UC Law SF Communications and Entertainment Journal

Volume 46 | Number 1 Article 2

12-2023

# New Problem, Same Old ECPA: Facebook, Inc. v. State of New Jersey and the Electronic Communications Privacy Act's Growing Inadequacy

Austin Fauni

# New Problem, Same Old ECPA: *Facebook, Inc. v. State of New Jersey* and the Electronic Communications Privacy Act's Growing Inadequacy

BY AUSTIN FAUNI*

**TABLE OF CONTENTS**



* J.D. Candidate, University of California College of the Law, San Francisco, 2024; B.A. Political Science, University of California, Santa Barbara, 2019. To my friends, family, and fellow Comm/Ent editors: I would not have been able to publish this Note without your unwavering support throughout law school, for which I am immensely grateful. I owe this Note to you.

## I. INTRODUCTION

Rapid technological advancements have revolutionized how society communicates over the past thirty-six years since Congress enacted the Electronic Communications Privacy Act (the "ECPA").[1] At the time of the ECPA's enactment, Congress likely could not have imagined the internet-based communication methods that are now profoundly entrenched in modern life. Indeed, words like "internet" and "world wide web" are nowhere in the ECPA's text or legislative history.[2] The ECPA's initial purpose was to develop a more comprehensive statutory framework that ensured Fourth Amendment privacy protections for electronic communications.[3] Yet, Congress has not significantly amended the ECPA in twenty-two years.[4] Given the development of technology during those twenty-two years, it is appropriate to ask whether the ECPA's current framework adequately serves its initial purpose.

*Facebook, Inc. v. State of New Jersey*, a recently decided case by the New Jersey Supreme Court, supports one answer to this question: the ECPA's current framework is becoming increasingly inadequate.[5] Before the New Jersey Supreme Court's *Facebook* decision, the New Jersey Appellate Division held that state law enforcement officials could compel Facebook[6] to disclose two of its users' prospective electronic communications—that is, future communications that have not yet

1. Electronic Communications and Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510–23, 2701–13, 3121–27.

2. Theodore Y. McDonough, *Internet Communications Privacy After United States v. Councilman*, 37 SETON HALL L. REV. 1051, 1054 (2007).

3. Michael D. Roundy, *The Wiretap Act—Reconcilable Differences: A Framework for Determining the "Interception" of Electronic Communications Following United States v. Councilman's Rejection of the Storage/Transit Dichotomy*, 28 W. NEW ENG. L. REV. 403, 413 (2006).

4. The last significant amendment to the ECPA was the USA PATRIOT Act in 2001. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) of 2001, Pub. L. No. 107–56, 115 Stat. 272 (2001).

5. *See* Facebook, Inc. v. State, 254 N.J. 329 (2023).

6. In October 2021, Facebook, Inc. changed its name to Meta Platforms, Inc. Following the lead of the New Jersey Supreme Court's *Facebook* opinion, this Note utilizes the name Facebook to maintain consistency with filings throughout the case. *Id.* at 342 n.1.

happened—every fifteen minutes for thirty days.[7] Moreover, the court held that law enforcement could engage in this practice after obtaining authorization to acquire those communications via communication data warrants ("CDWs"), which are equivalent to standard search warrants.[8] Unlike when law enforcement seeks to acquire certain communications via wiretapping, law enforcement may obtain CDWs with a showing of probable cause and without having to meet further requirements set forth to afford heightened privacy protections.[9] Ultimately, the New Jersey Supreme Court reversed and held that the law enforcement practice involved amounted to the "functional equivalent of wiretap surveillance," thereby affording heightened privacy protections to the communications sought.[10]

As a matter of first impression, the law enforcement practice in *Facebook* presents a meaningful opportunity to analyze how inadequate the ECPA's current framework is in combatting new privacy threats.[11] Additionally, while other jurisdictions have not had to address issues involving law enforcement officials similarly seeking to acquire electronic communications through a standard search warrant, *Facebook* may only be the beginning.[12] Without taking further measures, the electronic communications the ECPA intends to protect from privacy intrusion will eventually be defenseless against new threats like the law enforcement practice in *Facebook*. Widespread, cohesive judicial action is a potential solution. However, modifying the ECPA through legislative action is perhaps more viable.

Altogether, this Note argues that the ECPA's current framework for protecting privacy over electronic communications must be modified to maintain its strength in modern contexts. This Note uses *Facebook*'s facts to highlight two points that exemplify the ECPA's growing inadequacy. First, jurisdictions outside of New Jersey might reason like the New Jersey Appellate Division and permit law enforcement to circumvent the Wiretap Act's heightened privacy protections by seeking to acquire future electronic communications, even if the breadth of communications acquired and the near-contemporaneous basis in which they acquire it is akin to traditional wiretapping.[13] Second, electronic communications can no longer be clearly

7. Facebook, Inc. v. State, 471 N.J. Super. 430, 435-36 (Super. Ct. App. Div. 2022), *rev'd*, 254 N.J. 329 (2023).

8. *Id.* at 435–36, 444.

9. *Facebook*, 254 N.J. at 341–42.

10. *Id.* at 341.

11. New Jersey would have been the first state to allow this type of law enforcement practice. *Amicus Briefs: Facebook v. New Jersey*, ELEC. PRIV. INFO. CTR., https://epic.org/documents/facebook-v-new-jersey/ (last visited May 10, 2023).

12. *Facebook*, 254 N.J. at 369.

13. Brief for Center for Democracy & Technology, Electronic Privacy Information Center (EPIC), and Electronic Frontier Foundation as Amici Curae at 16–23, https://epic.org/documents/facebook-v-

categorized as "in storage" or "in transit" because, in modern contexts like the internet, electronic communications can simultaneously be in storage and transit, even if for just a brief duration.[14]

Part II of this Note provides a historical overview of privacy rights in the United States and the statutory framework governing privacy over electronic communications. Part III examines federal circuit courts' different interpretations and applications of the ECPA, with a focus on the emergence of and challenges to requiring acquisition of communications contemporaneous to transit for a finding of interception under the Wiretap Act and the Storage/Transit Dichotomy. Part IV contextualizes the ECPA's growing inadequacy by discussing the current state of modern electronic communications. Part V begins with an analysis of *Facebook*'s facts under the ECPA and federal precedent to support this Note's argument. Finally, Part V concludes by presenting judicial and legislative solutions to resolve the issues discussed in this Note and applies each solution to *Facebook*'s facts to illustrate their potential strength.

