WIRETAPPING IN A WIRELESS WORLD: ENACTING A VERMONT WIRETAP STATUTE TO PROTECT PRIVACY AGAINST MODERN TECHNOLOGY

INTRODUCTION

The ways in which Americans communicate have changed considerably in the 141 years since the installation of the first telephone

lines.[1] In 1968, when Congress enacted the first federal wiretap statute,[2] 20% of American homes did not have a telephone.[3] Today, over 95% of Americans own a mobile phone and 49 states have passed some form of wiretap statute.[4] Vermont is the only state that has not, thereby leaving its citizens' private communications vulnerable to interception.[5] However, merely enacting a wiretap statute will not sufficiently protect Vermonters because rapidly evolving technology threatens the privacy that wiretap laws protect.[6]

Wiretap laws have struggled to keep pace with the rapid changes in communications technology.[7] Even the term *wiretap* is outdated and no longer accurately reflects the manner in which interceptions occur.[8] For instance, today more than half of American households have only wireless phones.[9] Wiretap laws must be able to adapt to evolving communications technology to remain effective and enforceable.

As the only state without a wiretap statute, Vermont is in a unique position to learn from the challenges faced by other states when applying new technology to existing wiretap laws.[10] Vermont can use the most

---

1. *How Phones Work*, TELECOMM. HIST. GRP. VIRTUAL MUSEUM, http://www.telcomhistory.org/vm/sciencePhonesWork.shtml (last visited Dec. 4, 2018).

2. Omnibus Crime Control and Safe Street Act of 1968, Pub. L. No. 90-351, § 802, 82 Stat. 197, 212–23 (codified as amended at 18 U.S.C. §§ 2510–22 (2012)).

3. *Historical Census of Housing Tables: Telephones*, U.S. CENSUS BUREAU, https://www.census.gov/hhes/www/housing/census/historic/phone.html (last modified Oct. 31, 2011).

4. *Mobile Fact Sheet*, PEW RES. CTR. (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/mobile/; Carol M. Bast, *What's Bugging You? Inconsistencies and Irrationalities of the Law of Eavesdropping*, 47 DEPAUL L. REV. 837, 851 (1998).

5. Bast, *supra* note 4, at 868.

6. *See, e.g.*, *Modernizing the Electronic Communications Privacy Act*, ACLU, https://www.aclu.org/issues/privacy-technology/internet-privacy/modernizing-electronic-communications-privacy-act-ecpa (last visited Dec. 4, 2018) [hereinafter ACLU] (describing how outdated wiretap laws "allow[] the government to intercept and access a treasure trove of information" about an individual's communications and activity).

7. *See id.* ("Since 1986, technology has advanced at breakneck speed while electronic privacy law remained at a standstill.").

8. *See, e.g.*, Christopher Woolf, *The History of Electronic Surveillance, From Abraham Lincoln's Wiretaps to Operation Shamrock*, PUB. RADIO INT'L (Nov. 7, 2013), https://www.pri.org/stories/2013-11-07/history-electronic-surveillance-abraham-lincolns-wiretaps-operation-shamrock (describing how "the first wiretapping" involved an eavesdropper "literally tap[ping] the telegraph wire anywhere along its length" to hear transmitted messages).

9. NAT'L CTR. FOR HEALTH STAT., WIRELESS SUBSTITUTION: EARLY RELEASE OF ESTIMATES FROM THE NATIONAL HEALTH INTERVIEW SURVEY, JULY–DECEMBER 2016 at 2 (2017).

10. *See, e.g.*, Miles v. State, 781 A.2d 787, 800 (Md. 2001) (holding that a call between a cell phone and a landline was a "wire communication" under Maryland law because "[t]he transmission . . . involves the sound waves of the conversation being transmitted over the cellular phone company's designated frequency to the cellular phone carrier's transmitter, which sends the signal over a land-based wire to the ordinary telephone"); State v. Tango, 671 A.2d 186, 188 (N.J. 1996) (discussing

effective state approaches as models for its own law while also avoiding the mistakes of less successful states. Thus, Vermont will ensure that its wiretap law can adequately protect private communications even as technology continues to evolve.

This Note analyzes the various approaches states have taken to draft and enact wiretap laws, and the effectiveness of applying those laws to new technology. It also recommends the approach Vermont should take to draft a wiretap statute that will endure future technological changes. Part I provides a historical overview of federal and state approaches to wiretapping and discusses how Vermont courts have addressed wiretapping in the absence of a statute. Part II addresses the importance of wiretap statutes that can adapt to rapidly changing technology and the unique challenges that recent technologies pose. Part III compares the successes and failures of different state approaches to wiretapping. Finally, Part IV proposes how Vermont can avoid similar problems with evolving technological issues with wiretap laws. This Part includes a recommendation as to how Vermont should draft its own wiretap statute.

I. DEVELOPMENT AND EVOLUTION OF WIRETAP LAWS

A. Definitions of Wiretapping and Related Terms

"Wiretapping" traditionally referred only to the interception of communications sent by wire.[11] However, this definition has evolved over time. The Communications Act of 1934 referred to "interstate or foreign communication[s] [transmitted] by wire or radio."[12] The Omnibus Crime Control and Safe Street Act of 1968 (Title III) defined wiretapping as the interception of "wire or oral communication."[13] In 1986, the Electronic Communications Privacy Act (ECPA) expanded that definition to include "electronic communication" as well.[14]

Alternatively, some state laws use the term "eavesdropping."[15] Eavesdropping is "[t]he act of secretly listening to the private conversation

---

whether a cell phone wiretap could comply with the requirement that a warrant state the location of the phone to be tapped, because cell phones do not have a fixed location).

11. *See* Woolf, *supra* note 8 (discussing the origin of the term "wiretap").

12. Communications Act of 1934, ch. 652, 48 Stat. 1064, 1103 (codified as amended at 47 U.S.C. § 605 (2012)).

13. Pub. L. No. 90-351, § 802, 82 Stat. 197, 211–23 (1968) (codified as amended at 18 U.S.C. §§ 2510–22 (2012)).

14. Pub. L. No. 99-508, § 101, 100 Stat. 1848, 1848–49 (1986) (codified as amended at 18 U.S.C. §§ 2510–22 (2012)).

15. *See, e.g.*, 720 ILL. COMP. STAT. 5/14-1 (2018) ("An eavesdropping device is any device capable of being used to hear or record oral conversation or intercept, or transcribe electronic

of others without their consent."[16] Therefore, wiretapping is technically a method of eavesdropping via wires.[17] However, because the statutory definition of wiretapping is much broader than the original use of the word, the terms eavesdropping and wiretapping are essentially interchangeable.[18] This Note uses the term *wiretap* to refer to the interception of "wire, electronic, or oral communication," even when discussing historical events that predate the current definition, unless otherwise indicated.

"Wiretapping" is the act of intercepting communications, not accessing stored communications.[19] Intercepting is the overhearing or recording of oral, wire, or electronic communications.[20] Accessing stored communications is the act of obtaining communications data that is electronically stored, such as data logs maintained by phone companies, emails stored on a server, voicemails, and other similar stored records.[21] Evolving technology creates similar challenges for both intercepted and stored communications.[22] The two issues are closely related, but this Note focuses only on intercepted communications because Vermont has already codified a statute on stored communications.[23]

---

communications whether such conversation or electronic communication is conducted in person, by telephone, or by any other means . . . ."); ALA. CODE § 13A-11-30 (2018) ("[To eavesdrop is] [t]o overhear, record, amplify or transmit any part of the private communication of others without the consent of at least one of the persons engaged in the communication, except as otherwise provided by law.").

16. *Eavesdropping*, BLACK'S LAW DICTIONARY (10th ed. 2014).

17. *See Wiretapping*, BLACK'S LAW DICTIONARY (10th ed. 2014) (defining "wiretapping" as "[e]lectronic or mechanical eavesdropping") [hereinafter *Wiretapping*, BLACK'S LAW DICTIONARY].

18. *Compare* KY. REV. STAT. ANN. § 526.020 (West 2018) ("A person is guilty of eavesdropping when he intentionally uses any device to eavesdrop, whether or not he is present at the time."), *with* MO. REV. STAT. § 542.402 (2017) (indicating that a person is guilty of "illegal wiretapping" if he or she "[k]nowingly intercepts, [or] endeavors to intercept," any wire or oral communication). *But cf.* COLO. REV. STAT. § 18-9-303 (2018) (stating that an individual commits a wiretap when he or she "overhears, reads, takes, copies, or records a telephone, telegraph, or electronic communication"); COLO. REV. STAT. § 18-9-304 (indicating that an individual eavesdrops when he or she "[k]nowingly overhears or records . . . [a] conversation or discussion" to which the eavesdropper is not "visibly present").

19. *Wiretapping*, BLACK'S LAW DICTIONARY, *supra* note 17.

20. 18 U.S.C. § 2510(4) (2012) ("'[I]ntercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.").

21. *Id.* § 2510(17)(A)–(B) (defining "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," as well as the storage of those communications "by an electronic communication service for purposes of backup protection of such communication").

22. For example, the Supreme Court decided a case in which police officers accessed cell phone tower records without a warrant in order to place the defendants at the locations of multiple burglaries. Carpenter v. United States, 138 S. Ct. 2206, 2212–13 (2018). The defendants argued, and the Court agreed, that accessing the records without a warrant violated the Fourth Amendment. *Id.* at 2219.

23. VT. STAT. ANN. tit. 13, §§ 8101–08 (2017).

B. Federal Common Law

Over time, the U.S. Supreme Court has expanded the reach of the Fourth Amendment from a more literal interpretation to a broader, conceptual interpretation to protect individual privacy against modern technology. In 1928, the Court first addressed whether wiretapping violated the Fourth Amendment in *Olmstead v. United States*.[24] Olmstead ran an illegal rum-runner operation during Prohibition, smuggling liquor by boat from British Columbia into Seattle and then distributing it around the city.[25] Federal prohibition officers tapped several phones associated with Olmstead's operations.[26] Olmstead and 11 associates received convictions for violating the National Prohibition Act.[27] Evidence obtained from wiretaps conducted by the prohibition officers formed the basis for the defendants' convictions.[28] Olmstead and the other petitioners challenged their convictions, claiming that the wiretaps were an unreasonable search and seizure in violation of the Fourth Amendment.[29]

Applying a strict textualist interpretation, the Court held that wiretapping did not violate the Fourth Amendment.[30] Because the "historical purpose of the Fourth Amendment . . . was to prevent the use of governmental force to search a man's house, his person, his papers and his effects," the Court concluded that "the search [must] be of *material things*— the person, the house, his papers or his effects."[31] Therefore, a search must involve a physical trespass into a private space to violate the Fourth Amendment.[32] In the Court's view, telephone wires merely allowed people to talk with one another at a greater distance, and listening through a

---

24. Olmstead v. United States, 277 U.S. 438, 455 (1928).

25. *Id.* at 456.

26. *Id*. Prohibition officers were agents of the Bureau of Prohibition. The Bureau was created under the Volstead Act, which regulated enforcement of the Eighteenth Amendment. National Prohibition (Volstead) Act, Pub. L. No. 66, ch. 5, 41 Stat. 306 (1919).

27. *Olmstead*, 277 U.S. at 455.

28. The officers intercepted communications detailing the time and place of boat deliveries from Canada and calls from customers placing orders. *Id.* at 456–57.

29. *Id.* at 455.

30. *Id.* at 464.

31. *Id.* at 463–64 (emphasis added).

32. *Id.* at 466 ("Neither the cases we have cited nor any of the many federal decisions brought to our attention hold the Fourth Amendment to have been violated as against a defendant unless there has been an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure.").

wiretap was the same as overhearing a face-to-face conversation.[33] The prohibition officers' use of wiretaps did not violate the Fourth Amendment because there was no physical trespass.[34] Thus, they had obtained evidence not through the search or seizure of any material thing, but "by the use of the sense of hearing and that only."[35]

In his dissent, Justice Brandeis advocated for a broader interpretation of the Fourth Amendment.[36] In his view, the Constitution protects against certain evils and those protections should not "be necessarily confined to the form that evil had theretofore taken."[37] In other words, the drafters used their own experiences as a framework for the *principles* they intended to enshrine in the Constitution, but they did not intend for its protections to apply only to their specific *experiences*.[38] According to Justice Brandeis, the Fourth Amendment fundamentally protects against governmental invasion of individual privacy, which the drafters had only experienced as a physical invasion.[39] Consequently, Justice Brandeis believed the Court should interpret the Fourth Amendment to prohibit the government from *any* invasion of privacy, not only the physical invasion the drafters had experienced.[40]

The *Olmstead* decision led to the widespread, authorized use of wiretapping by both government and private actors for several decades, during which time both communications and wiretap technology evolved.[41] The Communications Act of 1934 prohibited the dissemination or interception of radio or wire transmissions, with an exception for law enforcement with a subpoena.[42] The Act applied only to actions that

---

33. *Id.* Chief Justice Taft likened a telephone wire to a long-distance loudspeaker, saying that "one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside." *Id.*

34. *Id.* at 464.

35. *Id.*

36. *Id.* at 472 (Brandeis, J. dissenting).

37. *Id.* (quoting Weems v. United States, 217 U.S. 349, 373 (1910)).

38. *Id.*

39. *Id.* at 473.

40. *Id.* at 478.

41. Bast, *supra* note 4, at 840. *See, e.g.*, Alan F. Westin, *The Wire-Tapping Problem: An Analysis and a Legislative Proposal*, 52 COLUM. L. REV. 165, 197–98 (1952) (discussing, in 1952, the issues with widespread wiretapping in the wake of *Olmstead*, and the inability of the law to keep pace with technology). *See also* Arthur C. Clarke, *Extra-Terrestrial Relays – Can Rocket Stations Give World-wide Radio Coverage?*, WIRELESS WORLD, Oct. 1945, at 305–08 (1945) (proposing for the first time using satellites for communication relay); G.W.A. DRUMMER, ELECTRONIC INVENTIONS AND DISCOVERIES 150 (3d ed. 1983) (describing the first transatlantic telephone cable, which went into service on September 25, 1956 and connected North America and Europe via Scotland and Newfoundland).

