warranted from that country eavesdropping on his or her conversations.⁴

Terrorism has increased, and has continued to do so over the last fifteen years. Patterns have shown, that when tragedies occur, more domestic and international surveillance occurs. Some of this surveillance is conducted through wiretapping. Although there are laws in place for wiretapping, the laws are not strict enough and tend to infringe on the privacy of many individuals living within that country.

This article will focus on raising awareness and attention to domestic surveillance, specifically wiretapping, the ease of obtaining a warrant for such surveillance, as well as how the United States’ laws and frequent wiretapping compare to other countries in Europe especially during times of terror.

First, this article will give a brief overview of the structure of the United States government, followed by an explanation of the laws used and procedures in place to allow wiretapping. Next, this article will contain background information about the structure of the three European countries’ type of government—Russia, Italy, and France—followed by an explanation of the laws and procedures in place for wiretapping to occur. Additionally, this article will compare the four countries and applicable laws, and discuss the correlation between terrorism occurrences and domestic surveillance, with a focus on wiretapping. Then, this article will discuss society’s opinion regarding whether they agree or disagree with the government watching them. This article concludes with a brief recap of the information shared on wiretapping and changes that should be made to the wiretapping laws and domestic surveillance as a whole.

II. LAWS AND EVENTS IN DIFFERENT COUNTRIES

A. *The United States*

The most alarming statistic released from the United States Courts in 2015 stated, “[n]o wiretap applications were reported as denied in 2015.”⁵

3. THE FREE DICTIONARY, <http://legal-dictionary.thefreedictionary.com/Wiretapping> (last visited Sept. 23, 2016).

4. *How the NSA’s Domestic Spying Program Works*, EFF.COM, <https://www.eff.org/nsa-spying/how-it-works> (last visited Sept. 23, 2016).

5. *Wiretap Report 2015*, U.S. CTS. (Dec. 31, 2015), <http://www.uscourts.gov/statistics-reports/wiretap-report-2015>.

This statistic is alarming because it shows that it is extremely easy to obtain a warrant to wiretap and that judges generally will not deny such request.

Wiretapping in the United States began in 1857 when the telegraph was invented, and furthered upon the invention of the telephone.⁶

The United States is a federal presidential republic.⁷ As such, the powers of the federal government are limited, therefore allowing the states to retain a degree of sovereignty, and giving the citizens the power to vote and choose the individuals that will represent their government.⁸ The Congress is a bicameral legislature, thus dividing the legislators into two branches or houses—the Senate and the House of Representatives—and giving each state the same number of seats regardless of population to ensure equal representation in Congress of the smaller less-populated states.⁹ The legislative branch enacts legislation and the executive branch is charged with enforcing the law and carrying it out.¹⁰ The President of the United States is the head of the executive branch.¹¹ This article was written during the final days of President Barack Obama’s second and last term.

In January of 2016, the estimated population in the United States was 322,762,018.¹² While there may not have been nearly as many people living in the United States when wiretapping first began, by 1934, Congress realized it was time to pass the first federal wiretapping law upon rise of multiple challenges pertaining to the admissibility of wiretap evidence as being violations of the Fourth Amendment.¹³ The Fourth Amendment establishes:

[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon

6. Howard J. Kaplan et al., *The History and Law of Wiretapping*, A.B.A. SEC. OF LITIG. 1, 2 (2012), http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/sac_2012/29-1_history_and_law_of_wiretapping.authcheckdam.pdf.

7. *The World Factbook*, C.I.A., <https://www.cia.gov/library/publications/the-world-factbook/docs/notesanddefs.html?fieldkey=2128&term=Government%20type> (last visited Sept. 23, 2016).

8. *Id.*

9. *Senate Legislative Process*, SENATE.GOV, http://www.senate.gov/legislative/common/briefing/Senate_legislative_process.htm (last visited Sept. 23, 2016).

10. *Branches of Government*, USA.GOV, <https://www.usa.gov/branches-of-government> (last visited Sept. 23, 2016).

11. *Id.*

12. Robert Schlesinger, *The Size of the U.S. and the World in 2016*, U.S. NEWS: THOMAS JEFFERSON STREET (Jan. 5, 2016, 4:05 PM), <http://www.usnews.com/opinion/blogs/robert-schlesinger/articles/2016-01-05/us-population-in-2016-according-to-census-estimates-322-762-018>.

13. Kaplan et al., *supra* note 6, at 2–3.

probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.¹⁴

The Communications Act of 1934 made wiretapping a criminal offense and inadmissible in court.¹⁵ However, this law only lasted until 1960, when the government was unable to enforce laws that were in place due to a large amount of criminal activity.¹⁶ The case that changed everything was *Katz v. United States*. In *Katz v. United States*, the police had placed an eavesdropping device on a public payphone to record the telephone conversations of an illegal gambling operation which led to Katz ultimately being arrested and convicted.¹⁷ On appeal, the Supreme Court of the United States ruled seven-to-one that police action in this situation violated the Fourth Amendment. The Court determined that Katz's expectation of privacy was reasonable under the circumstances; thus, changing the original requirement of a "physical trespass," previously established in *Olmstead v. United States*.¹⁸ In *Olmstead*, the Supreme Court held that the government did not violate Olmstead's privacy because the wiretaps were placed in the street, and therefore, did not trespass onto Olmstead's property and did not constitute a "search" under the Fourth Amendment.¹⁹

Today, constitutional challenges are limited because of 18 U.S.C. § 2518 which outlines in depth the procedure that a federal prosecutor must take to intercept wire, oral, or electronic communications.²⁰ To obtain an order authorizing or approving the interception of a wire, oral, or electronic communication, an application must be made under oath or affirmation to a judge with jurisdiction over the matter, and include the following:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application; (b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be

14. U.S. CONST. amend. IV.

15. Kaplan et al., *supra* note 6, at 3.

16. *Id.*

17. *Katz v. United States*, 389 U.S. 347, 348–49 (1967); *see also* Kaplan et al., *supra* note 6, at 3.