## II. BACKGROUND

### A. PRIVACY RIGHTS AND THE FOURTH AMENDMENT

Privacy rights are deeply rooted in the common law and United States history.[15] During the colonial period, the law acknowledged some right to privacy within one's home based on the long-held understanding that one's home is their castle.[16] Early protections against eavesdropping also exemplify how the law acknowledged some right to privacy in one's communications.[17] Following the Revolutionary War, the Framers' implicitly recognized a need to prevent the government's intrusion onto one's right to privacy, as reflected in in the Third, Fourth, and Fifth Amendments of the Bill of Rights.[18] Since then, the law has continually developed alongside society to address newer privacy threats.[19]

---

new-jersey/. [hereinafter EPIC Amicus Brief]; *see* Facebook, Inc. v. State, 471 N.J. Super. 430, 438 (Super. Ct. App. Div. 2022), *rev'd*, 254 N.J. 329 (2023).

14. United States v. Councilman, 418 F.3d 67, 79 (1st Cir. 2005).

15. Daniel J. Solove, PROSKAUER ROSE LLP, *A Brief History of Information Privacy Law, in* PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE, § 1:2, at 4 (Kristen J. Matthews ed., 2nd ed. 2016).

16. *Id.*

17. *Id.*

18. *Id.* at 5. The Third Amendment protects the privacy of one's home by prohibiting forced quartering of soldiers without the homeowner's consent. U.S. CONST. amend. III. The Fourth Amendment protects privacy over one's person, houses, papers, and effects by prohibiting unreasonable searches and seizures without judicial approval. U.S. CONST. amend. IV. The Fifth Amendment protects one's privacy by protecting against self-incrimination. U.S. CONST. amend. V.

19. Jay Campbell, *Protecting the Future: A Strategy for Creating Laws not Constrained by Technological Obsolescence*, 7 VAND. J. ENT. & TECH. 533, 535 (2005).

In particular, evolving technology has largely shaped privacy law.[20] For example, in the late 19th century, the growth of sensationalist media, compounded with newer technology, like cameras, influenced Louis Brandeis and Samuel Warren to pen their hallmark Harvard Law Review article, "The Right to Privacy."[21] In "The Right to Privacy," Brandeis and Warren were alarmed by the abundant opportunities these advancements posed for invading an individual's right to privacy, which they famously described as a right to be let alone or a right to inviolate personality.[22] Their description was significant because the notion that disseminating information about one's private life to others could cause harm had been relatively unexplored at the time.[23]

Today, Brandeis and Warren's description of the right to privacy remains the touchstone of privacy law. They are best known for defining the implicit acknowledgments of an existing right to privacy in the common law and U.S. history.[24] Further, their urgent call for greater privacy protections through the law influenced the development of privacy torts.[25] Intrusion upon seclusion was the first privacy tort included in the Restatement of Torts.[26] As Comment B to the Restatement of Tort's definition of "intrusion upon seclusion" describes, intrusion upon seclusion is also the type of privacy invasion at the core of modern wiretapping laws.[27]

Federal protections against the government's intrusion onto one's right to privacy through wiretapping originally developed in the Supreme Court's Fourth Amendment jurisprudence.[28] The purpose of the Fourth Amendment[29], which addresses warrants and writs of assistance, was to limit

20. Solove, *supra* note 15, § 1:1, at 3.

21. Louis Brandeis & Samuel Warren, *The Right to Privacy*, 4 HARV. L. REV. 193, 210–11 (1890).

22. *Id.* at 205, 211.

23. Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 ARIZ. L. REV. 1, 2 (1979).

24. *Id.* at 3. Brandeis and Warren examined the underlying principles of various areas of law, including contracts, property, trusts, copyright, trade secrets, and torts, to formulate their description of the right to privacy. *Id.*

25. Solove, *supra* note 15, § 1:4.1, at 12.

26. Roundy, *supra* note 3, at 406.

27. *Id.* The definition of intrusion upon seclusion reads: "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." Restatement (Second) of Torts § 652B. Comment B reads: "The invasion may be by physical intrusion into a place in which the plaintiff has secluded himself… It may also be by the use of the defendant's senses, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs, as by looking into his upstairs windows with binoculars or tapping his telephone wires. It may be by some other form of investigation or examination into his private concerns, as by opening his private and personal mail, searching his safe or his wallet, examining his private bank account, or compelling him by a forged court order to permit an inspection of his personal documents…" *Id.* at cmt. B.

28. Campbell, *supra* note 19, at 536.

29. The Fourth Amendment reads: "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." U.S. CONST. amend. IV.

the government's ability to search or seize one's person, houses, papers, and effects.[30] Nevertheless, in the early 20th century, the majority in *Olmstead v. United States* refused to interpret the Fourth Amendment's prohibition against unreasonable searches and seizures to include warrantless wiretapping by the government.[31] Instead, the majority's interpretation required physical trespass for violations, positing that the Fourth Amendment's protections could not be read to extend beyond the practical meaning of houses, papers, and effects or to forbid hearing or sight.[32]

Justice Brandeis vigorously dissented in the Court's 5-4 split in *Olmstead*, echoing the sentiments expressed in his and Warren's "The Right to Privacy."[33] Brandeis argued that the ongoing discoveries and inventions of the time necessitated further privacy protections and a flexible interpretation of the Fourth Amendment to accommodate a changing society.[34] Brandeis again found it harrowing that subtler and more far-reaching methods for governmental invasion of privacy could become available, be it through newer means to invade the privacy of one's intimacies in their home or one's unexpressed beliefs, thoughts, and emotions.[35] Moreover, Brandeis emphasized that new surveillance methods, particularly wiretaps, not only invaded the privacy of the subject of the wiretap, but also the privacy of every individual who communicated with or was contacted by the subject.[36]

Congress and the Supreme Court began to slowly align with Brandeis' dissenting view in *Olmstead*. Six years after the *Olmstead* decision, Congress enacted protections against wiretapping through the Federal Communications Act (the "FCA") of 1934.[37] Section 605 of the FCA provided safeguards against unauthorized electronic surveillance of private communications, including the interception and disclosure of such communications through wiretapping.[38] In 1967, the Supreme Court's *Berger v. New York* decision signaled a shift in its stance on the privacy threats posed by wiretapping.[39] In *Berger*, the Court overturned a state law that had authorized the collection of private communications without particularity sufficient to satisfy the Fourth Amendment.[40] While the Court noted that electronic surveillance of private conversations by the government

30. Olmstead v. United States, 277 U.S. 438, 464 (1928).
31. *Id.* at 466.
32. *Id.* at 465–66.
33. *Id.* at 471–485.
34. *Id.* at 474.
35. *Id.*
36. *Id.* at 475–476.
37. Roundy, *supra* note 3, at 408.
38. Communications Act of 1934, ch. 652, tit. VI, § 605, 48 Stat. 1064, 1103-04 (1934) (current version at 47 U.S.C. 605(a) (2000)).
39. Berger v. New York, 388 U.S. 41 (1967).
40. *Id.* at 55.