42. Communications Act of 1934, ch. 652, 48 Stat. 1064, 1103 (codified as amended at 47 U.S.C. § 605 (2012)).

involved a wire or radio transmission.[43] It did not cover any other type of interception, such as listening through walls, or wearing a wire to record a conversation.[44] Previous arguments that the Fourth Amendment prohibited surreptitious recordings not prohibited by the Communications Act had been unsuccessful.[45] Those arguments failed because the wiretaps did not involve a physical invasion, which was an essential element of a Fourth Amendment violation under *Olmstead*.[46]

However, the Court changed course in the early 1960s. In 1961, the Court ruled in *Silverman v. United States* that recording oral communications did constitute a search and seizure under the Fourth Amendment.[47] Six years later, in *Katz v. United States*, the Court overturned *Olmstead*, holding a search and seizure did not require a physical trespass, thereby bringing wiretapping within the scope of Fourth Amendment protections.[48]

In *Silverman*, police officers used a microphone to record conversations that incriminated multiple defendants of illegal gambling.[49] The officers were in an adjoining row house and used the shared heating ducts to run a microphone into the defendants' home.[50] The Court held that the recording violated the Fourth Amendment because the officers used the microphone in a way that physically entered the defendants' home.[51] Although *Silverman* brought the recording of oral communications within the scope of the Fourth Amendment, the Court declined to extend its ruling

---

43. *Id. See also* Goldman v. United States, 316 U.S. 129, 133 (1942) ("Words spoken in a room in the presence of another into a telephone receiver do not constitute a communication by wire within the meaning of the [Communications Act].").

44. *See Goldman*, 316 U.S. at 133 (holding that the use of a detectaphone, a device that was pressed against the wall to hear what was said on the other side, to listen to the defendant having a conversation over the telephone, was not a violation of the Communications Act); On Lee v. United States, 343 U.S. 747, 752, 754 (1952) (stating that a conversation between a police informant and the defendant in the defendant's laundry business, which was transmitted to a police officer stationed outside by a wire worn by the informant, was not a violation of the Communications Act).

45. *See* Westin, *supra* note 41, at 174–78 (providing an overview of unsuccessful Fourth Amendment challenges after *Olmstead*).

46. *See Goldman*, 316 U.S. at 134–35 (finding that the use of a detectaphone did not violate the Fourth Amendment because there was no physical trespass); *On Lee*, 343 U.S. at 754 (holding that an informant wearing a radio transmitter was not a physical trespass because the device had "the same effect on his privacy as if agent Lee had been eavesdropping outside an open window").

47. Silverman v. United States, 365 U.S. 505, 511 (1961).

48. Katz v. United States, 389 U.S. 347, 353 (1967) (citing *Silverman*, 365 U.S. at 511).

49. *Silverman*, 365 U.S. at 506.

50. *Id.*

51. *Id.* at 512 ("[The] decision here does not turn upon the technicality of a trespass upon a party wall as a matter of local law. It is based upon the reality of an actual intrusion into a constitutionally protected area.").

to recordings that did not involve a physical trespass.[52] The Court did not find it necessary to reassess its previous holding in *Olmstead*, stating:

> We are told that re-examination of the rationale . . . of *Olmstead v. United States* . . . is now essential in the light of recent and projected developments in the science of electronics . . . . We need not here contemplate the Fourth Amendment implications of these and other frightening paraphernalia which the vaunted marvels of an electronic age may visit upon human society.[53]

Despite the Court's unwillingness to reassess those implications in *Silverman*, the Court overturned *Olmstead* only six years later in *Katz v. United States*.[54] The government convicted Katz for violating interstate gambling laws, based on evidence obtained by FBI agents who recorded Katz's phone calls in a public phone booth.[55] In a stark departure from *Olmstead,* the Court held that a physical trespass was no longer an essential element of a search under the Fourth Amendment.[56] According to the Court, the Fourth Amendment protects individuals in any situation where they have a reasonable expectation of privacy, not only when the government trespasses upon their physical, private property.[57]

The Court in *Katz* emphasized that "the Fourth Amendment protects people, not places."[58] Recognizing the way that society's perceptions of telephones had evolved since *Olmstead*, the Court held that failing to recognize a reasonable expectation of privacy in a phone booth would "ignore the vital role that the public telephone has come to play in private communication."[59] The Court indicated that Fourth Amendment protections must evolve over time to adapt to new technology and changing social and cultural norms.[60] This more flexible, conceptual interpretation upheld the spirit of the Fourth Amendment, in which the framers intended to protect an individual's reasonable expectation of privacy against government intrusion.[61]

---

52. *Id.* ("We find no occasion to re-examine *Goldman* here, but we decline to go beyond it, by even a fraction of an inch.").

53. *Id.* at 508–09.

54. Katz v. United States, 389 U.S. 347, 353 (1967).

55. *Id.* at 348–49. There was no physical trespass in *Katz* because recording device was located on the outside of the phone booth. *Id.*

56. *Id.* at 353.

57. *Id.*

58. *Id.* at 351.

59. *Id.* at 352.

60. *Id.* at 351–52.

61. *Id.* at 350.

C. Federal Statutory Law

In response to the Court's ruling in *Katz*,[62] and in order to clarify federal authority to wiretap, Congress passed Title III.[63] Title III covered only "wire or oral communication."[64] Under the ECPA, Congress modified the language of Title III to include "wire, electronic, or oral communication."[65] The ECPA, which remains in force today,[66] generally prohibits the interception of wire, electronic, or oral communication, as well as the disclosure of information obtained through interception.[67] Wiretapping is permissible under the ECPA when one party to a communication conducts the interception or consents to third-party interception.[68] Wiretapping by law enforcement (or others acting under the color of law) is also permitted, but typically requires authorization in the form of a warrant.[69] Except for those situations, the ECPA prohibits interception and disclosure by both government and private actors.[70]

Title III and the ECPA have undoubtedly helped to define the scope of prohibited and permitted wiretapping.[71] Nevertheless, federal courts have experienced challenges in applying the law to new technology.[72] One issue courts have addressed is whether new technology is a form of "wire,

---

62. *See* S. REP. NO. 90-1097, at 28 (1968) (indicating that the "proposed legislation [in Title III] conforms to the constitutional standards set out" in *Katz*).

63. Omnibus Crime Control and Safe Street Act of 1968, Pub. L. No. 90-351, § 802, 82 Stat. 197, 212 (codified as amended at 18 U.S.C. §§ 2510–22 (2012)).

64. *Id.* § 802, 82. Stat. at 213.

65. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 101, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510–22(2012)).

66. Since 1986, Congress has made some minor modifications to 18 U.S.C. §§ 2510–22, but the ECPA still generally remains in force. *See, e.g.*, Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 202, 108 Stat. 4279, 4290–91 (1994) (adding "cordless telephone communication that is transmitted between the cordless telephone handset and the base unit" to §§ 2511(4)(b)(i)–(ii)); FISA Amendments Act of 2008, Pub. L. No. 110-261, § 403, 122 Stat. 2436, 2474 (making technical and conforming amendments to § 2511(2)(a)(ii)(A) to comply with related FISA amendments).

67. 18 U.S.C. § 2511(1)(a)–(c) (2012).

68. *Id.* § 2511(2)(c).

69. *Id.* § 2511(2).

70. *Id.* § 2511(1) (referring to "any person").

71. *Compare* § 2511 (listing prohibited forms of interception), *with* § 2516 (listing authorized forms of interception).

72. *See, e.g.*, Edward P. Sisk, Note, *Technical Difficulties: Protecting Privacy Rights in the Digital Age*, 42 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 101, 111–12 (2016) (discussing how "courts have repeatedly criticized the ECPA for being confusing and difficult to apply"); Sara E. Brown, Note, *An Illusory Expectation of Privacy: The ECPA Is Insufficient to Provide Meaningful Protection for Advanced Communication Tools*, 114 W. VA. L. REV. 277, 295–96 (2011) (noting the federal court circuit split of the ECPA to "advanced communication tools").

electronic, or oral communication."[73] Another problem that arises is whether the courts consider the manner in which the new technology works as performing an "intercept[ion]."[74]

Technology has evolved at an increasingly fast pace while the challenges of applying wiretap statutes to new technology have remained the same.[75] For example, in 1976, the Fifth Circuit addressed the use of a cassette tape to intercept a communication.[76] In that case, police found a cassette during a search of an individual's car.[77] The officers listened to the tape and discovered that it contained a phone call recording that incriminated the defendant.[78] The court had no difficulty finding that the individual who tape-recorded his conversation with the defendant had intercepted the communication.[79] The more complicated issue was whether the officers had also intercepted the communication when they listened to the tape.[80] The court concluded that it would be an overly broad interpretation of the statute to include listening to a recording made by someone else in the definition of an interception.[81]

In 2002, the Ninth Circuit also addressed what constitutes an interception, but in the context of a website rather than a cassette tape.[82] The court had to determine if viewing information on another person's

---

73. 18 U.S.C. § 2510(1)–(2). *See, e.g.*, United States v. Steiger, 318 F.3d 1039, 1047 (11th Cir. 2003) (holding that information obtained by hacking into another person's computer was an "electronic communication[]" because it was transferred to the hacker via one of the mediums listed in the statute).

74. 18 U.S.C. § 2510(4). *See, e.g.*, United States v. Herring, 933 F.2d 932, 934, 939 (11th Cir. 1993) (holding that a device that unscrambles satellite television signals accomplishes an "interception" despite the fact that the communications are first received by the satellite dish connected to the device).

75. *See* ACLU, *supra* note 6 (distinguishing the technology in 1986, when Congress enacted the ECPA, from modern technology and arguing that "[o]nline privacy law shouldn't be older than the Web"). *See also* Carlos Perez-Albuerne & Lawrence Friedman, *Privacy Protection for Electronic Communications and the "Interception-Unauthorized Access" Dilemma*, 19 J. MARSHALL J. COMPUTER & INFO. L. 435, 440–45 (2000) (providing a brief historical overview of different cases involving statutory interpretations of the term "intercept"); Béla Nagy et al., *Statistical Basis for Predicting Technological Progress*, 8 PLOS ONE 1, 7 (Feb. 2013), https://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0052669&type=printable (indicating that there is a "strong tendency, across different types of technologies, toward constant exponential growth rates," and "super-exponential improvement for information technologies over long time spans").

76. United States v. Turk, 526 F.2d 654, 657 (5th Cir. 1976).

77. *Id.* at 656.

78. *Id*. at 656–57.

79. *Id.* at 657.

80. *Id.*

81. *Id*. at 658 ("The argument that a new and different 'aural acquisition' occurs each time a recording of an oral communication is replayed is unpersuasive. That would mean that innumerable 'interceptions,' and thus violations of the Act, could follow from a single recording.").

82. Konop v. Hawaiian Airlines, 302 F.3d 868, 876 (9th Cir. 2002).

secure website constituted an interception.[83] The court found that, to qualify as an interception, the communication "must be acquired during transmission, not while it is in electronic storage."[84] Although the scope and reach of federal wiretap laws has increased significantly, new technology continues to complicate the interpretation and application of those laws.

D. State Wiretap Laws

States proactively passed wiretap laws long before the federal government took action: at the time of the *Olmstead* decision in 1928, 26 states had laws criminalizing wiretapping and 35 states prohibited telephone and telegraph operators from disclosing communications.[85] Today, all states except Vermont have enacted a wiretap statute.[86] Wiretapping is a criminal offense under all but three state wiretap laws, but only 35 states allow for civil action.[87] Thirteen states have two-party consent laws, which prohibit an interception unless all parties to a communication to consent to it.[88] The remaining 36 states require single-party consent, as does the federal statute.[89] Under single-party consent laws, only one party to a communication must consent to its interception for the wiretap to be valid.[90] These consent rules apply regardless of whether the interceptor is a party to the communication.[91]

E. Vermont Common Law

Vermont is the only state that does not have a wiretap statute to protect citizens from interception of private communications.[92] In the absence of such law, Vermont courts apply the Supreme Court's analysis from *Katz* to the state constitution, which contains a search and seizure provision—

---

83. *Id.* at 874.

84. *Id.* at 878.

85. *See* Olmstead v. United States, 277 U.S. 438, 479 n.13 (1928) (listing state statutes in effect at the time of the opinion).

86. Bast, *supra* note 4, at 868.

87. *Id.*

88. *Id.* at 930. Some states require two-party consent to all communications, but others only require two-party consent to certain types of communications. *See, e.g.*, CONN. GEN. STAT. § 52-570d (2017) (requiring two-party consent only for interception of "oral private telephonic communication").

89. Bast, *supra* note 4, at app. B at 930.

90. *Id.* at 869.

91. *Id.* For example, in a single-party consent state, if an individual records his or her own phone conversation with the other caller, then it is a valid interception. Alternatively, either caller could consent to a third-party interception, such as an informant making a phone call to a suspect while a law enforcement officer listens.

92. *Id.* at 868.

Article 11—similar to the Fourth Amendment.[93] Vermont courts generally find that an interception violates Article 11 of the Vermont Constitution if the interception occurs where the individual has a reasonable expectation of privacy.[94] The following cases illustrate Vermont's current approach.