18. *Katz*, 389 U.S. at 353; *see also* Kaplan et al., *supra* note 6, at 3.

19. *Katz*, 389 U.S. at 353; *see also* *Olmstead v. United States*, 277 U.S. 438, 457, 466 (1928).

20. Kaplan et al., *supra* note 6, at 3.

committed, (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted; (c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous; (d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter; (e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and (f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.²¹

Although there were procedures in place that require the federal prosecutor to obtain a court order prior to intercepting wire, oral, or electronic communication, in 2001—shortly after the September 11th terrorist attacks, the U.S.A. Patriot Act (Patriot Act) was passed. The purpose of the Patriot Act was to expand and aid the government’s power in anti-terrorism investigations while streamlining the process to obtain the necessary warrants to wiretap. Unfortunately, this proved to be insufficient.²²

In 2002, former President George W. Bush, expanded the authority by approving wiretaps without warrants by authorizing a domestic spying program designed to help prevent future attacks by conducting surveillance amongst citizens’ phone calls, e-mails, and other forms of

21. 18 U.S.C. §§ 2518(1)(a–f) (2012).

22. See also Alex Markels, *Timeline: Wiretaps’ Use and Abuse*, NPR.ORG (Dec. 20, 2005, 12:00 AM), <http://www.npr.org/templates/story/story.php?storyId=5061834>; see generally Larry Abramson & Maria Godoy, *The Patriot Act: Key Controversies*, NPR.ORG (Feb. 14, 2006), <http://www.npr.org/news/specials/patriotact/patriotactprovisions.html>.

communications.²³ This law is still currently in place sans a few provisions that have been removed.²⁴ The first provision removed was section 215 which allowed the National Security Agency (NSA) to collect metadata on millions of Americans and store the information for five years.²⁵ Metadata is defined as data which describes other data by providing information pertaining to a certain item's content.²⁶ The second provision removed was the law enforcement officer's ability to have a roving tap, which means an order that is continuous even if the suspect frequently changes communication devices.²⁷ As a result, law enforcement officers are now required to get a new court order.²⁸ Lastly, the government is no longer allowed to use national security tools against "lone-wolf" terror suspects if there is no connection found to a foreign terror group.²⁹

There is no doubt, that when terrorism strikes, there is an increase in domestic surveillance. The Paris attacks which occurred in November of 2015, triggered a plan from the FBI to increase domestic surveillance of suspected ISIS sympathizers as a way to protect against potential threats in the United States.³⁰ Further, the Federal Communications Commission (FCC) chairman had suggested to expand wiretap laws.³¹ Inaccurate news reports on the Paris attacks stated that the attackers communicated via a game console, PlayStation 4, which was not defined under the 1994 Communications Assistance for Law Enforcement Act (CALEA).³² The CALEA requires telecom companies, internet providers, and some online voice services to build their networks in ways that allow simpler access for authorities when it is necessary to lawfully intercept a suspect's telephone and online communication.³³ The PlayStation 4 was not something that

23. Markels, *supra* note 22.

24. Jeremy Diamond, *Patriot Act provisions have expired: What happens now?* CNN.COM (June 1, 2015, 10:48 AM), <http://www.cnn.com/2015/05/30/politics/what-happens-if-the-patriot-act-provisions-expire/>.

25. *Id.*

26. *Metadata*, TECHTERMS, <http://techterms.com/definition/metadata> (last visited Sept. 23, 2016).

27. Diamond, *supra* note 24.

28. *Id.*

29. *Id.*

30. Evan Perez, *After Paris: More wiretaps of U.S.-based suspects*, CNN (Nov. 15, 2015, 3:03 PM), <http://www.cnn.com/2015/11/15/politics/paris-attacks-us-wiretaps>.

31. Brian Fung & Andrea Peterson, *FCC chairman suggests expanded wiretap laws in response to the Paris attacks*, WASH. POST (Nov. 17, 2015), <https://www.washingtonpost.com/news/the-switch/wp/2015/11/17/the-fcc-suggests-expanded-wiretap-laws-in-response-to-the-paris-attacks/>.

32. *Id.*

33. *Id.*

was considered in 1994, and while the reports of communication via the gaming console are allegedly untrue, the FCC chairman believes this is something worth looking into in the event something were to take place in the future.³⁴

The 2016 shooting at Pulse Nightclub in Orlando, Florida has become “the deadliest shooting rampage in U.S. history.”³⁵ A recent interview that was transcribed took place between FRESH AIR contributor Dave Davies and Eric Lichtblau, who is a winner of the Pulitzer Prize for national reporting for breaking the story of President Bush’s administration’s warrantless wiretapping program, in which they discussed the Orlando attack.³⁶ This is an excerpt of the conversation which took place:

DAVIES: Let’s start by talking about Omar Mateen, the shooter in the massacre in Orlando. The FBI, we know, did investigate him. What drew their attention to Omar Mateen?