is permissible, it maintained that it should be limited to "the most precise and discriminate circumstances" and for specific offenses because of the potential for collecting excessive swaths of information.[41]

Six months after the *Berger* decision, the Supreme Court in *Katz v. United States* eliminated the *Olmstead* physical intrusion requirement.[42] According to the *Katz* court, "the Fourth Amendment protects people, not places."[43] Paramount in *Katz* was Justice Harlan's concurrence, which established the "reasonable expectation of privacy" standard that still governs privacy law analyses today.[44] Under this standard, the Fourth Amendment's protections are implicated when an individual holds both a subjective and objective expectation of privacy, with objective meaning that society is ready to accept their expectation of privacy as reasonable.[45] The *Katz* decision, along with *Berger*'s limitations on permissible wiretapping, highly influenced the subsequent statutory framework for privacy protections.[46]

### B. STATUTORY PRIVACY PROTECTIONS

One year after the *Berger* and *Katz* decisions, Congress enacted the Omnibus Crime Control and Safe Streets Act of 1968, which included "Title III – Wiretapping and Electronic Surveillance" (the "Wiretap Act").[47] The Wiretap Act was motivated by several congressional findings: the widespread use of unsanctioned wiretaps and other surveillance devices, wiretapping's utility given the legitimate needs of law enforcement, and the exigency of developing a uniform system for ensuring privacy protections over the communications of parties involved.[48] Congress also incorporated the *Berger* requirements[49] and limited permissible wiretapping to certain major crimes.[50] Nevertheless, the Wiretap Act's reach only extended to "aural" communications and did not cover visual surveillance or other forms

41. *Id.* at 56. The permissible circumstances for wiretapping enumerated in *Berger* require, "(1) prior judicial authorization, (2) specification of particular offenses said to justify the intrusion, (3) specification 'with particularity' of the conversations sought to be seized, (4) minimization of the duration of the wiretap, (5) termination once the conversation sought is seized, and (6) a showing of exigent circumstances justifying the use of the wiretap procedure." Nixon v. Admin. of Gen. Serv., 433 U.S. 425, 463 (1977).

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

43. *Id.* at 351.

44. *Id.* at 360–62.

45. *Id.* at 361.

46. McDonough, *supra* note 2, at 1054.

47. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211 (1968) (codified as amended at 18 U.S.C. §§ 2510-2522 (2000)).

48. Roundy, *supra* note 3, at 411.

49. *Electronic Communications Privacy Act (ECPA)*, ELEC. PRIV. INFO. CTR., https://epic.org/ecpa/ (last visited May 10, 2023).

50. Roundy, *supra* note 3, at 411.

of electronic communication that eventually arose in prominence, like email.[51]

In 1986, Congress extended the Wiretap Act's reach through the ECPA.[52] Within the context of newer computer and telecommunications technology, the Wiretap Act's clear inadequacy in addressing privacy concerns motivated Congress to bring surveillance of electronic communications within the scope of the statutory framework.[53] The ECPA is comprised of three major parts: (1) Title I, which amended the original Wiretap Act[54] to include electronic communications; (2) Title II, which introduced the first regulations for access to stored wire and electronic communications (the "Stored Communications Act" or "SCA"); and (3) Title III, which regulated the use of pen registers and trap and trace devices (the "Pen Register Act").[55]

Following the ECPA, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act[56] (the "PATRIOT Act") amended the Wiretap Act and SCA.[57] Among other things, the PATRIOT Act erased communications in electronic storage from the Wiretap Act's definition of "wire communication," and, in effect, aligned it more closely with the definition of "electronic communication."[58] The PATRIOT Act also eased some restrictions on law enforcement's access to stored communications.[59] Although several of the PATRIOT Act's other provisions were set to sunset on December 31, 2005 because of some legislator's concerns about their constitutionality, Congress reauthorized the PATRIOT Act in 2006.[60]

Today, the Wiretap Act and SCA govern protections over wire, oral, and electronic communications.[61] The SCA relies on definitions provided in the Wiretap Act, which are integral to understanding current issues involving courts' differing analyses and applications of the ECPA.[62] Notably, the

51. Solove, *supra* note 15, § 1:4.2, at 21; *see also* Roundy, *supra* note 3, at 413.

52. *See* Electronic Communications and Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510–23, 2701–13, 3121–27.

53. Roundy, *supra* note 3, at 413.

54. From this point forward in this note, "Wiretap Act" will refer to the Wiretap Act as amended by the ECPA.

55. Roundy, *supra* note 3, at 413; Solove, *supra* note 15, § 1:4.3, at 32–33; Electronic Communications and Privacy Act (ECPA), 18 U.S.C. §§ 2510–22, 2701–11, 3121–27.

56. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) of 2001, Pub. L. No. 107–56, 115 Stat. 272 (2001).

57. Samantha L. Martin, *Interpreting the Wiretap Act: Applying Ordinary Rules of "Transit" to the Internet Context*, 28 CARDOZO L. REV. 441, 451–52 (2006).

58. *Id.* at 451 n. 78. The SCA relies on definitions provided under the Wiretap Act. *Id.*

59. *Electronic Communications Privacy Act of 1986 (ECPA)*, BUREAU OF JUST. ASSISTANCE, https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285 (last visited May 10, 2023).

60. *Id.*; *see also* Brian Duignan, *USA PATRIOT Act*, BRITANNICA, https://www.britannica.com/topic/USA-PATRIOT-Act (Sept. 18, 2023).

61. Martin, *supra* note 57, at 452.

62. Martin, *supra* note 57, at 452 n. 78.

definitions of wire[63], oral[64], and electronic[65] communications do not explicitly include or exclude communications in electronic storage.[66]This ambiguity surrounding communications in electronic storage, especially those in temporary or transient storage, has become increasingly problematic for courts.[67]

In particular, this ambiguity is problematic when courts must decide whether the Wiretap Act or SCA should govern issues involving the ease with which law enforcement might be able to obtain such communications.[68] To better understand the different implications that the Wiretap Act and SCA pose to law enforcement, it is essential to note that the Wiretap Act prohibits intentional and unauthorized interception, use, and disclosure of wire, oral, or electronic communications, as defined in the statute.[69] The Wiretap Act defines "intercept[ion]" as "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."[70] Notwithstanding communications in temporary or transient storage, the ultimate question is whether law enforcement can—in general—intercept communications in electronic storage within the meaning of the Wiretap Act, thus triggering its protections.

If law enforcement *can* intercept communications in electronic storage, despite the Wiretap Act neither including nor excluding such communications in its definitions of wire, oral, and electronic communications, the crucial implication is that law enforcement must meet

63. The Wiretap Act defines "wire communication" as, "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce" 18 U.S.C. § 2510(1).