In *State v. Blow*, an undercover police officer wearing an electronic radio transmission device entered Blow's residence to buy drugs.[95] A detective stationed outside listened to and recorded the transmitted conversation.[96] Blow objected to the admission of the recording as an unlawful search and seizure in violation of the state constitution.[97] In its analysis, the court adopted Justice Harlan's concurrence in *Katz*, establishing a two-part test to determine whether Blow had a reasonable expectation of privacy.[98] The test requires "first that a person ha[s] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable."[99] The court recognized the possible effect of evolving technology, stating that "[i]n assessing the constitutionality of technologically enhanced government surveillance in a particular case, [the court] must identify the values that are at risk, and vest the reasonable-expectation-of-privacy test with those values."[100]

The court concluded that Blow had not intended to transmit the conversation outside his home, satisfying the first part of the test.[101] The court also held that "reasonableness" under the second part of the test "must be tied to identifiable constitutional values."[102] Because "Article 11 concerns the deeply-rooted legal and societal principle that the coveted

---

93. *Compare id.* at 841 (summarizing the Supreme Court's holding in *Katz* that Fourth Amendment protections extend to a private conversation in a public telephone booth), *with id.* at 863–64 (explaining the Vermont Supreme Court's holding in *Blow* that a defendant had "no reasonable expectation of privacy" in a public parking lot). *See also* VT. CONST. ch. I, art. 11 ("That the people have a right to hold themselves, their houses, papers, and possessions, free from search or seizure, and therefore warrants without oath or affirmation first made, affording sufficient foundation for them, and whereby by any officer or messenger may be commanded or required to search suspected places, or to seize any person or persons, his, her, or their property, not particularly described, are contrary to that right, and ought not to be granted.").

94. Bast, *supra* note 4, at 863.

95. State v. Blow, 157 Vt. 513, 514, 602 A.2d 552, 553 (1991).

96. *Id.*

97. *Id.* at 515, 602 A.2d at 555.

98. *Id.* at 517, 602 A.2d at 555.

99. *Id.* (alteration in original) (internal quotations omitted) (quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

100. *Id.* at 518, 602 A.2d at 555.

101. *Id.* (citing *Katz*, 389 U.S. at 351).

102. *Id. See also* VT. CONST. ch. I, art. 11 (stating that "the people have a right to hold themselves, their houses, papers, and possessions, free from search or seizure").

privacy of the home should be especially protected," Blow therefore had a reasonable expectation of privacy because he was in his own home when the officer recorded and transmitted the conversation.[103]

In *State v. Geraw*, a case very similar to *Blow*, the court held that the defendant still had a reasonable expectation of privacy even when the police officer involved was not undercover.[104] Once again, the court focused on the importance of the conversation having taken place in the defendant's home.[105] The officer was uniformed and began the conversation by telling the defendant that he was investigating an allegation that the defendant had sexually abused a minor.[106] That the officer in *Geraw* was uniformed (unlike the officer in *Blow*) was irrelevant in the eyes of the court, "for the heart of [its] holding in *Blow* was a recognition of the 'deeply-rooted legal and societal principle that the coveted privacy of the home should be especially protected.'"[107]

One fact the court did find relevant in *Geraw* was that the officer concealed the recording device from the defendant.[108] When speaking with a police officer, an individual "should reasonably expect that the conversation will be carefully noted and subsequently repeated," but that person should not expect that the officer will record the conversation, thereby "exposing every word and phrase one speaks, every inflection or laugh or aside one utters, to the scrutiny of the world at large."[109] The court concluded that the officers hid the recording device from the defendant because they "understood that his expectations and, hence, his very words might be different if he knew that he was being recorded."[110]

Vermont's common law approach to wiretapping protects only against interceptions made by government actors without a warrant.[111] The courts

---

103. *Blow*, 157 Vt. at 517, 602 A.2d at 555. In another case decided on the same day as *Blow*, the court concluded that there was no reasonable expectation of privacy where a conversation was similarly transmitted and recorded, but took place in a shopping center parking lot through an open car window. State v. Brooks, 157 Vt. 490, 493, 601 A.2d 963, 963–64 (1991).

104. State v. Geraw, 173 Vt. 350, 354, 795 A.2d 1219, 1222 (2002).

105. *Id.*, 795 A.2d at 1223.

106. *Id.* at 352, 795 A.2d at 1220–22.

107. *Id.* at 354, 795 A.2d at 1222–23 (quoting *Blow*, 157 Vt. at 517, 602 A.2d at 555).

108. *Id.* at 357, 795 A.2d at 1225 ("The dissent would excuse the underhanded method the police utilized in this case to record the conversation with defendant, insisting that it was not 'trickery.' With respect, if it was not trickery to hide a tape recorder to secretly record a conversation with an unsuspecting citizen, what was it?").

109. *Id.* at 356–57, 795 A.2d at 1224.

110. *Id.* at 357, 795 A.2d at 1224.

111. VT. STAT. ANN. tit. 13, § 8108 (2018).

have placed a strong emphasis on the privacy of an individual's home.[112] This emphasis essentially makes any interception inside an individual's home a *de facto* violation of the state constitution.

F. Current Vermont Statutory Law

Notwithstanding the absence of a broad, all-encompassing wiretap statute in Vermont, there are some narrow statutory privacy protections within existing laws. Vermont's voyeurism statute prohibits recording an individual without his or her knowledge.[113] However, this only applies when the individual is "in a place where he or she would have a reasonable expectation of privacy *within* a home or residence."[114] Additionally, in June 2016, Vermont passed Act 169, titled "An act relating to privacy protection and a code of administrative rules."[115] The Act addresses one new technology in particular that poses a danger to privacy: it includes a provision requiring law enforcement to obtain a warrant in order to use drones for surveillance.[116] The Act also includes a prohibition on real-time interception by law enforcement officers without a warrant.[117] However, this essentially only codifies the protections already afforded by the state constitution and provides no protection against interception by private actors.[118]

G. Inadequacies of Vermont's Current Approach

Vermont's current approach does not provide sufficient guidance to courts faced with interpreting new technology. A lack of clarity can lead to incongruous decisions depending on how individual judges interpret

---

112. *See, e.g.*, State v. Blow, 157 Vt. 513, 518, 602 A.2d 552, 555 (1991) (emphasizing that "the deeply-rooted . . . societal principle that the coveted privacy of the home should be especially protected").

113. VT. STAT. ANN. tit. 13, § 2605 (2017).

114. *Id.* (emphasis added).

115. 2016 Vt. Acts & Resolves 169 (codified as amended in scattered sections of VT. STAT. ANN.). The most relevant section of Act 169 was codified at VT. STAT. ANN. tit. 13, §§ 8101–08 (2017).

116. VT. STAT. ANN. tit. 20, §§ 4621–24 (2017).

117. VT. STAT. ANN. tit. 13, § 8108 (2017).

118. *Compare id.* ("A law enforcement officer shall not use a device which . . . intercepts in real time from a user's device a transmission of communication content, real time cellular tower-derived location information, or real time GPS-derived location information, except for purposes of locating and apprehending a fugitive for whom an arrest warrant has been issued."), *with* VT. CONST. ch. 1, art. 11 (prohibiting "warrants without oath or affirmation first made, affording sufficient foundation for them" from authorizing "any officer or messenger . . . to search suspected places, or to seize any person or persons, his, her, or their property").

technology.[119] In *Geraw*, the court made an acknowledgement that draws attention to this weakness in Vermont's current approach to wiretapping:

> We have, to be sure, disagreed at times about the degree of emphasis to be placed on the location of the search and seizure, to the exclusion of other considerations, such as *advanced technologies* that may alter or intensify the nature of the intrusion.[120]

Although the court adopted Justice Harlan's reasonable-expectation-of-privacy test, it is still unclear how much value to assign different factors, especially the technology involved.[121] Additionally, changing technologies are subject to the court's interpretation of their importance.[122]

A court's interpretation of how technology works, and the purpose it serves, can have serious ramifications for the future.[123] For example, the U.S. Supreme Court's interpretation of telephones in *Olmstead* permitted wiretapping of private conversations for decades.[124] This is especially true when technology's role or function in society evolves over time—Chief Justice Taft could not predict how integral telephones would become to everyday life.[125] He certainly could not have predicted that less than 100 years after *Olmstead*, most Americans would carry phones in their pockets and purses and that making calls would not be the phone's most important or common function.[126]

---

119. *See* Suzanne M. Monte, *The Lack of Privacy in Vermont*, 24 VT. L. REV. 199, 224–25 (1999) (detailing how the Vermont Supreme Court's interpretation of the "modified open fields doctrine," in which there is a reasonable expectation of privacy in an open field only when the landowner purposefully excludes others from their land by use of signage or fencing, led to a result that was contrary to public perceptions of privacy, and a "complicated and imprecise" application of the doctrine).

120. State v. Geraw, 173 Vt. 350, 353, 795 A.2d 1219, 1222 (2002) (emphasis added).

121. *Id.* at 353–54, 795 A.2d at 1222.

122. "Judges struggle to understand even the basic facts of such technologies, and often must rely on the crutch of questionable metaphors to aid their comprehension. Judges generally will not know whether those metaphors are accurate, or whether the facts before them are typical or atypical given the technology of the past or the present." Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 875–76 (2004).

123. *Id.* at 843–45.

124. *See* Westin, *supra* note 41, at 168–69 (discussing the continued impact of *Olmstead* nearly thirty years later); Katz v. United States, 389 U.S. 347, 353 (1967) (noting that the Court "ha[d] since departed from the narrow view on which [the] decision [in *Olmstead*] rested").

125. *See Katz*, 389 U.S. at 352–53 (holding that failing to expand Fourth Amendment protections to a public phone booth would "ignore the vital role that the public telephone has come to play in private communication").

126. *See* Amanda Ray, *The History and Evolution of Cell Phones*, ART INSTS.: BLOG (Jan. 22, 2015), https://www.artinstitutes.edu/about/blog/the-history-and-evolution-of-cell-phones (explaining how "the purpose of the cell phone has shifted from a verbal communication tool to a multimedia tool,"

The lack of a clear, unified approach to interpreting wiretapping is also evident in Justice Skoglund's dissent in *Geraw*.[127] Justice Skoglund argued that the importance of protecting privacy in the home should not automatically create a reasonable expectation of privacy any time a conversation takes place there.[128] She highlighted several other courts that had reached different conclusions in cases involving an officer in a defendant's home.[129] She also emphasized several times that Geraw *invited* the officer into his home and knew that the officer was there to discuss the sexual assault allegations against him.[130] Justice Skoglund concluded: "I hesitate to speak for society as a whole, but respectfully suggest that Vermonters would not find reasonable a suspect's expectations that his responses to police questions about possible involvement in a crime are private."[131] Thus, not only is the current approach unclear and uneven, it may not accurately reflect Vermonters' values.

Justice Skoglund's dissent exposes another issue with the current Vermont approach.[132] In the absence of a statute, the courts are developing the state's approach to wiretapping.[133] This creates a twofold problem: first, this is a reactive, rather than proactive, approach; second, impartial, objective judges are less capable than elected representatives at developing a law that reflects the values and concerns of all Vermonters.[134]

Judge-made law is reactionary.[135] There must be an injury-in-fact before a plaintiff can bring a claim, and the judicial process can take a considerably long time.[136] As Professor Orin Kerr notes, reliance on judicial rulemaking "leads to Fourth Amendment rules that tend to lag behind

---

and that cell phones are now more often used "for surfing the web, checking email, snapping photos, and updating our social media status than actually placing calls").

127. State v. Geraw, 173 Vt. 350, 362–63, 795 A.2d 1219, 1227–28 (2002) (Skoglund, J., dissenting).

128. *Id.*, 795 A.2d at 1230.

129. *Id.* at 365–66, 795 A.2d at 1228–30.

130. *Id.*, 795 A.2d at 1231 ("I return again to the fact that defendant invited the officers into his home and agreed to answer questions surrounding their investigation.").

131. *Id.* at 368, 795 A.2d at 1233.

132. *Id.* at 361–68, 795 A.2d at 1228–33.

133. *Id.*

134. *See* Monte, *supra* note 119, at 223–24 (explaining how the Vermont Supreme Court's "modified open fields doctrine" failed to consider society's views on privacy and police surveillance).

135. Jeffery A. Pojanowski, *Reading Statutes in the Common Law Tradition*, 101 VA. L. REV. 1357, 1360 (2015).

136. *See* Kerr, *supra* note 122, at 868 ("For a trial court to address the Fourth Amendment implications of a technology, . . . the use of the technology must yield evidence of a crime; it must lead to an arrest; and then it must lead to a constitutional challenge requiring judicial resolution. Appellate decisions come only much later.").

parallel statutory rules and current technologies by at least a decade."[137] This lag "result[s] in unsettled and then outdated rules that often make little sense given current technological facts."[138] If Vermont continues to rely on judicial rulemaking to address wiretapping while technology evolves at an exponential rate, the lag between rules and technology will become even more pronounced.[139]

To combat this lag between judicial rulemaking and technology, Vermont's legislature must take control over the state's approach to wiretapping. The legislature can respond to emerging technology much faster than the courts.[140] Professor Kerr explains that the legislature is positioned to draft a law that better reflects societal values because "[l]egislative rules tend to be the product of a wide range of inputs, ranging from legislative hearings and poll results to interest group advocacy and backroom compromises."[141] Conversely, judicial rulemaking "tend[s] to follow from a more formal and predictable presentation of written briefs and oral arguments by two parties."[142] Thus, the legislature can draft a statute that considers the values of all Vermonters, not just two opposing parties arguing before a court.

The current Vermont approach to wiretapping does not provide courts with sufficient guidance to make uniform rulings.[143] Relying on judicial rulemaking creates rules that lag far behind current technology.[144] The current approach also fails to consider a broad range of perspectives and input from Vermonters, resulting in rules that may not reflect societal values.[145] This approach inadequately addresses concerns with current

---

137. *Id.*

138. *Id.*

139. *See* Nagy, *supra* note 75, at 7 (describing the "constant exponential growth rate[]" of technology over time, along with "super-exponential improvement for information technologies over long time spans").

140. *See* Kerr, *supra* note 122, at 870 ("Unburdened by the procedural barriers that limit and delay judicial power, legislatures can enact comprehensive rules far ahead of current practice rather than decades behind it."). For example, Kerr notes that the ECPA regulated email privacy in 1986, long before many Americans had even heard of email. *Id.* Congress has even enacted legislation involving technology before it was invented, such as blocking funding for Pentagon research to develop new data-mining technology. *Id.*

141. *Id.* at 875.