LICHTBLAU: Right. They actually looked at him twice They used an undercover informant to try and see whether he was really planning anything. They did surveillance. They did wiretapping. They interviewed the co-workers, obviously. They extended the investigation past the six months that they were originally allowed to go. And after about [ten] months, they closed it down. They said they did not have enough evidence to indicate that he was supporting terrorism or planned to act on his earlier comments. And the FBI kind of threw up its hands and closed the investigation.³⁷

This is one example of where wiretaps were used domestically to thwart potential terrorism and even though they investigated this person twice, an attack was still successfully carried out years later.

34. *Id.*

35. CNN LIBRARY, *Deadliest Mass Shootings in U.S. History Fast Facts*, CNN (June 13, 2016, 8:27 AM), <http://www.cnn.com/2013/09/16/us/20-deadliest-mass-shootings-in-u-s-history-fast-facts/>.

36. *How The FBI’s Wiretaps And Sting Operation Failed To Stop The Orlando Shooter*, NPR (June 29, 2016, 1:13 PM), <http://www.npr.org/2016/06/29/484006952/how-the-fbis-wiretaps-and-sting-operation-failed-to-stop-the-orlando-shooter>.

37. *Id.*

B. European Countries

1. Russia

Russia, formally a part of the Soviet Union, became independent in 1991 when the Soviet Union dissolved.³⁸ Russia is currently a federal multiparty republic with a bicameral legislative body.³⁹ This means that Russia is made up of a federal state with a constitution and other units that are self-governed.⁴⁰ The government consists of two bodies the Federation Council and the State Duma.⁴¹ The Federation Council currently has 170 seats and the State Duma currently has 450 seats.⁴² Russia has a head of state which is the president as well as a head of government which is the prime minister.⁴³ The current president is Vladimir Putin and the prime minister is Dmitry Medvedev.⁴⁴ The estimated population of Russia in 2015 was 146.3 million people.⁴⁵

Russia's national system of lawful interception of all electronic communication is The System of Operative-Investigative Measures (SORM).⁴⁶ There are a total of seven Russian investigative and security agencies that have been granted the legal right to intercept phone calls and emails; however, it is the Federal Security Service (FSB) who defines the procedures that take place to intercept electronic communications.⁴⁷ As bizarre as this sounds, the FSB must obtain a court order prior to intercepting the oral communications but they do not have to provide it to any telecom providers.⁴⁸ This means, that the FSB can obtain the court order and immediately tap right into an individual's line.⁴⁹ The FSB

38. ENCYCLOPEDIA BRITANNICA, <https://www.britannica.com/place/Russia> (last visited July 22, 2016) [hereinafter *About Russia*].

39. *Id.*

40. DICTIONARY.COM, <http://www.dictionary.com/browse/federal-republic> (last visited July 22, 2016).

41. *About Russia, supra* note 38.

42. *Id.*

43. *Id.*

44. *Id.*

45. *Russia Population*, TRADING ECON., <http://www.tradingeconomics.com/russia/population> (last visited July 22, 2016).

46. Andrei Soldatov et al., *Russia's Surveillance State*, WORLD POL'Y J., Fall 2013, at 23 [hereinafter WORLD POL'Y].

47. *Id.* at 24.

48. *Id.* at 25.

49. *Id.*

requires telecom providers to pay for the SORM equipment and its installation while having no access to the surveillance boxes.⁵⁰

On August 12, 1995, a law was passed on operative searches and seizures which gave the right to the FSB to carry some investigative activities without prior judicial approval.⁵¹ Some of the activities included were wiretapping telephones and monitoring other forms of communication.⁵² The FSB was allowed to engage in these activities if there was an emergency and serious crime was going to be committed, or if Russia's political, military, economic or environmental security were threatened.⁵³ A judge must be notified within twenty-four hours of any action taken and within forty-eight hours either cease the surveillance or have the appropriate court order to continue.⁵⁴ The biggest flaw found in this act, is the definition of what constitutes "security" and "emergency" because without a fine line, it becomes subjective.⁵⁵

In December 2010, a federal law was passed expanding the legal grounds for wiretapping domestically in Russia.⁵⁶ Receiving a report that an individual is preparing to commit a crime is sufficient; they do not need to back up those allegations.⁵⁷ The transcript of the conversation will remain even if the allegations hold no merit and may turn up later in another criminal case in the future.⁵⁸ Andrei Soldatov, who is a leading security expert stated, "telephone and e-mail intercepts and recordings have risen from 265,000 in 2007 to 466,000 in 2011 and that it is still on the rise."⁵⁹ He also stated, "there is a lack of parliament oversight and it is almost impossible to establish who is carrying out these wiretap operations, even against opposition leaders."⁶⁰ In 2011, only 3554 wiretap requests, or

50. *Id.*

51. *FSB Legislative Authority*, GLOBALSECURITY.ORG, <http://www.globalsecurity.org/intell/world/russia/fsb-legis.htm> (last visited July 21, 2016).

52. *Id.*

53. *Id.*

54. *Id.*

55. *Id.*

56. Irina Borogan & Andrei Soldatov, *The Kremlin Is All Ears*, MOSCOW TIMES (Dec. 28, 2012, 20:17), <http://www.themoscowtimes.com/opinion/article/the-kremlin-is-all-ears/473703.html>.

57. *Id.*

58. *Id.*

59. Tom Balmforth, *Spy vs. Spy: Wiretapping On The Increase In Russia*, RADIO FREE EUR. (July 16, 2012), <http://www.rferl.org/content/spy-wiretapping-on-increase-russia-rival-security-services/24647019.html>.