64. The Wiretap Act defines "oral communication" as, "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying any expectation, but such term does not include any electronic communication." 18 U.S.C. § 2510(2).

65. The Wiretap Act defines "electronic communication" as, "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photooptical system that affects interstate or foreign commerce, but does not include– (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (defined in section 3117 of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage of funds." 18 U.S.C. § 2510(12)(A)–(D).

66. Martin, *supra* note 57, at 452. The Wiretap Act defines "electronic storage" as, "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17)(A)–(B).

67. *Id.*

68. Martin, *supra* note 57, at 452–453.

69. 18 U.S.C. § 2511(1).

70. 18 U.S.C. §§ 2510(4), 2511(1)(a)–(b).

heightened requirements outlined in the Wiretap Act before receiving authorization through a warrant to engage in the interception of such communications.[71] Otherwise, they would violate the statute's prohibition against unauthorized interception.[72] The heightened requirements include establishing a showing of probable cause and meeting the several *Berger* requirements now codified in the statute, like stating with particularity the conversations sought to be seized and minimizing the duration of the wiretap.[73]

On the other hand, if law enforcement *cannot* intercept communications in electronic storage within the meaning of the Wiretap Act, the SCA would protect such communications. The SCA prohibits intentionally accessing or exceeding access to electronic communication in storage without prior authorization.[74] Notably, the standards that law enforcement must meet to receive authorization to obtain such communications are less stringent under the SCA.[75] For example, instead of requiring a showing of probable cause, the SCA only requires that law enforcement "offer specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[76] Given the varying levels of protection provided by the Wiretap Act and SCA, the answer to whether communications in electronic storage can be intercepted poses significant consequences for privacy over one's communications.

## III. THE ECPA IN ACTION

### A. TWO DISTINCT WAYS OF ANALYZING THE ECPA

Absent on-point United States Supreme Court precedent, federal circuit courts have generally analyzed and applied the ECPA in two distinct ways when addressing the ambiguity surrounding communications in electronic storage.[77]

Under the first type of analysis, a court begins by determining whether communications in electronic storage are within the scope of the Wiretap Act's definition of "electronic communication."[78] If the court answers "no," then the SCA governs the issue.[79] If the court answers "yes," the court will

71. 18 U.S.C. §§ 2516(3), 2518.
72. 18 U.S.C. §§ 2516(3), 2518.
73. 18 U.S.C. § 2518.
74. 18 U.S.C. § 2701(a).
75. 18 U.S.C. § 2703(d).
76. *Id.*
77. Martin, *supra* note 57, at 453.
78. *Id.* at 453–454.
79. *Id.*

only find that such communications were intercepted if their acquisition was contemporaneous to transit before the communications reached their final destination.[80] In other words, the court will view communications in storage at their final destination as incapable of interception, so the SCA will still govern instead of the Wiretap Act.[81] Ultimately, the court's analysis of interception will rest on whether the communications were in storage or transit when acquired.[82] This notion is known as the Storage/Transit Dichotomy.[83]

Under the second type of analysis, a court finds that "electronic communication" includes communications in temporary or transient electronic storage if storage is incidental to transmission.[84] As opposed to adhering to the Storage/Transit Dichotomy, the court's reasoning is that communications in transient electronic storage are in transit until they reach their final destination.[85] In this view, it is possible for electronic communications to be simultaneously in storage and transit.[86] While this type of court focuses less on the Storage/Transit Dichotomy, it still maintains that only acquisition contemporaneous to transit will amount to interception and trigger the Wiretap Act's protections.[87] Unsurprisingly, the Wiretap Act's lack of clarity[88] has influenced these differing and confusing analyses and applications of the ECPA.

### B. THE ACQUISITION CONTEMPORANEOUS TO TRANSIT REQUIREMENT AND THE STORAGE/TRANSIT DICHOTOMY

The acquisition contemporaneous to transit requirement for a finding of interception under the Wiretap Act can be traced back to the Fifth Circuit's 1976 decision in *United States v. Turk*.[89] At that time, the pre-ECPA Wiretap Act defined "intercept" as "the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device."[90] Based on this definition, the court held that no interception occurs when the contents of communications are acquired by replaying previously recorded communications.[91] The court reasoned that the central concern of the Wiretap Act's "intercept" definition is the surveillance

80. *Id.*
81. *Id.*
82. *Id.*
83. Roundy, *supra* note 3, at 418.
84. Martin, *supra* note 57, at 454.
85. *Id.*
86. *Id.* at 454–55.
87. Martin, *supra* note 57, at 454.
88. The Wiretap Act is "famous (if not infamous) for its lack of clarity." Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994).
89. Roundy, *supra* note 3, at 417; United States v. Turk, 526 F.2d 654, 658 (5th Cir. 1976).
90. 18 U.S.C. § 2510(4) (1970).
91. *Turk*, 526 F.2d at 659.

engaged in at the time of the communication that led it to be heard by uninvited listeners, not the hearing of the communication that might follow.[92] Thus, *Turk* established the rule that interception requires acquiring communications while in transit.[93] This requirement persisted in federal circuit decisions even after the ECPA's enactment in 1986, which, among other things, added electronic communications to the definition of "intercept" and amended the definition of "wire communication."[94]

The Fifth Circuit's later decision in *Steve Jackson Games, Inc. v. United States Secret Service* established the Storage/Transit Dichotomy and illustrated how *Turk* came into play with electronic communications.[95] In *Steve Jackson Games*, the court held that reading private emails sent to an electronic bulletin board, but not yet read by its intended recipients on a seized computer, did not constitute interception because electronic communications in storage cannot be contemporaneously acquired.[96] For support, the court pointed out that the Wiretap Act included communications in electronic storage in its definition of "wire communication," as revised by the ECPA, unlike the definition of "electronic communication."[97] Therefore, the plain text of the ECPA[98] supported a reading of the Wiretap Act that did not apply its "intercept" prohibition (and *Turk*'s contemporaneous acquisition requirement) to electronic communications in storage, including the emails at issue that were in storage and no longer in transit when read from the seized computer.[99]

The Ninth Circuit soon adopted an approach to the ECPA that matched the Fifth Circuit's approach. The Ninth Circuit first endorsed the *Steve Jackson Games* court's rationale in *United States v. Smith*.[100] In *Smith*, the court held that a non-party's retrieval of wire communications in storage, specifically voicemails, constituted interception under the Wiretap Act.[101] Regarding electronic communications, the court narrowly interpreted "intercept," stating, "it is natural to except non-contemporaneous retrievals from the scope of the Wiretap Act" and pointing to the *Steve Jackson Games* court's distinction between the post-ECPA definitions of "wire

92. *Id.* at 658–59.

93. *Id.* at 658.