142. *Id.*

143. *See* Monte, *supra* note 119 (referencing the inconsistency in court rulings based on the current law).

144. See Kerr, *supra* note 122, at 868 (Reliance on rulemaking "leads to Fourth Amendment rules that tend to lag behind parallel statutory rules and current technologies by at least a decade . . . .").

145. *See infra* Section III (describing cases involving statutory interpretation of wiretap statutes).

technology, and it will become increasingly ineffective as technology continues to evolve.

II. NEW TECHNOLOGY REQUIRES A PROACTIVE APPROACH TO PROTECT CITIZENS

As technology advances, it also becomes increasingly easy to use technology to intercept private communications.[146] For example, most smartphones have microphones, high-resolution cameras, voice control, and a constant connection to a wireless network or internet service.[147] These devices can easily intercept private communications.[148] The current Vermont approach would protect against those interceptions only if done by law enforcement without a warrant,[149] or in a place within a person's residence where they would have a reasonable expectation of privacy.[150] Almost all interceptions done by private actors are outside the scope of Vermont's current approach to wiretapping.

Even though protection against unreasonable governmental interference into individual privacy is a fundamental constitutional right, protection against unauthorized interceptions by private actors is particularly important today.[151] The widespread use of smartphones and the

---

146. *See, e.g.*, Stephanie K. Pell & Christopher Soghoian, *Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J. L. & TECH. 1, 46 (2014) (describing how "[s]urveillance has become democratized and, correspondingly, the motives for surveillance have multiplied" because of lower costs and greater accessibility to interception technology).

147. *See Smartphone Features*, PCMAG ENCYCLOPEDIA, https://www.pcmag.com/encyclopedia/term/64233/smartphone-features (last visited Dec. 4, 2018) (listing the primary built-in features and optional downloadable features of smartphones).

148. *See, e.g.*, Commonwealth v. Smith, 136 A.3d 170, 178 (Pa. Super. Ct. 2016) (finding that a smartphone "voice memo" app was an "interception device" under Pennsylvania's wiretap statute).

149. VT. STAT. ANN. tit. 13, § 8108 (2017). Additionally, the current approach does not provide sufficient guidance to law enforcement on when to obtain a warrant. *See, e.g.*, State v. Lizotte, 2018 VT 92, ¶ 1 (discussing whether law enforcement invalidated a warrant by opening an email attachment); State v. Wetter, 2011 VT 111, ¶ 15, 190 Vt. 476, 483, 35 A.3d 962, 968 (holding that a detective did not require a warrant to monitor a phone conversation between the defendant and an informant). Therefore, a wiretap statute would benefit law enforcement by clarifying the circumstances when a warrant is necessary. *Cf.* United States v. Staffeldt, 451 F.3d 578, 579–80 (9th Cir. 2006), *amended in part by* 523 F.3d 983 (9th Cir. 2008) ("[The ECPA] contains strict controls governing the issuance of wiretap warrants, and the use of wiretaps, in criminal investigations. Because Congress recognized the grave threat to privacy that wiretaps pose, it spelled out in elaborate and generally restrictive detail the process by which wiretaps may be applied for and authorized.") (internal citation and quotations omitted).

150. VT. STAT. ANN. tit. 13, § 2605 (2017).

151. *See* Sam Kamin, *The Private is Public: The Relevance of Private Actors in Defining the Fourth Amendment*, 46 B.C. L. REV. 83, 117–18 (2004) (discussing private conduct facilitated by modern technology that has raised new privacy concerns, such as workplace surveillance, consumer information misuse, and medical privacy intrusions); Margot E. Kaminski, *Robots in the Home: What*

increasing prevalence of devices such as Google Home and Amazon Echo[152] create a greater likelihood than ever before that someone, or some*thing*, is monitoring private communications.[153] Unique, unanticipated legal questions will almost certainly arise from this new technology: where does a reasonable expectation of privacy exist when someone carries their smartphone with them at all times?[154] Does a device owner consent to be recorded by their device at any time, or only when the owner expressly consents?[155] What about smart devices, like fitness trackers, or even home appliances—can those be *interception devices*?[156]

There are numerous examples—including many found in this Note—of how statutory language may constrain the application of a wiretapping law to new technology.[157] However, the absence of any comprehensive statutory provision provides even less protection against new forms of surreptitious surveillance and recording than a statute with outdated language.[158]

Will We Have Agreed to?, 51 IDAHO L. REV. 661, 664–66 (2015) (providing an overview of legal privacy considerations posed by household robots).

152. Google Home and Amazon Echo are both *smart speakers*, combining a wireless speaker with a virtual assistant that is controlled via voice command. New versions of these devices may include other features such as a camera that users can access remotely. *Amazon Echo*, PCMAG ENCYCLOPEDIA, https://www.pcmag.com/encyclopedia/term/67188/amazon-echo (last visited Dec. 4, 2018); *Google Home*, PCMAG ENCYCLOPEDIA, https://www.pcmag.com/encyclopedia/term/69078/google-home (last visited Dec. 4, 2018).

153. *See* Agatha French, *Q&A: Alexa May Be Listening, But Will She Tell on You?*, L.A. TIMES (Jan. 5, 2017), http://www.latimes.com/business/technology/la-fi-tn-amazon-echo-privacy-qa-20170105-story.html (discussing the potential privacy issues posed by Amazon Echo and similar devices).

154. *See* Huff v. Spaw, 794 F.3d 543, 556 (6th Cir. 2015) (finding that the owner of a cell phone did not have a reasonable expectation of privacy when he "pocket-dialed" a co-worker who recorded a conversation between the cell phone owner and his wife, but finding that the wife did have a reasonable expectation of privacy because she could not "be held responsible for her husband's pocket-dial").

155. *See* Kaminski, *supra* note 151, at 669–71 (explaining possible issues of implied consent by owners of household robots).

156. *See* Liz Sly et al., *U.S. Military Reviewing its Rules After Fitness Trackers Exposed Sensitive Data*, WASH. POST (Jan. 29, 2018), https://www.washingtonpost.com/world/the-us-military-reviews-its-rules-as-new-details-of-us-soldiers-and-bases-emerge/2018/01/29/6310d518-050f-11e8-aa61-f3391373867e_story.html (describing how a map posted online by a fitness tracking app allowed users to "identify individual users of the tracking service by name," including military personnel, "along with the jogging routes they use in war zones such as Iraq and Afghanistan," as well as the dates and times of each run); Ry Crist, *Here's What's Next for Samsung's Family Hub Smart Fridge*, CNET.COM (Jan. 7, 2018), https://www.cnet.com/news/heres-whats-next-for-samsung-family-hub-smart-fridge-ces-2018/ (listing features of Samsung's latest "smart fridge," including monitoring feeds from connected cameras, a "grocery-tracking fridge camera[]," and voice controls).

157. *See infra* Section III (describing various state court interpretation of wiretap statutes).

158. *See* Kerr, *supra* note 122, at 871–73 ("Judicial rulemaking is limited by strong stare decisis norms that limit the ability of judicial rules to change quickly; in contrast, legislatures enjoy wide-ranging discretion to enact new rules. The difference favors legislatures when technology is in flux because the privacy implications of particular rules can fluctuate as technology advances.").

Vermont's current approach to wiretapping does not sufficiently protect private citizens.[159] Vermont must act now to protect its citizens by codifying a statute that is able to adapt to rapidly changing technology.

III. STATE APPROACHES TO WIRETAPPING

When a new form of communications technology emerges, courts often struggle to define it by the terms used in the statute. Is the new technology an oral, wire, or electronic communication?[160] Can it be used as an *interception device*?[161] When the new technology is a modification of existing technology and used in a similar way, such as a call placed from a cell phone, rather than a landline, it may be relatively easy to define.[162] However, when the new technology is a departure from previous technology, such as using a cell phone to send text messages, it is not as simple to equate with existing technology, or with existing statutory terminology.[163]

Generally, states have adopted one of three approaches to wiretapping, with varying degrees of success: some state constitutions include an explicit right to privacy;[164] some states have modeled their wiretap laws on the federal statute;[165] and others have developed their own wiretap statutes not based on the federal statute.[166] This Note examines each model to determine how Vermont should proceed in addressing wiretapping.

---

159. *See supra* notes 4–5 and accompanying text (stating that Vermont is the only state that does not have a wiretap statute to protect citizens from interception of private communications).

160. *See, e.g.*, *In re* Contents of Stored Commc'ns From Twitter, 154 A.3d 169, 175 (N.J. Super. Ct. App. Div. 2017) (holding that the audio portion of a video posted to Twitter was an "oral communication" under New Jersey's wiretap statute).

161. *See, e.g.*, Commonwealth v. Diego, 119 A.3d 370, 375 (Pa. 2015) (finding that an iPad is not a telephone under Pennsylvania's wiretap statute).

162. *See, e.g.*, Davis v. State, 21 A.3d 181, 194 (Md. Ct. Spec. App. 2011) (stating that the "listening post" theory—which holds that an interception occurs at the place the intercepted communications are first heard—applies equally to landline and cellular phone calls).

163. *Compare* Commonwealth v. Cruttenden, 976 A.2d 1176, 1181 (Pa. Super. Ct. 2009) (holding that an officer posing as an accomplice who received text messages from a suspect had "intercepted" the text messages), *with* Commonwealth v. Cruttenden, 58 A.3d 95, 96 (Pa. 2012) (reversing the Superior Court's holding because an officer who directly receives text messages is "engaging in the communication," not intercepting the communication, even though the sender believed the police officer was someone else).

164. Bast, *supra* note 4.

165. *Id.* at app. B (showing that 13 state statutes contain wording similar to the federal act, and 16 statutes are partially or loosely similar to the federal act).

166. *Id.* (indicating that the statutes of Alabama, Arkansas, California, Connecticut, Georgia, Kansas, Kentucky, Maine, Michigan, Montana, Nevada, North Carolina, South Carolina, South Dakota, Tennessee, Texas, and Washington are not similar to the federal act).

A. Constitutional Privacy Provisions: Florida and New York

Although the U.S. Constitution does not contain an explicit right to privacy, courts have derived that right from other provisions.[167] Unlike the U.S. Constitution, eleven state constitutions include an explicit right to privacy.[168] Courts in those states thus often require strict construction of wiretap statutes to comply with the state constitution.[169] The Constitutions of New York and Florida directly prohibit interception of certain communications.[170]

Comparing cases from New York and Florida shows the challenges and successes that arise from a constitutional prohibition on intercepting communications. Both constitutions prohibit the "unreasonable interception" of communications.[171] New York's Constitution applies only to "telephone and telegraph communications."[172] The language of Florida's Constitution is considerably broader, prohibiting the interception of "private communications by any means."[173]

Even though both state constitutions contain a provision on intercepting communications, the subsequent statutes passed in each state have differentiated each state's approach. Not only is the statutory language used in each state different, so is the manner in which the courts interpret those statutes within the constraints of their respective constitutions.[174] Because both states' constitutions prohibit the interception of

---

167. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (holding that the "specific guarantees in the Bill of Rights have penumbras" that "create zones of privacy").

168. ALASKA CONST. art. I, § 22; ARIZ. CONST. art. 2, § 8; CAL. CONST. art. 1, § 1; FLA. CONST. art. I, § 23; HAW. CONST. art. I, §§ 6–7; ILL. CONST. art. 1, §§ 6, 12; LA. CONST. art. 1, § 5; MONT. CONST. art. II, § 10; S.C. CONST. art. I, § 10; WASH. CONST. art. 1, § 7.

169. *See, e.g.*, State v. Ault, 724 P.2d 545, 549 (Ariz. 1986) (stating that the "Arizona Constitution is even more explicit than its federal counterpart in safeguarding the fundamental liberty of Arizona citizens," and therefore the court would not allow for an exception to the statutory requirement that officers must have a warrant to enter a home).

170. N.Y. CONST. art. 1, § 12 ("The right of the people to be secure against unreasonable interception of telephone and telegraph communications shall not be violated . . . ."); FLA. CONST. art. I, § 12 ("The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, and against the unreasonable interception of private communications by any means, shall not be violated."). The Florida Constitution also separately recognizes the right to privacy. *Id.* art. I, § 23.

171. N.Y. CONST. art. 1, § 12; FLA. CONST. art. I, § 12.

172. N.Y. CONST. art. 1, § 12.

173. FLA. CONST. art. I, § 12.

174. *Compare* People v. Perez, 848 N.Y.S.2d 525, 531–32 (Sup. Ct. 2007) (discussing how New York courts have interpreted state wiretap statutes in relation to the state constitution), *with* Mozo v. State, 632 So. 2d 623, 630–31 (Fla. Dist. Ct. App. 1994), *aff'd*, 655 So. 2d 1115 (Fla. 1995) (analyzing the interception of cordless communications under state statute, and both the Florida and U.S. Constitutions).

communications, both states necessarily enacted wiretap statutes that outline when interception *is* acceptable.[175]

Florida courts view wiretap statutes as limited exceptions to the broad constitutional ban on interceptions.[176] Thus, the courts have taken a very narrow, textualist approach to interpreting wiretap statutes. The Florida Supreme Court articulated the necessity for this strict interpretation of wiretap laws as follows: "[T]he protection of privacy in the area of communications is constitutionally mandated in express language. This Court is not at liberty to relax this protection afforded by the State Constitution."[177] Because the language of Florida's constitutional provision is very broad, it applies to a wide range of eavesdropping, wiretapping, and other surreptitious recording activities.[178] However, this broad application also necessarily requires that exceptions be very clear and explicit since courts are "not at liberty to relax this protection."[179]

Conversely, the language of the New York Constitution is much more specific, and only applies to wiretapping phones.[180] The limited scope of the constitutional provision does not protect New Yorkers against an ever-growing number of other technologies.[181] Many of New York's wiretap statutes are not merely exceptions to the limited prohibition enshrined in the state constitution.[182] Therefore, the courts do not employ the same strict textualist approach when interpreting wiretap laws that do not infringe on the constitutional protection against intercepting telephone communications.[183]

---

175. *See, e.g.*, N.Y. PENAL LAW § 250.65 (McKinney 2017) (permitting wiretapping under specific circumstances); FLA. STAT. §§ 934.07–08 (2017) (authorizing wiretapping and the use of intercepted communications under certain conditions).