60. *Id.*

one percent out of 466,152 were rejected.⁶¹ One of those wiretaps conducted were of the Boston Marathon bombing suspect, Tamerlan Tsarnaev.⁶² In 2011, Russia secretly recorded a telephone conversation with his mother vaguely discussing jihad.⁶³ There was another telephone conversation recorded of the mother speaking to someone in Southern Russia who is under FBI investigation for an unrelated case.⁶⁴ The Russian government allegedly told the FBI these individuals were religious extremists.⁶⁵ Lastly, by way of domestic surveillance, the Moscow Times have reported that in January of 2016, Moscow has thwarted Islamic State terrorist attacks in Russia as they had “operational control” over them from the beginning.⁶⁶

2. Italy

“In Italy, you’re nobody if your phone isn’t tapped.”⁶⁷ Italy’s leading political provocateur and blogger Beppe Grillo stated, “this is a nation where if you cannot be blackmailed, you will never get ahead.”⁶⁸ Once a monarchy government being ran by a king was replaced shortly after World War II, on June 2, 1946, when the Italians voted in a referendum to replace the monarchy.⁶⁹ Today, Italy is now a republic government made up of two legislative houses, the senate and the chamber of deputies.⁷⁰ This means that this government is ruled by representatives of the citizen body.⁷¹ Italy has a head of state which is the president and a head of government which is the prime minister. The current president is Sergio Mattarella and the

61. *Wiretapping Doubles in Russia Since 2007*, SPUTNIK INT’L (Apr. 6, 2012, 18:27), <http://sputniknews.com/russia/20120604/173843249.html> [hereinafter Sputnik Int’l].

62. *Russia had wiretap on Boston Marathon bombing suspect, US officials say*, FOXNEWS.COM (Apr. 27, 2013), <http://www.foxnews.com/us/2013/04/27/russia-had-wiretap-on-boston-marathon-bombing-suspect-us-officials-say.html>.

63. *Id.*

64. *Id.*

65. *Id.*

66. *Moscow Says It Thwarted IS Terror Attacks in Russia*, MOSCOW TIMES (Jan. 29, 2016, 19:02), <http://www.themoscowtimes.com/news/moscow-says-it-thwarted-is-terror-attacks-in-russia-51648>.

67. Rachel Donadio, *An Untapped Phone Call in Italy? It’s Possible*, N.Y. TIMES (May 30, 2010), http://www.nytimes.com/2010/05/31/world/europe/31italy.html?_r=0.

68. *Id.*

69. Marino Berengo et al., *Italy: Government and society*, ENCYCLOPEDIA BRITANNICA (Aug. 12, 2016), <https://www.britannica.com/place/Italy/Government-and-society> [hereinafter *About Italy*].

70. *Id.*

71. André Munro, *Republic*, ENCYCLOPEDIA BRITANNICA (June 22, 2016), <https://www.britannica.com/topic/republic-government>.

prime minister is Matteo Renzi.⁷² The Senate has 322 seats currently which includes seven non-elective seats; five of which are presidential appointees and two former presidents serving.⁷³ The Chamber of Deputies has 630 seats currently and are popularly elected through a system of proportional representation and are considered the lower chamber.⁷⁴ In 2015 the Italian population was estimated at 60.8 million people.⁷⁵

Article 15 of the Italian Constitution states, “[t]he freedom and secrecy of correspondence and of every other form of communication is inviolable,”⁷⁶ but yet many individuals’ privacy is still being intruded on despite this constitutional guarantee. Article 266 of the Italian Code of Criminal Procedure states:

the interception of a telephone conversation or communication and other forms of telecommunications is allowed in proceedings relating to the following offenses: a) intentional crimes for which is provided for life imprisonment or imprisonment for a maximum of five years; determined in accordance with Article 4; b) crimes against the public administration for which is planned the penalty of imprisonment of not less than five years determined in accordance with Article 4; c) offenses relating to narcotic drugs and psychotropic substances; d) offenses relating to weapons and explosives; e) smuggling offenses; f) crimes of abuse, threats, usury, illegal financial activities, insider trading, market manipulation, harassment or annoyance to persons by means of telephone.⁷⁷

To obtain permission to wiretap in Italy the officer needs to ask the judge for preliminary investigations and obtain authorization for serious crimes as outlined above and essential for the continuation of the investigation.⁷⁸ In cases where serious harm to the investigation may occur the officer may move forward with the interception of communication so long as the court is notified not later than twenty-four hours.⁷⁹ The court, within forty-eight hours will render a decision on whether they will allow

72. *About Italy*, *supra* note 69.

73. *Id.*

74. *Id.*

75. *Italy Population*, TRADING ECON., <http://www.tradingeconomics.com/italy/population> (last visited July 22, 2016).

76. Art. 15 Costituzione [Cost.] (It.).

77. C.p.p. art. 266 (It.).

78. *Id.* at art. 267.