94. Martin, *supra* note 57, at 456; 18 U.S.C. § 2510(4).

95. Roundy, *supra* note 3, at 420; Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 460–63 (5th Cir. 1994).

96. *Steve Jackson Games*, 36 F.3d at 458–60.

97. *Id.* at 461.

98. "The plain meaning canon instructs that the ordinary meaning of the words in a statute should control interpretation." LINDA D. JELLUM, MASTERING LEGISLATION, REGULATION, AND STATUTORY INTERPRETATION 85 (3d ed. 2020).

99. *Steve Jackson Games*, 36 F.3d at 461–62.

100. United States v. Smith, 155 F.3d 1051,1057–58 (9th Cir. 1998).

101. *Id.* at 1059.

communication" and "electronic communication."[102] Namely, the court accepted the *Steve Jackson Games* court's argument that Congress' omission of communications in electronic storage from the definition of "electronic communication" reflected an intent not to apply the Wiretap Act's prohibition against interception to electronic communications in storage.[103] On these grounds, the *Smith* decision implied that the SCA, rather than the Wiretap Act, governed issues involving electronic communications in storage, but not wire communications in storage.[104]

However, when assessing *Smith* and *Steve Jackson Games* in modern contexts, it is essential to recognize how the PATRIOT Act undercuts both courts' reasoning. To begin, Congress' goal for including communications in electronic storage in the definition of "wire communications" was to provide protections for voicemails under the Wiretap Act—it had nothing to do with electronic communications like the emails at issue in *Steve Jackson Games*.[105] When Congress passed the PATRIOT Act and sought to lessen those protections in 2001, they succeeded by erasing communications in electronic storage from the definition of "wire communication."[106] This revision effectively placed voicemails outside the scope of the Wiretap Act and within the scope of the SCA and its less stringent requirements for authorized access.[107] Essentially, the PATRIOT Act eliminated the *Smith* and *Steve Jackson Games* courts' key textual distinction between "wire communication" and "electronic communication" and their analysis of Congress' intent behind the ECPA, weakening the soundness of their holdings and the Storage/Transit Dichotomy.[108]

Nonetheless, in 2002, the Ninth Circuit continued to uphold a narrow interpretation of "intercept" and apply a contemporaneous acquisition requirement.[109] In *Konop v. Hawaiian Airlines, Inc.*, the court held that stored contents on a password-restricted website fell within the meaning of "electronic communication."[110] But to constitute interception, unauthorized access to the website's contents still required contemporaneous acquisition rather than acquisition from electronic storage.[111] The court reasoned that Congress was aware of this narrow judicial interpretation of "intercept" and chose not to modify it through the PATRIOT Act, thereby implicitly

102. *Id.* at 1057.

103. *Id.* (quoting *Steve Jackson Games*, 36 F.3d at 461–62).

104. *Id.* at 1059.

105. United States v. Councilman, 418 F.3d 67, 76 (1st Cir. 2005).

106. Robert A. Pikowsky, *An Overview of the Law of Electronic Surveillance Post September 11, 2001*, 94 L. LIBR. J. 601, 609 (2002).

107. Martin, *supra* note 57, at 458 n. 115.

108. Martin, *supra* note 57, at 451 n. 78. The SCA relies on definitions provided under the Wiretap Act. *Id.*

109. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002).

110. *Id.* at 876.

111. *Id.* at 878.

approving it.[112] Ultimately, Congress had re-instated the pre-ECPA definition of "intercept," which required the contemporaneous acquisition of communications, as interpreted in earlier cases like *Turk*.[113]

### C. CHALLENGING THE ACQUISITION CONTEMPORANEOUS TO TRANSIT REQUIREMENT AND THE STORAGE/TRANSIT DICHOTOMY

The Fifth and Ninth Circuits' approach to applying the ECPA did not come without critiques or challenges. For example, Judge Reinhard's dissent in *Konop* called the majority's holding confusing and incoherent.[114] First, Reinhard argued it was illogical to simultaneously include and exclude electronic communications in storage from the ECPA's prohibition against interception, as the majority did by holding that electronic communications in storage are within the definition of "electronic communications" but still requiring acquisition contemporaneous to transit.[115] This, according to Reinhard, rendered the ECPA's prohibition against interception of electronic communications superfluous and violated a precept against interpreting one part of a statute to negate another.[116] Second, Reinhard raised concerns about the nature of electronic communications and the soundness of the Storage/Transit Dichotomy.[117] Reinhard pointed out that electronic communications spend an "infinitesimal" amount of time in transit, yet the majority held that electronic communications, which are typically acquired by obtaining a copy in transit or at their destination, are in storage.[118]

Judge Reinhard's second point underlies the First Circuit's later rejection of the Storage/Transit Dichotomy in *United States v. Councilman*.[119] In *Councilman*, the defendant, a vice president of a company that ran an online listing service for rare and out-of-print books, was indicted with conspiracy to violate the Wiretap Act.[120] The company provided book dealers with an email address at their domain and acted as the email provider, with the defendant managing the email service and dealer subscription list.[121] Hoping to gain a commercial advantage, the defendant instructed employees

112. *Id.*; "By far the most common legislative response to a judicial interpretation of a statute is silence. Some judges reason that a legislature's silence to an interpretation means acquiescence, or agreement, with that interpretation." JELLUM, *supra* note 98, at 298.

113. *Konop*, 302 F.3d at 878.

114. *Id.* at 887 (Reinhard, J. dissenting).

115. *Id.* at 888.

116. *Id.*; "According to the *rule against surplusage*, the proper interpretation of a statute is one in which every word has meaning; nothing is redundant or meaningless." JELLUM, *supra* note 98, at 190.

117. *Konop*, 302 F.3d at 888.

118. *Id.*

119. United States v. Councilman, 418 F.3d 67 (1st Cir. 2005); *see also In re* Pharmatrak Privacy Litig., 329 F.3d 9, 21 (1st Cir. 2003) (suggesting that the storage-transit dichotomy adopted by earlier courts may be less than apt to address current problems because of evolving technology and its increasing prominence).

120. *Councilman*, 418 F.3d at 70–71.