176. *See, e.g.*, Jackson v. State, 636 So. 2d 1372, 1374 (Fla. Dist. Ct. App. 1994) ("[Wiretap] statutes are exceptions to the federal and state constitutional rights to privacy and must be strictly construed.") (internal citation omitted).

177. Tollett v. State, 272 So. 2d 490, 493 (Fla. 1973).

178. *See, e.g.*, *Jackson*, 636 So. 2d at 1376 (holding that "information transmitted to a display pager is an electronic communication," and in order to lawfully intercept that information, "the state must strictly comply with the requirements" laid out in the state law authorizing the interception of electronic communications by law enforcement); Holt v. Chief Judge of Thirteenth Judicial Circuit, 920 So. 2d 814, 818 n.4 (Fla. Dist. Ct. App. 2006) (discussing the court's concern that an electronic court reporting system could unintentionally violate the Florida Constitution).

179. *Tollett*, 272 So. 2d at 493.

180. N.Y. CONST. art. 1, § 12.

181. *See, e.g.*, People v. Di Raffaele, 433 N.E.2d 513, 516 (N.Y. 1982) (rejecting defendant's argument that telephone toll-billing records were subject to a "more restrictive standard" under the New York Constitution).

182. *See* People v. Perez, 848 N.Y.S.2d 525, 531–32 (Sup. Ct. 2007) (listing cases in which New York courts have strictly interpreted the state statute authorizing wiretaps otherwise prohibited by the Constitution, and other cases in which the courts have not employed a strict interpretation).

183. *Id.*

i. *McDade v. State* and *People v. K.B.*

The first pair of cases this Note discusses illustrates how the differences between two constitutional provisions can lead to drastically different results. These cases are factually very similar, but the results of each case are in almost direct opposition to one another. For context, it is necessary to note that Florida law requires two-party consent, whereas New York requires only single-party consent.[184]

In *McDade v. State*, a minor in Florida used an MP3 player to secretly record a conversation with her stepfather, in which he admitted to sexually abusing her.[185] The minor turned the recordings over to police who arrested the stepfather, McDade.[186] The court sentenced McDade to two terms of life imprisonment for sexual battery on a child.[187] McDade appealed, claiming that the recordings were inadmissible as evidence because his stepdaughter recorded him without his consent, thus violating Florida's two-party consent requirement.[188] The Florida Supreme Court agreed with McDade, and ruled that the recordings were inadmissible.[189] The court applied a strict, narrow reading of the state statute, finding that the law did not make any exceptions for a circumstance where one party was committing a crime.[190] The court recognized that there might be a "compelling case" to allow for an exception to the two-party consent rule under circumstances such as those in *McDade*, but stated that "the adoption of such an exception is a matter for the Legislature."[191]

In New York, a near-identical case yielded a different result.[192] In *People v. K.B.*, a minor gave police a tape recording she made in which her father admitted to raping her.[193] The father filed a motion to exclude the recording, claiming that even though the statute required only single-party consent, the daughter could not legally consent to the recording she had made because she was a minor.[194] The court concluded that the daughter

184. FLA. STAT. § 934.03(d) (2017); N.Y. PENAL LAW § 250.00(2) (McKinney 2017). *See supra* notes 87–91 and accompanying text (describing single-party and two-party consent laws).

185. McDade v. State, 154 So. 3d 292, 295 (Fla. 2014).

186. *Id.* at 294.

187. *Id.* at 295.

188. *Id.*

189. *Id.* at 298.

190. *Id.* at 299.

191. *Id.*

192. People v. K.B., 984 N.Y.S.2d 547, 550 (Sup. Ct. 2014).

193. *Id.* at 548.

194. *Id.* at 549.

could give consent, and denied the father's motion to exclude the recordings.[195]

Unlike the Florida court, the New York court looked outside the bounds of the statute's plain language to reach its conclusion.[196] The court stated that one "policy consideration" of prohibiting minors from consenting to an interception under New York's single-consent law was to "prevent the police from coercing minors into acting as police agents against their parents or other family members."[197] The victim in *K.B.* had made the recording on her own, prior to any police involvement in her case, so that policy consideration was irrelevant.[198] The law was "enacted for the benefit of minors" and therefore "should not be interpreted as to deprive a minor who is an alleged crime victim of what could obviously be powerful evidence against the perpetrator."[199]

The court's reasoning also referred to technological changes, stating that, "courts cannot ignore the fact that the prevalence of technology has provided minors even younger than 14, with access to cell phones, smart phone apps, and other recording devices."[200] Therefore, while courts should review circumstances involving minors on a case-by-case basis, there was "no rational basis to reject a recording such as this because one party to the conversation is a minor."[201]

These cases demonstrate how the differences between the two state constitutions can lead to very different results. Florida's broad constitutional provision protects against all interceptions.[202] Florida wiretap laws therefore carve out narrow exceptions to this broad protection.[203] The courts cannot expand those exceptions beyond the plain language of the

---

195. *Id.* at 550.

196. *Id.* at 549–50.

197. *Id.* at 549. Curiously, the statute does not make any specific reference to minors, prohibiting only "intentional overhearing or recording of a conversation or discussion, without the consent of at least one party thereto." N.Y. PENAL LAW §§ 250.00, 250.05 (McKinney 2017).

198. *People v. K.B.*, 984 N.Y.S.2d at 549.

199. *Id.* at 550.

200. *Id.*

201. *Id.* In a separate case where a non-custodial parent recorded the other parent abusing their child over an open phone line, the Court of Appeals found that the parent could consent "on behalf of his child" because he had a good-faith basis to believe that it was necessary to vicariously consent for his child. People v. Badalamenti, 27 N.Y.3d 423, 432 (2016). Interestingly, the court also concluded that the parent's actions were not "wiretapping" under the state constitution because he was a "sender or receiver" of the telephonic communication, but his actions did constitute the crime of "mechanical overhearing of a conversation," which under New York law was considered "bugging." *Id.* at 431–32.

202. *See* FLA. CONST. art. I, § 12 (providing that all people shall be protected "against the unreasonable interception of private communications by any means").

203. FLA. STAT. ANN. § 934.03 (West 2018).

statutes.[204] In *McDade*, the court recognized that there was a "compelling case" to recognize an exception to the constitutional prohibition.[205] However, the court could not expand statutory exceptions beyond those clearly stated in the statute without infringing upon McDade's constitutional rights.[206] Conversely, the New York court was able to expand the statute beyond its plain language.[207] This case shows how in a very similar scenario, the New York Constitution can provide no protection, whereas the Florida Constitution does. While this led to a more just result in *K.B.* than in *McDade*, under different circumstances Florida's constitution may lead to a better result than would New York's.

ii. *State v. McCormick* and *People v. Darling*

The next pair of cases provide examples of how the state constitutions can be applied to new technology. In these cases, the two states came to relatively similar conclusions. Both cases concerned the particularity with which a warrant authorized a wiretap.

In *State v. McCormick*, Florida prosecutors appealed a trial court's ruling that a warrant to wiretap a cell phone was overbroad because it did not list the defendant's address.[208] The court reversed the trial court's decision, finding that because the warrant listed the unique phone number, it contained sufficient detail to "lead a reasonable person to the proper subject of the wire interception."[209] The court further acknowledged that the case "involve[d] new and evolving areas of both law and technology," and that the court's conclusion was "a logical solution to the problems created by the mobility of cellular telephones and the difficulty in locating them."[210]

In *People v. Darling*, a New York case, the defendants appealed a lower court's ruling that a warrant was sufficient even though the defendants had changed phone numbers.[211] The warrant listed the correct address, and the house had only one phone line.[212] The defendants pointed to the "[c]ourt's strict compliance jurisprudence," in which the court had

204. McDade v. State, 154 So. 3d 292, 297 (Fla. 2014).

205. *Id.* at 299.

206. *Id.*

207. *See* People v. K.B., 984 N.Y.S.2d 547, 550 (Sup. Ct. 2014) (providing evidence of the court's expansion of § 710.30(1)(a) beyond the plain language of the statute).

208. State v. McCormick, 719 So. 2d 1220, 1221 (Fla. Dist. Ct. App. 1998).

209. *Id.* (quoting State v. Buffa, 347 So. 2d 688, 688 (Fla. Dist. Ct. App. 1977)).

210. *Id.* at 1223.

211. People v. Darling, 742 N.E.2d 596, 598–99 (N.Y. 2000).

212. *Id.* at 599, 601.

suppressed evidence "when the authorities failed to comply strictly with constitutional and statutory requirements."[213] The court rejected the defendant's argument, stating that "[s]trict compliance does not entail hypertechnical or strained obedience, nor is common sense its enemy."[214] The court concluded that the warrant was adequate: "No confusion was created merely because the number changed. There was no possibility for misdirection . . . . In the context of this case, the change in telephone number had no bearing on the established probable cause."[215]

As these cases demonstrate, a constitutional provision can be applied to new technology or unanticipated scenarios, though the specific language used may limit its scope and effectiveness. A broad constitutional provision such as Florida's provides greater protection, but also necessarily requires very clear, specific language in any subsequent statutes.[216] Additionally, it does not allow for judicial discretion to interpret statutes in light of technological changes or other important considerations.[217] Alternatively, New York's narrow constitutional provision provides no protection over any non-telephonic recording.[218] This allows for greater flexibility based on changing technological norms.[219] However, the narrow language may also render the constitutional protection essentially obsolete because of those same changing norms.

B. State Statutes Developed Using the Federal Wiretap Statute as a Framework: Maryland and Massachusetts

Unlike states with their own explicit constitutional provisions like Florida and New York, other states have used the ECPA as a guiding document when drafting their own statutes, or have adopted the language of Title III or the ECPA either in full or in part.[220] To assess the effectiveness of this approach, this Note examines two states that have borrowed from

---

213. *Id.* at 599–600.

214. *Id.* at 601 (internal quotations omitted).

215. *Id.*

216. *See supra* notes 205–07 and accompanying text (discussing the broad protections and narrow exceptions provided by Florida's Constitution).

217. *See supra* notes 208–09 and accompanying text (examining the judicial constraints of Florida's Constitution).

218. *See supra* notes 181–84 and accompanying text (describing the limited language of New York's constitutional provision).

219. *See supra* note 182 and accompanying text (explaining that the court in New York does not have to apply a strict textualist approach).

220. *See* Bast, *supra* note 4, at app. B (indicating which state laws contain wording similar to the ECPA).

federal law: Maryland and Massachusetts. Maryland uses the ECPA as guidance, and Massachusetts has partially adopted the language of Title III.

The following cases demonstrate the successes and challenges of each approach. Maryland modeled its wiretap law on the ECPA, but the state statute contains some departures from the federal law, such as requiring two-party consent.[221] Maryland's approach allows courts to use the ECPA and related cases as compelling persuasive authority. Alternatively, Massachusetts partially adopted the language of Title III, but not the ECPA's amended language.[222] This approach has created significant, unnecessary confusion in Massachusetts courts.

i. *Davis v. State*

The Maryland case *Davis v. State* demonstrates how Maryland's approach to wiretapping provides guidance to its courts. In *Davis*, the question presented was whether evidence obtained from an authorized wiretap of a cell phone was admissible under § 10-408(c) of Maryland's wiretap statute, even when the defendant traveled across state lines.[223] The court looked to federal court opinions interpreting similar cases under the ECPA, because "Maryland's wiretap statutory scheme is an 'offspring'" of the Act.[224] Therefore, federal court opinions interpreting the ECPA were a source of persuasive guidance.[225] Similarly, the court also looked to state court opinions from other states with wiretap laws modeled on the ECPA to see how those courts had interpreted their own related statutes.[226]

The state's legislative history also supported the court's decision to look to the federal courts because it indicated that the legislature intended for the ECPA to "serve[] as the guiding light for the Maryland Act."[227] The legislative history also showed the intended scope and reach of Maryland's statute.[228] The court's analysis showed that § 10-408(c) was enacted specifically "to account for the development of cellular phone technology."[229] After looking at several revisions to the statute's language over time, the court recognized that "[a]lthough none of the legislative

221. MD. CODE ANN., CTS. & JUD. PROC. § 10-402 (West 2009). *See supra* notes 87–91 (defining two-party consent).

222. *See* Bast, *supra* note 4, at app. B (noting Massachusetts's partial adoption of the pre-amendment language of Title III).

223. Davis v. State, 43 A.3d 1044, 1047–48 (Md. 2012).

224. *Id.* at 1051.

225. *Id.*

226. *Id.* at 1052–53.

227. *Id.* at 1051.

228. *Id.* at 1050.