79. *Id.*

the intercepting of communications to continue or cease and if it is not validated, the interception must cease and the evidence collected cannot be used.⁸⁰ After the September 11, 2001 terrorist attacks, Italy has allowed anticipatory wiretapping even without any ongoing investigation.⁸¹

Italy is infamous for wiretapping.⁸² Wiretapping is such a common practice in Italy that even former Secretary of State, and current Presidential Candidate, Hillary Clinton, and Pope Benedict XVI when they were speaking with the head of Italy's civil protection agency, Guido Bertolaso, were wiretapped as he was being wiretapped as part of an investigation.⁸³ In 2006, the Max Planck Institute calculated that seventy-six out of every 100,000 Italians had their phones tapped.⁸⁴ Further, in 2008 as reported by the ministry of justice, 124,326 phones were tapped.⁸⁵ With the increase of terrorism in Europe, the Russian Today reported that Italy had recently stopped potential ISIS attacks on the Israeli embassy in Rome as well as on the Vatican by intercepting communications.⁸⁶ Despite the great news, "Italy is the eavesdropping centre of Europe," putting many Italians' privacy expectations at risk.⁸⁷

3. France

France is a republic government with two legislative houses.⁸⁸ The two houses of the French parliament consist of the Senate and the National Assembly.⁸⁹ The Senate has 348 seats currently and the National Assembly currently has 577 seats.⁹⁰ France also has a head of state which is the

80. *Id.*

81. Elizabeth F. Defeis, *Italy--Journalists, Privacy and A Right To Information*, 20 DIG., NAT'L ITALIAN A.B.A. L.J. 41, 42 (2012).

82. *See* Donadio, *supra* note 67.

83. Nick Squires, *Silvio Berlusconi wiretap victory in confidence vote*, THE TELEGRAPH (June 10, 2010, 5:46 PM), <http://www.telegraph.co.uk/news/worldnews/europe/italy/7818509/Silvio-Berlusconi-wiretap-victory-in-confidence-vote.html>.

84. *Italian bill to limit wiretaps draws fire*, BBC NEWS (June 11, 2010), <http://www.bbc.com/news/10279312> [hereinafter *Italian bill*].

85. *Id.*

86. *Italy busts ISIS supporters cell mulling attacks on Vatican & Israeli embassy in Rome*, RT NEWS (Apr. 29, 2016, 00:10), <https://www.rt.com/news/341304-italy-arrests-isis-supporters/>.

87. *Italian bill*, *supra* note 84.

88. T.N. Bisson, et al., *France: The role of the president*, ENCYCLOPEDIA BRITANNICA (July 15, 2016), <https://www.britannica.com/place/France/The-role-of-the-president>.

89. *Id.*

90. *Id.*

president and a head of government which is the prime minister.⁹¹ The current president is François Hollande, and the current prime minister is Manuel Valls.⁹² Currently, France's estimated population is 66.6 million people.⁹³

On July 10, 1991 France passed the 1991 Wiretapping Act which gave freedom of telecommunications from being intruded on without a court order.⁹⁴ The only ones that can intrude were police officers without magistrate approval or for national security purposes which did not require magistrate approval.⁹⁵ If the reason for intruding telecommunications was for national security purposes it only had to be approved by the current prime minister who in turn was required to tell an independent three-member commission of two legislators and of a chair who would be named by the courts.⁹⁶

On January 7, 2015 terror struck in France and was considered one of the “worst security crises in decades.”⁹⁷ After the attacks, France passed a new law allowing domestic surveillance of anyone linked to a “terrorist inquiry” by intelligence agencies without prior approval.⁹⁸ The new law allows the intelligence agencies to collect metadata which will be subject to analysis for any potential suspicious behavior, place cameras and recording devices in private homes, and install key logger devices which record every key stroke on a computer that is bugged in actual live time.⁹⁹ Initially, the metadata collected is anonymous but if necessary with follow-up requests, the agencies could reveal the identity.¹⁰⁰ Metadata is stored for five years and recordings only one month.¹⁰¹ The law also allows the use of IMSI catchers, which is something flown over a specific area that collects data and records all types of conversations whether it is via phone, internet, or

91. *Id.*

92. *Id.*

93. *France Population*, TRADING ECON., <http://www.tradingeconomics.com/france/population> (last visited July 22, 2016).

94. Edward A. Tomlinson, *The Saga of Wiretapping in France: What It Tells Us About the French Criminal Justice System*, 53 LA. L. REV. 1091, 1091–92 (1993).

95. *Id.* at 1092.

96. *Id.*

97. *Charlie Hebdo attack: Three days of terror*, BBC NEWS (Jan. 14, 2015), <http://www.bbc.com/news/world-europe-30708237>.

98. Angelique Chrisafis, *France passes new surveillance law in wake of Charlie Hebdo attack*, THE GUARDIAN (May 5, 2015, 19:00), <https://www.theguardian.com/world/2015/may/05/france-passes-new-surveillance-law-in-wake-of-charlie-hebdo-attack>.

99. *Id.*

100. *Id.*

101. *Id.*

text-messaging within a specific area.¹⁰² Current Prime Minister, Manuel Valls, backed the bill and said it was “necessary and proportionate.”¹⁰³ Valls also stated that “previous French law on wiretapping dated back to 1991, ‘when there were no mobile phones or internet,’ and the new bill was crucial in the face of extremist threats.”¹⁰⁴ The law also gained more support after a “jihadist killing spree” as well as when police stopped the attack on a church in April of 2015.¹⁰⁵

III. COMPARATIVE ANALYSIS OF LAW

A. Differences

While there are differences between the United States and European countries, these differences are not too drastic. While the Patriot Act still stands today, things such as metadata collection and storing it for five years, roving wiretaps, and the use of national security tools on lone-wolf suspects are no longer allowed.¹⁰⁶ This is a recent change as of 2015.¹⁰⁷

Unlike the United States, France, the very same year, passed a law which allowed the metadata collection the United States no longer allows as well as other intrusive surveillance tools.¹⁰⁸ Further, while the United States has to show a court order to telecom providers to conduct a legal wiretap that falls outside of the scope of the Patriot Act, the FSB in Russia does not. All the FSB simply has to do is obtain permission and conduct the wiretap because they require any telecom provider to pay for the SORM equipment and installation giving them no access to the surveillance boxes either.¹⁰⁹

The telecom providers would never know if a wiretap was being conducted.¹¹⁰ Also, in Russia, merely receiving a report that an individual

102. *French court approves sweeping new surveillance powers*, FR. 24 (July 24, 2015), <http://www.france24.com/en/20150724-france-surveillance-law-approved-phone-taps-internet-hollande-terrorism> [hereinafter *French Court*].