121. *Id.* at 70.

to intercept and copy all communications from a competing company.[122] Additionally, the defendant had the email server modified so that all of the competitor's communications would be copied and stored in a separate mailbox before reaching their intended recipients.[123] The defendant had access to the separate mailbox, and the scheme ultimately allowed the defendant and other employees to intercept and read thousands of the competitor's messages.[124] Sitting en banc, the First Circuit held that the emails fell within the Wiretap Act's purview because they were merely in transient storage, and "electronic communication" includes communications in transient storage.[125]

In particular, the First Circuit rejected the defendant's argument that the Wiretap Act did not protect the emails because "electronic communication," as defined by the plain text of the ECPA, generally excluded communications in electronic storage.[126] The court began by pointing to the ambiguity in the ECPA's text to rebut the presumption that Congress acted intentionally when they included communications in electronic storage in the definition of "wire communication" but not "electronic communication."[127] Further, the court argued that the ECPA's text remained ambiguous on whether electronic communications in transient storage during transmission fell within "electronic communication" because Congress did not explicitly include them as an exception to the general prohibition against interception of an electronic communication.[128] The court relied on the interpretive principle that additional exceptions should not be implied when they are not explicitly listed and reasoned that Congress would have listed an exception for electronic communications in transient storage if they intended to not afford such protections under the Wiretap Act.[129]

The First Circuit also examined the ECPA's legislative history to reject the defendant's argument.[130] First, the court emphasized that Congress

122. *Id.*

123. *Id.* at 70–71 (1st Cir. 2005). The parties stipulated that the emails were in the random-access memory (RAM), hard disks, or both within the company's computer system and therefore fell within the ECPA's definition of electronic storage. *Id.* at 73.

124. *Id.* at 70–71; 79.

125. *Id.* at 69.

126. *Id.* at 73–76.

127. *Id.* at 73–76; "*Expressio unius* presumes . . . that when the legislature includes some circumstances explicitly, then the legislature intentionally omitted other similar circumstances that would logically have been included. In other words, the canon presumes that the legislature considered and rejected every related possibility." JELLUM, *supra* note 98, at 193.

128. *Id.* at 74–76. The ECPA states that an electronic communication does not include "(A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device…; or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds." 18 U.S.C. § 2510(12).

129. *Councilman*, 418 F.3d at 74–76.

130. *Id.* at 76–79.

broadly defined "electronic storage" to increase privacy protections for stored data under the Wiretap Act.[131] Therefore, Congress likely did not intend to exclude emails stored during transmission, like those at issue, from its heightened protections.[132] Second, the court highlighted that Congress's sole purpose for adding communications in electronic storage to the definition of "wire communication" was to protect voicemails—it had nothing to do with emails.[133] The fact that Congress later chose to lessen protections for voicemails by removing electronic storage from the definition of "wire communication" through the PATRIOT Act supported this point because the PATRIOT Act's revision effectively removed stored voicemails from the Wiretap Act's scope and placed them within the SCA's scope.[134]

Thus, the First Circuit's holding that electronic communications in transient storage are capable of interception under the Wiretap Act served as a rejection of the Storage/Transit Dichotomy supported by the Fifth and Ninth Circuits.[135] According to the First Circuit's perspective, there is a possibility that communications like emails are simultaneously in storage and transit because "an email does not cease to be an 'electronic communication' during the momentary intervals intrinsic to the communication process, at which the message resides in transient electronic storage."[136] Moreover, it did not make sense that Congress would have contemplated the "existential oddity" posited by the *Councilman* defendant's argument that electronic communications briefly cease to be electronic communications for short intervals and then suddenly become electronic communications again.[137] Altogether, *Councilman* clearly answered whether "electronic communication" includes communications in electronic storage: yes, but only those in transient storage incidental to transit.[138]

Nonetheless, another important aspect of the decision is the specific nature of the defendant's indictment, which only charged the defendant with conspiracy to violate the Wiretap Act.[139] Because of this, the court did not need to directly address whether the defendant's actions constituted interception under the Wiretap Act, which in turn would have required

131. *Id.* at 76.

132. *Id.*

133. *Id.*

134. *Id.* at 78-79. Section 209 of the USA PATRIOT Act amended the Wiretap Act and Stored Communications Act, "to clear up the ambiguity about which governs access to voicemail. Law enforcement officers can now obtain judicial authorization for access to voicemail pursuant to the lesser requirements of the Stored Communications Act." Pikowsky, *supra* note 106, at 609.

135. *Councilman*, 418 F.3d at 79.

136. *Id.*

137. "Congress contemplated the existential oddity that Councilman's interpretation creates: messages – conceded by stipulation to be electronic communications – briefly cease to be electronic communications for very short intervals, and then suddenly become electronic communications again." *Id.* at 78.

138. *Id.* at 69.

139. *Id.* at 71.

answering whether the Wiretap Act's prohibition against interception only applies to acquisitions contemporaneous to transit or acquisitions of fully transmitted communications too.[140] From the Fifth and Ninth Circuits' perspective, the answer would be that the defendant did not intercept the emails because they were acquired from storage, and interception requires acquisition contemporaneous to transmission.[141] While the First Circuit did not directly answer this question, it still rejected the idea that the very nature of a communication being in storage negated the need to assess whether interception had occurred, as the Fifth and Ninth Circuits would have done.[142] The First Circuit also suggested that the defendant likely could not have successfully argued that fully transmitted electronic communications are incapable of interception, implying that the fact that the defendant acquired the emails before they reached their intended recipients carried some weight in the assessment of interception.[143]

## IV. THE ECPA IN MODERN CONTEXTS

*Councilman* highlighted the struggle that courts face when applying the ECPA to issues involving modern communication forms like email; however, the ECPA has not evolved like technology has continued to do since *Councilman*. The most recent legislative developments affecting the ECPA includes the PATRIOT Act in 2001, its reauthorization in 2006, and the Foreign Intelligence and Surveillance Amendments Act in 2008, none of which have specifically addressed the courts' struggles discussed above.[144] The proliferation of the internet and online communication, compounded with the lack of a new statute or amendments to the ECPA to protect these communications, also leaves a growing number of these communications vulnerable to new and emerging privacy threats.[145] Altogether, the ECPA's lack of comprehensive updates exemplifies the legal system's inherent and inimical slowness in adapting to evolving technology: legislators write laws to address technology that exists at the time, but as that technology becomes obsolete, so do those laws.[146]

140. *Id.* at 80.

141. *See* Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 458 (5th Cir. 1994); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002).

142. *See Councilman*, 418 F.3d at 79–80.

143. *Id.* at 80.

144. Summary of the *Electronic Communications Privacy Act of 1986 (ECPA)*, BUREAU OF JUST. ASSISTANCE, https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285 (last visited May 10, 2023).

145. McDonough, *supra* note 2, at 1051.

146. Campbell, *supra* note 19, at 534. Words like "internet" and "world wide web" do not even appear in the ECPA's text, nor do those words appear in the ECPA's legislative history. McDonough, *supra* note 2, at 1054.