229. *Id.*

history speaks directly to the interception of communications emanating from an out-of-state source, it is clear that the statute has been evolving steadily, trying to keep pace with emerging technology."[230]

ii. *Schmerling v. Injured Workers' Insurance Fund*

Another Maryland case illustrates how Maryland's approach can be particularly useful to courts when analyzing new technology. *Schmerling v. Injured Workers' Insurance Fund* presented the Maryland Court of Appeals with a case of first impression concerning a telephone monitoring system that recorded phone calls at a company call center.[231] Although it was a case of first impression in Maryland, other jurisdictions had previously examined similar monitoring systems.[232] Therefore, the court reasoned that it should look to "case law from jurisdictions which have considered the permissibility of using similar equipment pursuant to *similarly enacted wiretapping laws* [that] may help guide [the court's] ultimate conclusion."[233]

In addition to case law from other jurisdictions with similar wiretap statutes, the court also considered Maryland's "heightened interest in the privacy of its citizens" in reaching its "ultimate conclusion."[234] According to the court, although Maryland modeled their statute on federal law, "[t]he alterations that were made . . . before enacting the Maryland Act were obviously designed to afford the people of [Maryland] a greater protection than Congress provided in Title III."[235] Therefore, the court must reach a conclusion that protects "the privacy sought by the Legislature."[236]

Because Maryland's wiretap statute is similar, but not identical, to the ECPA, and because Maryland's legislature has proactively modified their statute over time to keep pace with technology, the legislature has provided courts with extensive, yet flexible, guidance on statutory interpretation.[237] When the Maryland statute contains similar or identical language to the federal statute, then the Maryland courts may look to the federal courts and other jurisdictions with similar statutes when presented with a novel

230. *Id.* at 1051.

231. Schmerling v. Injured Workers' Ins. Fund, 795 A.2d 715, 716 (Md. 2002).

232. *Id.* at 725.

233. *Id.* (emphasis added).

234. *Id.*

235. *Id.* at 722 (first alteration in original) (quoting Standiford v. Standiford, 598 A.2d 495, 499 (Md. Ct. Spec. App. 1992)).

236. *Id.* at 725.

237. *Id.*; *see also* MD. CODE ANN., CTS. & JUD. PROC. §§ 10-401 to 10-414 (West 2009) (providing extensive definitions of terms).

issue.[238] If the language in Maryland's statute differs from the ECPA, then the courts can assume that the legislature intended to provide more stringent protections than the federal statute.[239] By looking at changes to the statutory language over time, the courts can assess the legislature's intent to address new technological advancements.[240]

In contrast to Maryland's statutes, which the state drafted using the ECPA as a "guiding light,"[241] Massachusetts adopted large swaths of Title III almost verbatim in 1968.[242] However, after Congress passed the ECPA in 1986,[243] the Massachusetts legislature did not similarly amend the state statute.[244] On multiple occasions, litigants have challenged the applicability of the state statute to anything beyond wire and oral communication, which is the language used in the statute.[245] Despite the absence of any amendments to the Massachusetts statute, the state courts have expanded the scope of the law beyond only wire and oral communication.[246] However, justifying and supporting the courts' interpretations of the statute requires significant time and research that could have been avoided by simply amending the statute after Congress passed the ECPA.[247]

iii. *Commonwealth v. Moody*

Massachusetts courts have relied upon federal legislative history to ascertain the scope of the state wiretap law. In *Commonwealth v. Moody*,

238. *See, e.g.*, Davis v. State, 43 A.3d 1044, 1051 (Md. 2012) (explaining that Maryland is seeking guidance from federal opinions for the current case because of the similarities between the Maryland and federal statutes).

239. *See, e.g.*, *Schmerling*, 795 A.2d at 722 (noting that the Maryland act clearly intended to extend more protections than the federal scheme).

240. *See, e.g.*, *id.* at 723 (stating that the reasoning and "discussion surrounding" amendments made to the language of Maryland's statute "provide great insight into the purpose and scope" of the law).

241. *Davis*, 43 A.3d at 1051.

242. Bast, *supra* note 4, at app. B. Despite adopting the federal act in large part, the Massachusetts wiretap statute does contain some differences. *See* Commonwealth v. Vitello, 327 N.E.2d 819, 836 (Mass. 1975) ("[W]e note that the Massachusetts statute in major portion matches section for section the provisions of Title III. Admittedly, the phraseology of our State statute is not word for word that of the Federal act.").

243. *See supra* notes 65–66 and accompanying text (describing the ways in which the ECPA updated the statutory language of Title III).

244. Commonwealth v. Moody, 993 N.E.2d 715, 720 (Mass. 2013).

245. *Id. See also* Dillon v. Mass. Bay Transp. Auth., 729 N.E.2d 329, 332–33 (Mass. App. Ct. 2000) (rejecting plaintiff's argument in favor of a strict literal reading of the statute because "an insistence on words over sense would be preposterous"); Commonwealth v. Alleyne, No. ESCR2006-1982, 2007 WL 4997621, *2 (Mass. Super. Ct. Nov. 1, 2007).

246. *Moody*, 993 N.E.2d at 720.

247. *See, e.g.*, *id.* at 722 (determining the scope of Massachusetts's law by examining federal legislative history of the ECPA).

the defendants appealed their drug trafficking convictions, arguing that the trial court should have suppressed the state-issued warrants to intercept their cell phone calls and text messages.[248] Because the legislature did not amend the state law after the passage of the ECPA, the defendants claimed that cell phones and text messages were beyond the scope of the state law, which referred only to wire and oral communication.[249] Therefore, the defendants argued, the judge did not have the authority under state law to issue a warrant to intercept cell phone and text message communications because they were not wire or oral communications.[250]

In analyzing whether the state statute covered cell phones and text messages, the court looked to the legislative history of the ECPA.[251] The legislative history indicated that Title III had covered a call from a cell phone to a landline because the call partially traveled over a standard telephone line, and was thus a "wire communication."[252] The court reasoned that "[w]hat was left in some doubt by [Title III] was whether a call from one cellular telephone to another, which traveled entirely by radio signals, except for its passage through a switching station, was protected."[253] The Congressional record noted that the ECPA *clarified* that cell-to-cell calls were, in fact, "wire communications" under Title III, not that the ECPA "mark[ed] the *beginning* of Title III's coverage of cellular telephone calls."[254] Even though the Massachusetts legislature did not amend its statute after the passage of the ECPA, the court still ruled that the statute covered cell-to-cell calls, because the ECPA merely clarified that Title III already covered those calls.[255]

The question of whether the statute covered text messages was more complicated.[256] The ECPA narrowed the definition of "wire communication" from "any communication" to "any aural transfer."[257] It also moved non-oral communications to the newly created category of "electronic communication."[258] Unlike cell phone communications, which the ECPA merely clarified, the amended language intentionally excluded

---

248. *Id.* at 716.
249. *Id.* at 717.
250. *Id.*
251. *Id.* at 722–23.
252. *Id.* at 722.
253. *Id.*
254. *Id.* at 723 (emphasis added).
255. *See id.* (holding that the retention of the 1968 language "does not mean that the Massachusetts statute is less protective than Title III—it only means that on its face the Massachusetts wiretap statute is less clear than its Federal counterpart").
256. *Id.* at 723–24.
257. *Id.* at 720.
258. *Id.* at 723.

non-oral communications from the new definition of "wire communications."[259]

Once again, the court found the federal legislative history instructive.[260] Congress anticipated that the revisions to the Federal Act *may* make it necessary for states to revise their statutes, but indicated that this might not be *required* in all circumstances.[261] The ECPA gave states a two-year grace period to amend their statutes to comply with the changes to the federal statute.[262] Thus, because the Massachusetts statute did not narrow the scope of "wire communications" as the ECPA had, text messages could still be included under the state's definition of that term.[263]

Even though the Massachusetts statute largely paralleled the language of Title III, one important difference between the statutes remained: the definition of "intercept."[264] The state statute's definition of "intercept" was broader than the definition under Title III.[265] The ECPA broadened the federal statute's definition of intercept.[266] The court concluded that the Massachusetts statute did not require any amendments to provide the same protections to text messages as the ECPA because its definition was already broader than Title III's.[267]

iv. *Commonwealth v. Hyde*

Despite the Massachusetts legislature's failure to update the state statute, it nevertheless provides the courts with guidance in interpreting the law through a preamble outlining the legislature's purpose and intent of

---

259. *Id.*

260. *Id.*

261. *Id.* ("[T]he defendants' argument runs head long into the legislative history of the ECPA, which explicitly recognized the possibility that 'state laws [might] not need [to] be changed to accommodate revisions on interceptions of wire or oral communications.'" (second and third alterations in original) (quoting H.R. Rep. No. 99-647, at 62 (1986))).

262. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 111(b)(2), 100 Stat. 1848, 1859.

263. *Moody*, 993 N.E.2d at 724. ("Given that a text message is a communication transmitted over a cellular network that travels in part by wire or cable or other like connection within a switching station, it seems self-evident that text messages fall within the plain language of the definition of 'wire communication' in § 99.").

264. *Id.*

265. *Id.*

266. *Id.*

267. *Id.* ("In light of the broad statutory definitions of the terms 'wire communication' and 'interception,' we conclude that the Massachusetts wiretap statute provides protection for the electronic transmission of text messages consistent with the protections currently provided by Title III . . . .").

enacting the wiretap law.[268] The preamble addresses the risks that evolving technology pose to the privacy of Massachusetts citizens:

> The general court further finds that the uncontrolled development and unrestricted use of modern electronic surveillance devices *pose grave dangers to the privacy of all citizens of the commonwealth*. Therefore, the secret use of such devices by private individuals must be prohibited. The use of such devices by law enforcement officials must be conducted under strict judicial supervision and should be limited to the investigation of organized crime.[269]

The following case demonstrates how the preamble acts as a broad prohibition on wiretapping. In *Commonwealth v. Hyde*, during a traffic stop, the defendant used a handheld tape recorder to secretly record the arresting officer, which led to the defendant's conviction for wiretapping.[270] The defendant argued that he had not violated the wiretap statute, because the police officer had no reasonable expectation of privacy during a traffic stop.[271] The court held that "[t]he statute's preamble expresses the Legislature's general concern that" technology "'pose[d] grave dangers to the privacy of all citizens of the commonwealth' and this concern was relied on to justify the ban on the public's clandestine use of such devices."[272] Whereas many jurisdictions have adopted the "reasonable expectation of privacy" standard from *Katz*, the Massachusetts court found that the preamble showed clear legislative intent to prohibit *all* "clandestine" use of recording devices.[273] The lack of any exception to that rule led the court to conclude that the Massachusetts statute applied at all times, not only when the parties to a communication had a reasonable expectation of privacy.[274]

---

268. MASS. GEN. LAWS ch. 272, § 99(A) (2017). *See also* O'Sullivan v. Nynex Corp, No. 95-6600-D., 1996 WL 560274, *9 (Mass. Super. Ct. Sept. 26, 1996) (noting that § 99 "commences with a long preamble setting out the legislature's purposes in enacting the statute").

269. § 99(A). Massachusetts is a two-party consent state. *Id.* § 99(B)(4).

270. Commonwealth v. Hyde, 750 N.E.2d 963, 965 (Mass. 2001).

271. *Id.*

272. *Id.* at 967 (second alteration in original) (quoting MASS. GEN. LAWS ch. 272, § 99(A) (2017)).

273. *Id. See also* Katz v. United States, 389 U.S. 347, 353 (1967) (holding that the Fourth Amendment protects individuals in any situation where they have a reasonable expectation of privacy).

274. *Hyde*, 750 N.E.2d at 966. *See also* Commonwealth v. Jackson, 349 N.E.2d 337, 340 (Mass. 1976) (rejecting an argument that the wiretap statute did not apply to a kidnapper when calling the victim's family demanding ransom, because it "would render meaningless the Legislature's careful choice of words if [the court] were to interpret 'secretly' as encompassing only those situations where an individual has a reasonable expectation of privacy").

v. *Dillon v. Massachusetts Bay Transportation Authority*

In contrast, the court was willing to depart from a strict, literal reading of the statute in a case concerning the application of the telephone equipment exception to the definition of "intercepting device[s]."[275] The Massachusetts Bay Transportation Authority (MBTA), which is responsible for public transportation operations in and around Boston, recorded almost all telephone communications at its major operational centers.[276] The MBTA used one of those recordings in a disciplinary proceeding against an MBTA employee who made profane and insulting comments while on a business call.[277] The employee filed suit against the MBTA, claiming that it had violated the state wiretap statute by recording her without consent.[278]

In response, the MBTA claimed that the recordings were valid under the telephone equipment exception to the wiretap statute.[279] The exemption omits telephone equipment "furnished to a subscriber or user by a communications common carrier in the ordinary course of its business . . . and being used by the subscriber or user in the ordinary course of its business" from the definition of an "intercepting device."[280] The employee argued that the exception did not apply because the MBTA purchased the recorders from a commercial equipment manufacturer, not a "communications common carrier."[281] Opposing a strict, literal interpretation of the statute, the MBTA "urge[d] that in enacting the provision many years ago the Legislature could not have foreseen the sweeping changes in the telecommunications industry by which telephone equipment has become widely available from entities other than telephone companies."[282] Because of this unanticipated development, the MBTA argued that "an insistence on words over sense would be preposterous."[283]

The court agreed with the MBTA, holding that a literal reading of the statute would fail to "preserve [the statute] in its intrinsic intended scope."[284] The court "d[id] not depart lightly from the express wording of a

---

275. Dillon v. Mass. Bay Transp. Auth., 729 N.E.2d 329, 331(Mass. App. Ct. 2000).

276. *Id.* The MBTA's reasons for recording calls included "improving efficiency, ensuring public safety, and seeing to employee compliance with applicable law." *Id.*

277. *Id.* at 332.

278. *Id.*

279. *Id.*

280. MASS. GEN. LAWS ch. 272, § 99(B)(3) (2017).

281. *Dillon*, 729 N.E.2d at 331. *See also* MASS. GEN. LAWS ch. 272, § 99(B)(12) (2017) ("The term 'communications common carrier' means any person engaged as a common carrier in providing or operating wire communicating facilities.").

282. *Dillon*, 729 N.E.2d at 332–33.

283. *Id.* at 333.

284. *Id.* at 334.

statute," but indicated that the changed circumstances compelled such a departure.[285] A literal reading of the telephone equipment exception would cause absurd results, "allowing the fortuity of the source of the equipment to entail serious material consequences."[286]

The preamble thus acts as a broad prohibition on wiretapping, similar to Florida's constitutional provision.[287] However, the preamble is a statutory provision, not a constitutional one.[288] Thus, the Massachusetts courts have a greater degree of leniency when interpreting their statutes than the Florida courts do in interpreting their Constitution.[289] Massachusetts courts refuse to create exceptions not explicitly included in the preamble, but the preamble functions especially well as evidence of legislative intent.