103. Chrisafis, *supra* note 98.

104. *Id.*

105. *France politician approve sweeping new spying powers months after Paris attacks*, TELEGRAPH (May 5, 2015, 9:46 PM), <http://www.telegraph.co.uk/news/worldnews/europe/france/11584786/French-politicians-approve-sweeping-new-spying-powers-months-after-Paris-terror-attacks.html> [hereinafter *French Politicians*].

106. Diamond, *supra* note 24.

107. *Id.*

108. Chrisafis, *supra* note 98.

109. Soldatov et al., *supra* note 45, at 25.

110. *Id.*

is preparing to commit a crime is sufficient grounds for a wiretap, the allegations do not even have to be backed up with hard facts.¹¹¹ This differs from the United States because 18 U.S.C. §§ 2518(1)(a)–(f) outlines detailed requirements to obtain a court order to intercept any type of communication, backed up facts being one of the many requirements.¹¹²

Lastly, Italy allows preemptive wiretapping of its citizens without an ongoing investigation¹¹³ whereas the United States, even with the Patriot Act, requires a warrant if it is seeking to intercept communications between two United States citizens on American soil.¹¹⁴ While the concept and the goals are the same, to avoid terrorism and prevent crime; the process, requirements, and information collected are what most differs the most from the countries.

B. Similarities

France, Italy, Russia, and the United States have more in common than one would think. Wiretapping has become a “norm” in these countries. Specifically, the statistics show that “[n]o wiretap applications were reported as denied in 2015” in the United States.¹¹⁵ Comparably in 2011, out of 466,152 wiretap applications, only one percent were rejected in Russia.¹¹⁶

Whenever there is a terrorist attack, there is a push for heightened security measures and an increase in surveillance and the countries know no end when expanding their powers of domestic surveillance.¹¹⁷ In Italy, shortly after the terrorist attacks on September 11, 2001 in the United States, Italy allowed preemptive wiretapping which expanded its powers.¹¹⁸ Further, after the terrorist attacks, former President Bush passed the Patriot Act and a domestic surveillance spying program.¹¹⁹ Likewise, shortly after the 2015 France terrorist attacks, France passed a new law that allows domestic surveillance of anyone linked to a “terrorist inquiry” by

111. Borogan & Soldatov, *supra* note 56.

112. 18 U.S.C. §§ 2518(1)(a)–(f) (1998).

113. Defeis, *supra* note 81.

114. *NSA Warrantless Wiretapping Timeline*, N.Y. C.L. UNION, http://www.nyclu.org/nsa_spying_timeline.html (last visited Sept. 23, 2016).

115. *Wiretap Report 2015*, *supra* note 5.

116. Balmforth, *supra* note 59.

117. See Defeis, *supra* note 81; see also Abramson & Godoy, *supra* note 22; Chrisafis, *supra* note 97; *French court*, *supra* note 102; Markels, *supra* note 22.

118. Defeis, *supra* note 81.

119. See Markels, *supra* note 22.

intelligence agencies without prior approval.¹²⁰ France's Prime Minister Manuel Valls' heavily disapproved of the comparison of the two laws.¹²¹

Further, after the 2015 France terrorist attacks, the FBI increased the amount of wiretaps and surveillance against those who were "ISIS sympathizers."¹²² The laws of France and the United States are strikingly similar because of the data that is allowed to be collected such as the metadata that was once allowed in the Patriot Act.¹²³ Lastly, the frequency of wiretapping being conducted in Russia, Italy, and the United States are practically identical because the request for a wiretap is hardly denied leading to many wiretaps being conducted.¹²⁴

IV. SOCIETY'S VIEW AROUND THE GLOBE

A. *The United States*

Research shows that results of the polls conducted were somewhat dependent on the survey's phrasing and the way the person completing the survey perceived it.¹²⁵ There was a "controlled study" done by CBS News/New York Times with two separate versions of the same poll, version "A" and "B".¹²⁶

Version A: After 9/11, President Bush authorized government wiretaps on some phone calls in the U.S. without getting court warrants, saying this was necessary in order to reduce the threat of terrorism. Do you approve or disapprove of the president doing this?

Version B: After 9/11, George W. Bush authorized government wiretaps on some phone calls in the U.S. without getting court warrants. Do you approve or disapprove of George W. Bush doing this?¹²⁷

When the random sample of people took the poll in version "A" the results were the following; fifty-three percent approved the president doing

120. Chrisafis, *supra* note 98.

121. *Id.*

122. Perez, *supra* note 30.

123. See Chrisafis, *supra* note 97; see also Diamond, *supra* note 24.

124. See Italian bill, *supra* note 84; see also Sputnik Int'l, *supra* note 61; *Wiretap Report 2015*, *supra* note 5.

125. Frank Newport, *Where Do Americans Stand on the Wiretapping Issue*, GALLUP.COM (Feb. 24, 2006), <http://www.gallup.com/poll/21628/where-americans-stand-wiretapping-issue.aspx>.