Today, engaging in electronic communication over the internet is the norm.[147] Messaging apps on smartphones and laptops, such as Facebook Messenger and WhatsApp, are the most popular form of electronic communication over the internet and offer users virtually instantaneous transmission of messages.[148] To do so, their systems break messages down into smaller pieces of data ("packets"), which are sent and stored along intermediate routers until they reach their final destination.[149] The technological structure of messaging apps is similar to that of electronic communication via email or messaging systems like iMessage.[150] Essentially, this structure illustrates how many electronic communications may simultaneously be in storage and transit, as the Fifth Circuit in *Councilman* acknowledged.[151]

Furthermore, electronic communication nowadays involves more than an exchange of words.[152] Beyond instant messaging, messaging apps enable millions of users to share photos, make voice or video calls, and engage in e-commerce, among other features.[153] Launched in 2011, Facebook Messenger is the most popular messaging app in the United States, with approximately 135.9 million users in 2021.[154] Globally, WhatsApp is the most popular messaging app[155], though Facebook Messenger still maintains almost one billion monthly active users who utilize it to communicate with friends, family, and businesses.[156] Several factors have played into these messaging apps' growing popularity, such as their free or low cost, quick response times, the ability to engage in multiple conversations simultaneously, and multigenerational appeal.[157] Notably, their popularity will only continue growing.[158]

Overall, the proliferation of electronic communication over the internet emphasizes the need to revisit the ECPA. As the popularity of messaging

147. EPIC Amicus Brief, *supra* note 13, at 18; The internet is, "an international network of interconnected computers that allows millions of people to communicate and exchange information." Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002).

148. *Messaging App Statistics: The Most Popular Messaging Platforms in 2023 & Beyond*, SPECTRM (Oct. 25, 2022), https://spectrm.io/insights/blog/messaging-app-statistics-most-popular-communication-method-2020/; EPIC Amicus Brief, *supra* note 13, at 17.

149. Richard T. Wang, *Cookies and Wires: Can Facebook Lure Users into Divulging Information Under the Wiretap Act's Party Exception?*, 106 CORNELL L. REV. 1937, 1945 (2022).

150. EPIC Amicus Brief, *supra* note 13, at 17–18; Shira Ovide, *American's Can't Quit SMS*, N.Y. TIMES (Feb. 2, 2022), https://www.nytimes.com/2022/02/02/technology/sms-whatsapp.html; Wang, *supra* note 149, at 1945–46.

151. United States v. Councilman, 418 F.3d 67, 79 (1st Cir. 2005).

152. *See* SPECTRM, *supra* note 148.

153. *Id.*

154. Claire Beveridge, *22 Facebook Messenger States Marketers Must Know in 2022*, HOOTSUITE (Apr. 27, 2022), https://blog.hootsuite.com/facebook-messenger-stats/; SPECTRM, *supra* note 148.

155. SPECTRM, *supra* note 148.

156. Beveridge, *supra* note 154.

157. SPECTRM, *supra* note 148.

158. *Id.*

apps and similar technologies continues growing, more communications are left open to privacy threats that the ECPA is ill-equipped to address. These threats may come from citizens or corporations seeking to acquire private communications or from the government, as the Fourth Amendment acknowledges.[159] Currently, a salient issue is whether the ECPA requires law enforcement to apply for a wiretap warrant to receive authorization to acquire certain electronic communications. Central to this Note and illustrative of this issue is the New Jersey Supreme Court's decision in *Facebook*, which involves a law enforcement practice of seeking near-contemporaneous acquisition of prospective electronic communications—that is, future communications that have not yet occurred—without a wiretap warrant.[160]

## V. *FACEBOOK, INC. V. STATE OF NEW JERSEY*

### A. INTRODUCTION

Before delving into this Note's analysis, it is necessary to acknowledge that *Facebook* is a state case rather than a federal case brought under New Jersey's analog to the ECPA: the New Jersey Wiretapping and Electronic Surveillance Control Act (the "NJWESCA").[161] The NJWESCA and ECPA share the same definitions for "intercept,"[162] "electronic communication,"[163] and "electronic storage."[164] Like the Wiretap Act, the NJWESCA maintains heightened protections against privacy intrusion by the government through wiretapping, such as requiring the government to state with particularity the conversations sought to be seized and minimizing the duration of the wiretap.[165] New Jersey's Appellate Division and Supreme Court in

159. U.S. CONST. amend. IV.

160. Facebook, Inc. v. State, 254 N.J. 329, 340 (2023).

161. *Id.* at 348–53 (2023); The New Jersey Wiretapping and Electronic Surveillance Control Act, N.J. STAT. ANN. § 2A:156A-1-37 (1968).

162. The ECPA and NJWESCA define "intercept" as "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." Facebook, Inc. v. State, 471 N.J. Super. 430, 448–49 (Super. Ct. App. Div. 2022), *rev'd*, 254 N.J. 329 (2023); 18 U.S.C. § 2510(4); N.J. STAT. ANN. § 2A:156A-2(c) (1968).

163. The ECPA and NJWESCA define "electronic communication" to include, "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system that affects interstate or foreign commerce." *Facebook*, 471 N.J. Super. at 450; 18 U.S.C. § 2510(12); N.J. STAT. ANN. § 2A:156A-2(m) (1968).

164. The ECPA and NJWESCA define "electronic storage" as, "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," as well as, "any storage of such communication by an electronic communication service for . . . backup protection." *Facebook*, 471 N.J. Super. at 450; 18 U.S.C. § 2510(17); N.J. STAT. ANN. § 2A:156A-2(q) (1968).

165. NJWESCA provides, "No order entered under this section shall authorize the interception of any wire, electronic or oral communication for a period of time in excess of that necessary under the circumstances. Every order entered under this section shall require that such interception begin and terminate as soon as practicable and be conducted in such a manner as to minimize or eliminate the

*Facebook* also looked to federal circuit decisions involving the ECPA in its analysis,[166] explaining, "Where the federal and state statutes overlap, we look to the federal court for guidance."[167] As a matter of first impression, *Facebook*'s facts present a meaningful opportunity to analyze the ECPA's strength against new and emerging privacy threats, despite the fact that it is a state case.[168] For the purpose of this Note's argument, this Note primarily examines *Facebook* under the ECPA and key federal precedent discussed above.

### B. FACTS AND PROCEDURAL HISTORY

*Facebook* is a consolidation of separate actions arising from criminal investigations by New Jersey law enforcement in Atlantic and Mercer Counties.[169] In each county, law enforcement obtained communication data warrants ("CDWs") to search the subjects' Facebook accounts after establishing probable cause that their accounts would provide or tend to show evidence of criminal conduct and the identity of individuals involved.[170] The CDWs required Facebook to disclose past communications starting at a specific date and prospective communications for thirty days post-issuance without notice to the subjects.[171] These communications included "images, videos, audio files, posts, comments, histories, and the contents of all private messages in all message folders, including inbox, sent, chat messenger, and trash folders."[172] With respect to the prospective communications, the CDWs granted law enforcement exclusive "real-time" access to "cloned" or "active duplicate" versions of the subjects' accounts.[173] The CDWs required Facebook to disclose the communications to law enforcement through the duplicate accounts in approximately fifteen-minute intervals.[174] These actions arose after Facebook challenged the portion of the CDWs that required disclosure of prospective communications.[175]

---

interception of such communications not otherwise subject to interception under this act by making reasonable efforts, whenever possible, to reduce the hours of interception authorized by said order." N.J.S.A. 2A:156A-12 (1968).