As these cases demonstrate, both Maryland's and Massachusetts's approaches to wiretapping contain some distinct advantages.[290] Maryland has successfully utilized the ECPA to offer guidance to its courts, and to signal legislative intent.[291] The greatest success of Massachusetts's approach is the statute's preamble, which provides its courts with concise, straightforward guidance to interpret the statute.[292] Maryland has successfully used the ECPA to its benefit, while Massachusetts's method of partially adopting the federal law has resulted in needless confusion.[293] The adoption of Title III and the subsequent failure to update the state statute's language after the passage of the ECPA in 1986 complicates the application and interpretation of the statue.[294] The inconsistencies with the ECPA's language open the door to many challenges and require courts to perform

---

285. *Id.* at 333–34.

286. *Id.* at 334.

287. *See supra* Part III.A (describing how the language in Florida's constitutional provision broadly prohibits interceptions).

288. MASS. GEN. LAWS ch. 272, § 99 (2017).

289. *See* Bast, *supra* note 4, at app. B (indicating which state laws contain wording similar to the ECPA).

290. *See supra* note 237 and accompanying text (highlighting the benefits of Maryland's approach); *see supra* notes 264–67 and accompanying text (noting that Massachusetts's wiretap law provides more protections than Title III).

291. *See supra* notes 223–30 and accompanying text (explaining how the court in *Davis* used interpretations of the EPCA as a source of "persuasive guidance" and as a window into the legislature's intent).

292. *See supra* note 268 (discussing how preambles provide legislative intent and purpose).

293. *Compare supra* note 237–40 and accompanying text (summarizing how Maryland has benefitted from using the ECPA framework), *with supra* notes 242–47 (discussing the confusion that arose when Congress modified the EPCA and Massachusetts did not amend the state statute to reflect the new language).

294. *See supra* Part III.B.iii (analyzing the differences between the federal and state statutes and pointing out unresolved issues relating to the failure to update the statutory language).

intensive interpretative analyses in order to determine the scope of the statute.

Nevertheless, Massachusetts courts have liberally applied common sense to adapt the statute to new technologies and situations.[295] However, as this Note previously explained, relying on judicial rulemaking leads to rules that lag behind current technology and rules that do not take a wide range of perspectives and opinions into consideration.[296] Thus, despite the court's liberal application of the law to new technology, this approach cannot keep pace with technological evolution.

C. State Wiretap Statutes Not Based on Federal Statute: Nevada

Some states have drafted wiretap statutes that are not modeled on Title III or the ECPA.[297] The federal law still affects these state statutes because state law cannot allow what federal law prohibits.[298] Even when the state law differs from federal law, courts may only interpret the state law as equal to, or more restrictive than, federal law.[299] Nevada will serve to illustrate the strengths and weaknesses of this approach.

Nevada first passed a wiretap law in 1864, the same year it received statehood.[300] Over 100 years later, after Congress passed Title III, Nevada revised its statute in order to comply with federal law, but did not parallel Title III's language.[301] Challenges to the state wiretap statute usually involve claims that federal law preempts the less restrictive state law.[302]

---

295. *See supra* notes 283–86 and accompanying text (recounting the common-sense argument by the MBTA that persuaded the court to liberally interpret the statute).

296. *See supra* notes 134–37 and accompanying text (discussing the lag behind technology of judge-made laws, and the lack of perspectives considered in judicial rulemaking).

297. *See* Bast, *supra* note 4, at app. B (listing state statutes not based on federal statute).

298. *See* Arizona v. United States, 567 U.S. 387, 399 (2012) ("[S]tate laws are pre-empted when they conflict with federal law. This includes cases where 'compliance with both federal and state regulations is a physical impossibility,' and those instances where the challenged state law 'stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress . . . .'" (internal citations omitted) (quoting Fla. Lime & Avocado Growers, Inc. v. Paul, 373 U.S. 132, 141–43 (1963))).

299. S. REP. NO. 90-1097, at 98 (1968) ("The proposed provision envisions that States would be free to adopt more restrictive legislation, or no legislation at all, but not less restrictive legislation.").

300. *See* REVISED LAWS OF NEVADA, vol. I, at 1314 (1912) (indicating that the law was approved on Feb. 16, 1864). The original law prohibited "any person not connected with any telegraph company . . . by means of any machine, instrument, or contrivance, or in any other manner, [from] wilfully [sic] and fraudulently read[ing], or attempt[ing] to read any message or to learn the contents thereof whilst the same [was] being sent over any telegraph line." *Id.* at 1316.

301. *See* Lane v. Allstate Ins. Co., 969 P.2d 938, 940 (Nev. 1998) ("In 1973, the Nevada legislature made substantial amendments to NRS 200.620 through NRS 200.690, in order to bring Nevada law somewhat in conformity with federal wiretap statutes.").

302. *See supra* Part III.C.ii (discussing the court's reasoning in *Lane*).

Because the two laws do not complement each other in structure or language, it is more difficult to identify where the federal language and state language overlap.[303]

i. *Sharpe v. State*

Similar to *Commonwealth v. Moody*,[304] one such challenge concerned the applicability of the state statute to cell phone calls and text messages.[305] As in Massachusetts, even though Nevada revised the state statute to conform to Title III, it did not make any similar changes after the passage of the ECPA.[306] In *Sharpe v. State*, the defendant argued that the state statute did not apply to cell phone calls and text messages because the statute only referred to "wire communications."[307] The court concluded, as in *Moody*, that even though the ECPA changed the federal definition of "wire communication," under Nevada law, "wire communication" still applied to cell phone calls and text messages.[308]

Sharpe also argued that federal law preempted Nevada's wiretap law, because Nevada had not updated its language since the passage of the ECPA.[309] The court rejected this argument because Sharpe did not demonstrate how Nevada's failure to change the state statute made it less restrictive than the ECPA.[310] The court held that "current Nevada wiretap law, like federal wiretap law, allows for the interception of cellular telephone calls and text messages."[311] The Nevada statute and the ECPA did not mirror one another's language, but both laws fundamentally restricted the same conduct.[312]

ii. *Lane v. Allstate Insurance Co.*

Other cases reveal that Nevada courts also use the distinct language of the state statute to determine legislative intent. In one case, the court

---

303. *See supra* notes 320–23 (overviewing the *Lane* court's discussion of the differences between the federal and state statutes).

304. *See supra* notes 248–67 and accompanying text (discussing *Moody*).

305. Sharpe v. State, 350 P.3d 388, 389 (Nev. 2015).

306. *Id.* at 390–91.

307. *Id.* at 389.

308. *Id.* at 391–92.

309. *Id.*

310. *Id.* ("Sharpe, however, fails to point out how Nevada wiretap law is less restrictive, i.e., what Nevada wiretap law allowed to occur here that federal wiretap law would have prohibited.").

311. *Id.*

312. *Id.* ("Although the statutes read differently, their allowances in this regard are equally restrictive.").

dismissed a plaintiff's complaint against his employer, because the plaintiff, Lane, secretly recorded hundreds of phone calls with his employer in violation of Nevada's general two-party consent requirement.[313] Lane appealed the dismissal, arguing that the two-party consent requirement did not apply when an individual records his or her own phone calls.[314] The court found that the legislative intent disproved Lane's argument.[315] The Nevada statute contains separate provisions for telephone conversations and in-person conversations.[316] Section 650 permits single-party consent when using a listening device to intercept in-person conversations.[317] The court determined that the legislature's decision not to use that same language for telephone conversations under § 620 was intentional.[318] The court reasoned that "[i]t seem[ed] apparent that the legislature believed that intrusion upon Nevadans' privacy by nonconsensual recording of telephone conversations was a greater intrusion than the recording of conversations in person."[319]

The court also looked to the ECPA to determine the Nevada legislature's intent.[320] Under § 2511(2)(d), the federal statute explicitly authorizes the interception of communications "where such person is a party to the communication."[321] When "the Nevada legislature made substantial amendments . . . in order to bring Nevada law somewhat in conformity with federal wiretap statutes," it did not adopt that provision of § 2511(2)(d).[322] According to the court, "[i]t must be presumed that the exclusion of this provision in the Nevada statute was deliberate and was intended to provide a different result from that achieved under the federal wiretap statute."[323]

Finally, the court examined the legislative history of a failed amendment to § 620 that would have permitted one-party consent to phone

313. Lane v. Allstate Ins. Co., 969 P.2d 938, 939 (Nev. 1998).

314. *Id.*

315. *Id.* at 940.

316. *Id. Compare* NEV. REV. STAT. § 200.620 (2017) (indicating that it is illegal for "any person to intercept or attempt to intercept any wire communication unless: (a) The interception or attempted interception is made with the prior consent of one of the parties to the communication; *and* (b) An emergency situation exists and it is impractical to obtain a court order as required" (emphasis added)), *with* § 200.650 (prohibiting the interception of "any private conversation engaged in by the other persons . . . unless authorized to do so by one of the persons engaging in the conversation").

317. § 200.650.

318. *Lane*, 969 P.2d at 940 ("If the legislature had wanted to create that limitation in NRS 200.620, it would have done so.").

319. *Id.*

320. *Id.*

321. 18 U.S.C. § 2511(2)(d) (2012).

322. *Lane*, 969 P.2d at 940.

323. *Id.*

calls by law enforcement.[324] The legislature specifically discussed the difference between individuals recording their own conversations and interception by a third party.[325] "However, legislators continued to express concern over potential abuses when judicial oversight is lacking," and the bill failed to pass.[326] The court concluded that the bill's failure "sp[oke] eloquently of the legislative intent to prohibit the unauthorized interception of wire communications."[327]

iii. *Abid v. Abid*

In another case involving a custody dispute, a father hid a recording device in his child's backpack to record conversations between the child and the mother.[328] The district court concluded that the father had illegally recorded the conversations, because neither the child nor the mother had consented to the recording.[329] The recordings were thus inadmissible as evidence in the custody dispute, but the district court allowed a child psychologist, who testified as an expert witness, to evaluate the recordings.[330] The mother appealed, arguing that the district court should not have allowed the psychologist to review illegally obtained evidence.[331]

Once again, the court found the distinctions between the state and federal laws illustrative of the legislature's intent. Unlike the ECPA, Nevada's law is silent on the admissibility of an illegal wiretap in a civil action.[332] The court therefore refused to "read a broad suppression rule" into the state statute, because the legislature's silence demonstrated that it did not intend for such a rule to apply in civil cases.[333] Additionally, preventing the psychologist from reviewing the recordings did not contradict the purpose of the statute.[334] Section 650 states that "a person shall not intrude upon the privacy of other persons," indicating that its purpose is to protect an individual's privacy.[335] Therefore, because the psychologist was "already

---

324. *Id.*

325. *Id.* at 940–41.

326. *Id.* (citing *Intercepted Communications: Hearing on A.B. 188 Before the S. Judiciary Comm.*, 1985 Leg., 63rd Sess. (Nev. 1985) (statement of Sen. Thomas R.C. Wilson, Chairman, S. Judiciary Comm.)).

327. *Id.*

328. Abid v. Abid, 406 P.3d 476, 478 (Nev. 2017).

329. *Id.*

330. *Id.*

331. *Id.*

332. *Id.* at 479.

333. *Id.*

334. *Id.*

335. NEV. REV. STAT. § 200.650 (2017).

inquiring into private details of the relationship between parent and child," the recordings did not further intrude upon the privacy of the mother and the child.[336]

Lane and *Abid* demonstrate how courts may find the differences between Nevada's wiretap statute and the ECPA useful when interpreting the state's wiretap laws. Nevada courts can ascertain legislative intent when the language of the state law is more restrictive and the federal law establishes a baseline for the legal protection that the law must provide.[337] In contrast to Massachusetts's approach, the Nevada legislature is able to tailor laws to their exact specifications without following the structure of the federal law to avoid causing confusion.[338] Alternatively, Maryland's approach allows the legislature to use departures from the ECPA to indicate legislative intent that the state law provides greater protections than the corresponding federal law.[339]

Nevada's approach makes challenges to the state law in relation to the federal law more frequent than in a state with laws modeled on the ECPA, because it is easier to identify differences between them and argue that those distinctions lead to different results. Maryland's approach demonstrates the value of being able to draw parallels between the state law and the ECPA. Conversely, Massachusetts's approach shows the potential problems that could arise from adopting the federal model.

Overall, Nevada's approach is effective at protecting privacy and addressing new technology.[340] However, like Massachusetts, Nevada's approach allows for more challenges to the state law simply because the distinct language used can easily be interpreted as a substantive difference.[341] Unlike Maryland, where the legislature uses distinct language to signal a purposeful departure from the ECPA, Nevada's legislature may not intend for its distinct language to create substantively different protections from the ECPA.[342] Similarly, the Massachusetts legislature has

---

336. *Abid*, 406 P.3d at 479.

337. *See supra* notes 318–27 and accompanying text (describing the *Lane* court's approach to statutory interpretation).

338. *See supra* Part III.B.iii (discussing the confusion that resulted from Massachusetts's initial adoption of Title III and subsequent decision not to adopt the ECPA's amendments).

339. *See supra* notes 223–30 and accompanying text (describing the effectiveness of this approach).

340. *See supra* notes 304–36 and accompanying text (highlighting the effectiveness of Nevada's approach).

341. *See supra* notes 313–27 and accompanying text (noting that the court in *Lane* focused on the "distinct language" of the statute).

342. *Compare supra* notes 237–40 and accompanying text (summarizing Maryland's approach to statutory interpretation), *with supra* notes 301–03 and accompanying text (emphasizing that the Nevada legislature did not parallel the federal language when it updated its wiretap law).

created significant confusion by not adopting the ECPA's amendments to Title III.[343] However, its preamble offers clear evidence of legislative intent that the courts can use to determine if differences in language are intentional departures from federal law.[344] Nevada courts must instead search elsewhere, including failed amendments, to deduce legislative intent. Therefore, Nevada's approach is effective, but it has some shortcomings that make it less successful than other states.