126. *Id.*

127. *Id.*

this, forty-six percent disapproved, and one percent was unsure.¹²⁸ When the remainder of the random sample of people took the poll in version “B”, the results flipped.¹²⁹ In version “B”, forty-six percent approved the president doing this, fifty percent disapproved, and four percent was unsure.¹³⁰ The versions varied in language, but the results remained split despite the wording.¹³¹ When the poll stated that it was “necessary,” there was a seven percent increase in approval rather than disapproval.¹³² There was also a seven percent decrease when former President George W. Bush was referred to as “George W. Bush” by itself rather than version “A” which stated, “President Bush.”¹³³ As previously mentioned, “[a]sk the American public if they want an FBI wiretap and they’ll say, ‘No’. If you ask them do they want a feature on their phone that helps the FBI find their missing child they’ll say, ‘Yes’.”¹³⁴ Essentially, this is same. American citizens do not want the FBI wiretapping their phones but at the same time, want to provide the FBI with information so that in the event their child goes missing, the FBI can track them.¹³⁵ This is a double standard amongst American citizens.

The Pew Research Center conducted a research experiment amongst registered voters from February 1, 2006 through February 5, 2006.¹³⁶ The survey stated the following: “[d]o you think it is generally right or generally wrong for the government to monitor telephone and e-mail communications of Americans suspected of having terrorist ties without first obtaining permission from the courts?”¹³⁷ Here, forty percent of registered voters were against it and fifty-four percent of registered voters were for it.¹³⁸

A little over nine years later, and only two years later from the Edward Snowden whistle blowing incident, the Pew Research Center released

128. *Id.*

129. *Id.*

130. Newport, *supra* note 125.

131. *Id.*

132. *Id.*

133. *Id.*

134. Louis Freeh, *supra* note 1.

135. *Id.*

136. Newport, *supra* note 125.

137. *Id.*

138. *Id.*

another study.¹³⁹ One survey response yielded the following result from a spring 2014 question; seventy-four percent of people said “they should not give up privacy and freedom for the sake of safety” and twenty-two percent felt the total opposite.¹⁴⁰ However, a narrower question such as the percentage of those that disapproved of the United States government’s collection of telephone and internet data as part of anti-terrorism efforts yielded the following results; fifty-four percent disapproved and forty-two percent approved of this action.¹⁴¹ Not much has changed over the years in the eyes of American citizens as the results are still demonstrating a large split of people that are for and against domestic surveillance tools, such as wiretapping, and these results are likely going to stay constant over the upcoming years.

B. European Countries

Europe’s views on wiretapping and domestic surveillance as a whole differs some from the United States. In 2013,¹⁴² the Pew Research Center released the following question that was asked globally, “[a]ccording to news reports, the American government has been monitoring communications, such as emails and phone calls, in the United States and many other countries. In your opinion, is it acceptable or unacceptable for the American government to monitor communications from American [c]itizens?”¹⁴³ Sixty-seven percent of the Russian respondents said that this was unacceptable and twenty-eight percent of the Russian respondents found it acceptable.¹⁴⁴ The Italians responded as well with sixty-three percent finding that this behavior was unacceptable and thirty-one percent finding that it was acceptable.¹⁴⁵ The French responded with an overwhelming percentage of disapproval.¹⁴⁶ Specifically, eighty-two percent of people found it unacceptable to do this while only eighteen

139. George Gao, *What Americans think about NSA surveillance, national security and privacy*, PEW RES. CTR. (May 29, 2015), <http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/>.

140. *Id.*

141. *Id.*

142. Corinne Purtill, *France's embrace of harsh anti-terror laws that go far beyond America's Patriot Act*, THE WEEK (Feb. 8, 2015), <http://theweek.com/articles/536453/frances-embrace-harsh-antiterror-laws-that-far-beyond-americas-patriot-act>.

143. *Global Opinions of U.S. Surveillance*, PEW RES. CTR., <http://www.pewglobal.org/2014/07/14/nsa-opinion/country/russia/> (last visited Sept. 23, 2016).

144. *Id.*

145. PEW RES. CTR. *supra* note 143.

146. *Id.*

percent found it acceptable.¹⁴⁷ The United States is split on this issue whereas Italy, Russia, and France find it mostly unacceptable conduct by the American government.

A couple years later, when terror struck in France on January 7, 2015, it changed the minds of many French citizens. Three months after the January attacks, the CSA poll, via the Atlantico news website was released, which demonstrated that the majority of French people were favoring the “restrictions on their freedoms in the name of fighting extremism” and only thirty-two percent were opposed to freedoms being reduced.¹⁴⁸ While large majorities of the French people are now accepting of the 2015 law that passed, many human rights organizations are against the law as it reduces freedom and infringes upon civil liberties.¹⁴⁹

C. *Comparison of Views*

The views of European citizens differ amongst each other as well as from the United States. While citizens of Russia and Italy heavily disapproved of the American government conducting domestic surveillance, France’s latest opinion is that they would rather have their rights reduced so that the government can conduct its surveillance and thwart potential terrorists.¹⁵⁰ Fear plays a role in helping shape the views of the citizens of a specific country, because when the French law first came about in 2015 allowing wiretaps without prior approval, there was heavy criticism, but when there were more killings and terror plots occurring, the new law gained much needed support.¹⁵¹ Over the last nine years however, American citizens have remained consistent in their views.¹⁵² With everything going on around the world, American citizens still have very split opinions on whether they agree or disagree with domestic surveillance.¹⁵³ With terrorism attacks occurring more and more it will be interesting to see how the polls change over the next few years and whether American citizens tip the scales and become overwhelmingly in favor of domestic surveillance.

147. *Id.*

148. TELEGRAPH, *supra* note 105.

149. Kateryna Khinkulova, *Surveillance: Who’s Watching What, and Why?*, EURONEWS.COM (June 5, 2015), <http://www.euronews.com/2015/05/06/surveillance-who-s-watching-what-and-why>.

150. TELEGRAPH, *supra* note 105.

151. Purtill, *supra* note 142.

152. *See* Gao, *supra* note 139; *see* Newport, *supra* note 125.

153. Gao, *supra* note 139.

V. CONCLUSION

As demonstrated, there are alleged safeguards and laws in place for wiretapping to ensure that society's privacy is not being intruded upon; however, this is not always the case. As the saying goes, "safety may come with a price." Even if safety may come with a price, society should have more requirements in place and warrantless wiretapping should come to an end. If the government has a reasonable belief that an individual poses a threat to United States soil, and there are concrete facts that support this threat, then that person should be investigated through the domestic surveillance tools necessary, including wiretapping with an appropriate warrant to do so. However, wiretapping should only be used for this one specific reason only to prevent terrorism.

Also, there should be stricter guidelines on what is necessary to obtain a warrant to wiretap. The fact that there were zero applications denied in 2015, meaning a total of 4148 warrants approved, is alarming because the judges are reluctant to deny them and/or it is too easy to obtain.¹⁵⁴ This does not even include the wiretaps that were obtained without warrants. According to Albert Gidari, a top privacy law attorney, there are way more wiretaps being conducted without our knowledge. Albert Gidari stated the following:

Since the Snowden revelations, more and more companies have started publishing "transparency reports" about the number and nature of government demands to access their users' data. AT&T, Verizon, and Sprint published data for 2014 earlier this year and T-Mobile published its first transparency report on the same day the AO released the Wiretap Report. In aggregate, the four companies state that they implemented 10,712 wiretaps, a threefold difference over the total number reported by the AO. Note that the 10,712 number is only for the four companies listed above and does not reflect wiretap orders received by other telephone carriers or online providers, so the discrepancy actually is larger.¹⁵⁵

This poses the question: what is the Government not saying? Who is being listened to now? Wiretapping is a powerful surveillance tool and should only be used for issues related to terrorism, not drug related offenses which happens very frequently as it was the most common type of criminal

154. *Wiretap Report 2015*, *supra* note 5.

155. David Kravets, *US government's reported numbers of wiretaps don't add up*, ARS TECHNICA (July 10, 2015, 3:20 PM), <http://arstechnica.com/tech-policy/2015/07/us-governments-reported-number-of-wiretaps-dont-add-up/>.

offense investigated with a wiretap in 2015.¹⁵⁶ With the latest terrorist attacks occurring around the world, citizens should be prepared for an expansion of the use of wiretapping, rather than a decrease, because the research has shown that there is a link between terrorism and domestic surveillance. A large percentage of society has little knowledge about the Patriot Act.¹⁵⁷ It is important to educate society about its rights starting from a young age because the more the government is allowed to intrude into society's privacy, the easier it will be for the government to do so.

Justice Potter Stewart said it best:

The Government stresses the fact that the telephone booth from which the petitioner made his calls was constructed partly of glass, so that he was as invisible after he entered it as he would have been if he had remained outside. But what he sought to exclude when he entered the booth was not the intruding eye—it was the intruding ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen.¹⁵⁸

American citizens should not have to deal with the “intruding ear,”—the government.¹⁵⁹ That is the court rationale that should be followed to protect society's privacy. Current legislation that is going to the Senate for consideration is H.R. 699: Email Privacy Act.¹⁶⁰ The proposed bill will eliminate the “loophole” by requiring government agencies to seek warrants for digital communications 180 days or older.¹⁶¹ Warrants require probable cause, versus what is being used now, subpoenas, which do not.¹⁶² This is a great bill to ensure more privacy to American citizens because it will increase the difficulty to obtain such information by government agencies. This is the type of legislation—ways of making wiretapping more difficult—needed to be enacted or it will be difficult to draw a distinct line of where domestic surveillance ends. Benjamin Franklin once said, “[t]hose who would give up essential liberty to purchase a little temporary

156. *Wiretap Report 2015*, *supra* note 5.

157. *The Patriot Act: What Is the Proper Balance Between National Security and Individual Rights?* CONST. RTS. FOUND. <http://www.crf-usa.org/america-responds-to-terrorism/the-patriot-act.html> (last visited Sep. 23, 2016) [hereinafter *The Patriot Act*].

158. *Katz*, 389 U.S. at 352.

159. *Id.*

160. Email Privacy Act, H.R. 699, 114th Cong. §§ 2–4 (2015); *Summaries for the Email Privacy Act*, GOVTRACK.US, <https://www.govtrack.us/congress/bills/114/hr699/summary> (last visited Sept. 23, 2016) [hereinafter *Email Privacy Act*].

161. *Id.*

162. *Id.*

safety deserve neither liberty nor safety.”¹⁶³ This founding father would definitely be disappointed in today’s society for allowing such intrusion into its privacy.

163. *The Patriot Act*, *supra* note 157.