IV. RECOMMENDATION FOR VERMONT

Based on other states' approaches, there are four recommendations that Vermont should follow. First, the statute should include a statement of legislative intent. Clear legislative intent guides courts in interpreting not only the literal language, but also the policy behind the law. Second, the statute must use broad language to define its scope and coverage. The combination of legislative intent and broad language will give courts greater flexibility to interpret the law in a manner consistent with its purpose, without being confined by the literal language. Third, the statute should generally follow the framework of the ECPA, thereby making any departure from its language a sign of a deliberate choice, rather than a legislative oversight. Finally, Vermont should pattern its statute on the federal law to provide a broader body of case law that courts can look to when faced with a novel issue.

A. Clear Statement of Legislative Intent

Vermont's statute must include a clear, straightforward statement of legislative intent. Massachusetts's preamble most effectively and concisely conveys legislative intent to its courts.[345] Florida's constitutional provision is too restrictive, and constitutional amendments are harder to both pass and change.[346] Maryland and Nevada courts have ascertained legislative intent from how their state statutes follow, or purposely do not follow, the ECPA.[347] However, Massachusetts's clear, straightforward preamble is part

343. *See supra* Part III.B.iii (recounting one example of an issue caused by the legislature's inaction).

344. *See supra* notes 268–74 and accompanying text (explaining how courts have used the preamble to Massachusetts's statute as evidence of legislative intent).

345. *See supra* notes 268–74 and accompanying text (illustrating how this preamble has been utilized by Massachusetts courts).

346. *See supra* Part III.A (examining the rigidity of Florida's constitutional provision).

347. *See supra* notes 223–30, 320–27, 332–38, and accompanying text (discussing approaches of the Maryland and Nevada courts for ascertaining intent).

of the state wiretap statute and therefore has greater authority over the courts than legislative intent gleaned from legislative history.[348]

Vermont has included provisions on the intent and purpose in other statutes. These provisions include policy guidelines,[349] statements of legislative intent,[350] and standards for construing and applying the law.[351] The legislature has also included statements on the intended relationship between a Vermont statute and federal law.[352] For example, Vermont's False Claims Act indicates the legislature's intent "that in construing this chapter, the courts of this State will be guided by the construction of similar terms contained in the Federal False Claims Act, 31 U.S.C. §§ 3729-3733, as from time to time amended by the U.S. Congress and the courts of the United States."[353] It is clear that the Vermont legislature is already familiar with, and comfortable including, statements of legislative intent or policy in statutes. Therefore, it could easily include a similar provision in a wiretap statute.

---

348. *See* Richard I. Nunez, *The Nature of Legislative Intent and the Use of Legislative Documents as Extrinsic Aids to Statutory Interpretation: A Reexamination*, 9 CAL. W. L. REV. 128, 130–31 (1972) (classifying preambles as more reliable evidence of legislative intent than "legislative evidence" such as floor hearings or committee reports); Daniel B. Listwa, *Uncovering the Codifier's Canon: How Codification Informs Interpretation*, 127 YALE L.J. 464, 472 (2017) ("[A]lthough not generating substantive law, [a preamble] gives the interpreter insight into how Congress expected the statute to apply . . . [and] the interpreter ought to accord it significant weight.").

349. *See, e.g.*, VT. STAT. ANN. tit. 6, § 2671 (2018) (declaring that it is the policy of the state to protect and promote Vermont dairy operations through supervision, inspection, and licensing); VT. STAT. ANN. tit. 9, § 2480aa (2017) ("It is the policy of this State that [structured settlement] agreements, which have often been approved by a court, should not be set aside lightly or without good reason.").

350. *See, e.g.*, VT. STAT. ANN. tit. 9, § 4170 (2018) ("The Legislature finds and declares that manufacturers, distributors, and importers of new motor vehicles should be obligated to provide speedy and less costly resolution of automobile warranty problems."); VT. STAT. ANN. tit. 18, § 4281 (2018) ("It is the intent of this chapter to create the Vermont Prescription Monitoring System . . . to promote the public health through enhanced opportunities for treatment for and prevention of abuse of controlled substances, without interfering with the legal medical use of those substances.").

351. *See, e.g.*, VT. STAT. ANN. tit. 16, § 2879e (2018) ("The purposes of this subchapter and all provisions of this subchapter with respect to powers granted shall be broadly interpreted to effectuate such intent and purposes and not as to any limitation of powers.").

352. VT. STAT. ANN. tit. 32, § 641(b) (2018). *See also* VT. STAT. ANN. tit. 9, § 4500(a) (2018) (indicating that it is the legislature's intent that Vermont's public accommodations law "be construed so as to be consistent with the Americans with Disabilities Act, 42 U.S.C. § 12101 et seq. and rules adopted thereunder, and [is] not intended to impose additional or higher standards, duties, or requirements than that act").

353. VT. STAT. ANN. tit. 32, § 641(b) (2018).

B. Broad Statutory Language

A statement of legislative intent will be most effective when paired with broad statutory language.[354] Vermont should adopt statutory language similar to Florida's constitutional provision: "The right of the people . . . against the unreasonable interception of private communications *by any means*, shall not be violated."[355] This language is effective because it does not reference any specific technology. For example, Nevada and Massachusetts both used a technical argument to expand the scope of "wire communications."[356] To cover cell phone calls, those states had to conclude that even if a small portion of the transmission happens over wire, it is still a "wire communication."[357] Using broad language prevents courts from having to grasp at straws in order to uphold the statute's purpose.[358] As Justice Brandeis stated in his dissent in *Olmstead*: "[A] principle to be vital must be capable of wider application than the mischief which gave it birth."[359]

C. Using the ECPA as a "Guiding Light" for Vermont's Statute

Vermont must walk a fine line between using the ECPA to its benefit, and becoming burdened by it. Massachusetts's approach has created some of the most complicated problems when comparing the state law to federal law.[360] That state's decision to parallel Title III, but not to amend it after the passage of the ECPA, creates confusion.[361] Even the Massachusetts courts have acknowledged that the legislature's decision makes Massachusetts's statute less clear than its federal counterpart.[362] Nevada's decision not to

---

354. *See supra* note 176 and accompanying text (explaining how the broad language of Florida's constitutional provision protects the privacy of Florida's citizens).

355. FLA. CONST. art. I, § 12 (emphasis added).

356. *See supra* notes 248–67, 304–12 and accompanying text (discussing the similarities between a Massachusetts case and a Nevada case interpreting "wire communication" as applied to cell phone calls).

357. *See supra* notes 247–67 and accompanying text (describing the technical analysis used Massachusetts to determine cell phone calls are "wire communications").

358. *See supra* Part III.B.iii (showing the complicated judicial analysis needed to broaden application of narrow statutory language).

359. Olmstead v. United States, 277 U.S. 438, 473 (Brandeis, J., dissenting) (quoting Weems v. United States, 217 U.S. 349, 373 (1910)).

360. *See supra* Part III.B.iii (explaining the problems created by the decision to adopt a federal statute but not amend it to continue to parallel the federal statute).

361. *See supra* Parts III.B.iii–iv (examining Massachusetts cases analyzing state wiretap laws).

362. *See* Commonwealth v. Moody, 993 N.E.2d 715, 723 (Mass. 2013) ("This does not mean that the Massachusetts statute is less protective than Title III—it only means that on its face the Massachusetts wiretap statute is less clear than its Federal counterpart.").

model its wiretap statute on the federal law at all also creates complications when comparing the two laws.[363]

Maryland has developed the most effective relationship between its own statute and the federal law. By patterning its statute on the ECPA, it clarifies where it departs from the federal law.[364] The relationship between the two laws is less ambiguous than between a statute that originally paralleled the federal law, but then later departed from it (as in Massachusetts), and a statute that contains no similarities whatsoever (as in Nevada). As technology evolves, so must wiretap laws. Maryland's statute has the flexibility to make changes that clearly and deliberately distinguish state law by departing from the federal language.

It is important that Vermont also be able to distinguish its laws from the ECPA without creating unnecessary confusion. Vermont has a history as a trailblazing state and a reputation for distinguishing itself from the rest of the country.[365] Vermont is sometimes years ahead of other states and the federal government in enacting laws.[366] For Vermont's wiretap law to reflect the state's progressive spirit, the language of the ECPA must not encumber Vermont's legislature or prevent it from making changes when necessary. However, that does not mean that Vermont should completely depart from the ECPA.

D. Using the ECPA as a Source of Persuasive Authority

Maryland's approach highlights the value of using the ECPA as guidance. This approach allows Maryland's courts to look to other jurisdictions when considering a novel application of its statute to new technology.[367] This is particularly important for a small state such as Vermont. If Vermont patterned its statute on federal law, the state would not have to rely only on its own relatively sparse jurisprudence.[368] It could look to other state and federal courts to see how those jurisdictions applied

---

363. *See supra* Parts III.C.i–iii (discussing Nevada cases interpreting state wiretap laws).

364. *See* Davis v. State, 43 A.3d 1044, 1051 (Md. 2012) (discussing the differences between the state and federal laws).

365. For example, in 2016, Vermont became the first state in the nation to require GMO food labeling. Stephanie Storm, *G.M.O.s in Food? Vermonters Will Know*, N.Y. TIMES (June 30, 2016), https://www.nytimes.com/2016/07/01/business/gmo-labels-vermont-law.html.

366. For instance, Vermont was the first state to pass a law granting full marital benefits to same-sex couples in 2000, three years before any other state, and 15 years before same-sex marriage was legal in all 50 states. Anthony Michael Kreis, *Stages of Constitutional Grief: Democratic Constitutionalism and Marriage Revolution*, 20 U. PA. J. CONST. L. 871, 884, 893 (2018).

367. *See supra* Part III.B.i (describing Maryland's process of examining other jurisdictions with similar laws).

368. *See supra* Part I.E (providing an overview of Vermont's common-law approach).

the same language to new technology. Vermont should follow Maryland's approach of using the federal law as guidance, while avoiding the pratfall that Massachusetts found itself in when it adopted Title III but not the ECPA.

In sum, Vermont's wiretap statute must contain a statement of legislative intent, similar to those found in other Vermont statutes. The language of the wiretap statute must be broad. It should not refer to anything that has the potential to limit the scope of its application in the future, such as wires or telephones. Vermont should use the ECPA as guidance when drafting its statute and parallel the ECPA's overall framework, but should not wholly adopt its language. This will allow the statute to distinguish itself from federal law when necessary, while also allowing judges to use case law from other jurisdictions if interpreting a novel issue. Finally, because of the increased prevalence of personal recording devices, the statute must include both criminal and civil penalties.[369]

CONCLUSION

Communications technology has changed considerably since the early days of the telegraph and will continue to evolve at an exponential rate.[370] Vermont must enact a proactive, forward-minded wiretap statute to protect privacy even as technology keeps changing. That does not mean that Vermont must be able to anticipate what kind of future technology will exist. This would be impossible. It does mean that the statute must be conceptual rather than literal. The drafters of the Fourth Amendment intended to protect individual privacy, and they chose language that reflected how they perceived privacy.[371] Similarly, the drafters of Title III chose language to reflect technology that existed in 1968.[372] As this Note has demonstrated, that well-intentioned language later lead to unintentional complications when technology and society changed. As the U.S. Supreme

---

369. *See supra* Part II (outlining the importance of protection against private actors as well as state actors).

370. Nagy, *supra* note 75.

371. U.S. CONST. amend. IV ("The 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 probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

372. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 90–351, 82 Stat. 197 (codified as amended at 18 U.S.C. § 2510 (2012)) (defining communications in terms of transmissions through "wire, cable, or other like connection between the point of origin and the point of reception," reflecting the era before wireless technology).

Court and others have found, what matters is the principles of privacy, not the form that an invasion of privacy takes.[373]

Vermont must enact a wiretap statute to protect its citizens and provide guidance to the judiciary. Vermont should not leave wiretapping to the courts. Judges can best serve the state when they are able to focus on upholding the purpose of the law, rather than debating whether a cell phone call can technically be a "wire communication." Furthermore, the legislature is able to make changes much faster than the courts, and to take input from the citizens they represent.[374]

Instead of observing how technology works at this point in history, the drafters of Vermont's statute must focus on the underlying societal values that a wiretap statute protects. Vermont's wiretap statute should not only protect individual privacy. It should set the scope and standards for permissible wiretapping. The statute protects against privacy violations by both state and private actors. The legislature should not fixate on specific technology because it will inevitably become obsolete. The statute must reflect the value Vermonters place on their privacy, not the specific way in which technology currently intrudes upon that privacy. If Vermont heeds the lessons learned from its sister states by following these guidelines, it can enact a wiretap statute that can endure for decades to come.

Hannah Clarisse[*†]

373. Olmstead v. United States, 277 U.S. 438, 440, 442 (1928) (finding that the principles of privacy apply to all invasions of the security of a person's home); Katz v. United States, 389 U.S. 347, 352 (1957) (noting that the principles of privacy applied in offices, apartments, taxicabs, and phone booths).

374. *See supra* notes 140–45 (describing how legislatures can make changes faster than courts).

* Juris Doctor candidate 2019, Vermont Law School.

† I wish to thank Thomas Flynn, Eliza Van Lennep, and Professor Peter Teachout for their invaluable feedback and guidance. I am incredibly grateful to the Volume 43 production team, Patrick Leary, Allyson Moore, Caitlyn Kelly, Sasha Gainen-Truslow, Kimberly Johnson, Mahmoudy Kemal, Brian Nguyen, Grace Patrick, Madison Pevey, and Amanda Vega, for their outstanding work preparing this Note for publication. Finally, many thanks to Bill Reynolds for giving me the internship that led me to discover this topic.