166. *Facebook*, 471 N.J. Super. at 455–59; see Facebook, Inc. v. State, 254 N.J. 329, 357–361 (2023).

167. *Facebook*, 471 N.J. at 444 n.5.

168. If allowed, New Jersey would have been the first state to allow this type of law enforcement practice. *Amicus Briefs: Facebook v. New Jersey*, ELEC. PRIV. INFO. CTR., https://epic.org/documents/facebook-v-new-jersey/ (last visited May 10, 2023).

169. *Facebook*, 471 N.J. Super. at 435–36.

170. *Id.* at 436–37.

171. *Id.* at 438. The Atlantic CDW provided law enforcement with 74 days' worth of past communications, while the Mercer CDW provided law enforcement with 63 days' worth. *Id.* at 436–39.

172. *Id.* at 438.

173. *Id.*

174. In its brief, the State represented that the Mercer CDW omitted this 15-minute procedure by error and that this police practice had been normal practice since at least February 2020. *Id.* at 438–39.

175. *Id.* at 439.

Both trial court judges quashed the CDWs in part, determining that wiretap warrants, rather than CDWs, were necessary to compel Facebook's disclosure of prospective communications.[176] According to the Atlantic judge, granting surveillance of communications that had not yet occurred was tantamount to interception, notwithstanding the fifteen-minute delay.[177] The Mercer judge held similarly but relied on cases like *Councilman* to explain how the CDWs' grant of ongoing acquisition of prospective electronic communications amounted to interception.[178] According to the Mercer judge, interception was possible because interception is not limited to acquisition contemporaneous to transit.[179] Instead, interception is possible when storage of communication is inherent to the transmission process, as it was here, given law enforcement's "real-time" access to duplicate accounts and communications stored on these accounts, notwithstanding the fifteen-minute delay.[180] The transmission process necessarily involved acquisition of stored communications because Facebook represented that their systems could not provide perfectly contemporaneous acquisition.[181] Like the appellate court, both trial court judges also noted their concern with the prolonged privacy intrusions and potential Fourth Amendment violation posed by the CDWs' thirty-day length.[182]

Once consolidated, the appellate court held that compelling disclosure of prospective communications did not require a wiretap warrant because doing so did not amount to interception, which, under the ECPA and NJWESCA, requires contemporaneous acquisition.[183] The appellate court followed the same Storage/Transit Dichotomy analysis employed by the Fifth and Ninth Circuits, arguing that communications in storage are incapable of interception because they are no longer in transit.[184] The communications at issue were acquired from storage, so law enforcement did not engage in interception.[185] In other words, the communications had already come to rest in storage on Facebook's servers before Facebook needed to disclose the communications pursuant to the fifteen-minute procedure in the CDWs.[186] To support their holding, the appellate court pointed to decisions like *Steve Jackson Games* and *Konop,* plus the ECPA's text, which does not explicitly include communications in electronic storage under the meaning of "intercept" as applied to an "electronic

176. *Id.* at 439–40.
177. *Id.* at 440.
178. *Id.* at 440–41.
179. *Id.*
180. *Id.*
181. *Id.*
182. *Id.* at 441.
183. *Id.* at 435–36.
184. *Id.* at 455–57.
185. *Id.* at 458–59.
186. *Id.*

communication."[187] Ultimately, the appellate court held that CDWs were appropriate because CDWs, much like the SCA, are concerned with the type of electronic communications at issue here: electronic communications in storage. [188]

### C. ANALYSIS OF THE ECPA'S INADEQUACY AND THE DANGERS POSED BY THE NEW JERSEY APPELLATE DIVISION'S REASONING

Again, the Wiretap Act is "famous (if not infamous) for its lack of clarity,"[189] so summarizing each side's argument from the perspective of the ECPA is helpful before analyzing its inadequacy. On the one hand, New Jersey argued that no wiretap warrant is necessary when seeking prospective electronic communications.[190] First, under the Wiretap Act, law enforcement did not "intercept" any communications because the prospective electronic communications are in storage when acquired, and an "electronic communication" does not include those in storage.[191] Instead, the SCA governs electronic communications in storage.[192] Second, electronic communications in storage are incapable of interception because interception requires acquisition contemporaneous with transit, and communications in storage are no longer in transit.[193] Ultimately, New Jersey's argument aligned with the Fifth and Ninth Circuit's approach to the ECPA.

On the other hand, Facebook argued—as the trial court judges found—that law enforcement did "intercept" the prospective electronic communications because electronic communications in storage do not cease to be an "electronic communication" when storage is merely incidental to transmission.[194] Here, storage of the prospective electronic communications on Facebook's servers was due to technological necessity, or in other words, incidental to transmission.[195] Thus, the communications are still an "electronic communication" within the meaning of the Wiretap Act.[196] Notwithstanding the fifteen-minute delay in disclosure, Facebook argued a wiretap warrant was necessary because law enforcement intercepted these

187. *Id.* at 455–57.

188. *Id.* at 458–59. The appellate court also reduced the CDWs' duration from 30 days to 10 days, citing Fourth Amendment concerns with respect to allowing repeated privacy intrusions only on one showing of probable cause. *Id.* at 464–65.

189. Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994).

190. *Facebook*, 471 N.J. Super. at 452–53.

191. *Id.*

192. *Id.*

193. *Id.*

194. *Id.* at 441.

195. *Id.* at 440–41.

196. *Id.*

electronic communications through their "real-time" access to the duplicate accounts.[197]

Ironically, the New Jersey Appellate Division suggested that its *Facebook* decision was an example of how the law is evolving in response to changing technology,[198] but it arguably exemplifies the opposite. For example, consider how both sides made sound and compelling arguments.[199] Concerning interception, New Jersey was correct that the great weight of federal precedent favors requiring acquisition contemporaneous to transit.[200] Even the Third Circuit, where New Jersey sits, requires contemporaneous acquisition.[201] However, Facebook's argument was compelling, too, given how surveillance of prospective electronic communications strongly resembles traditional wiretapping and the blurred line between when electronic communications are in storage or transit.[202] The appellate court nevertheless failed to give much weight to Facebook's argument and the concerns arising in this new context of prospective electronic communications and, more generally, the realities of modern electronic communications.[203] Ultimately, the appellate court's attempt to coherently apply the ECPA when faced with both compelling arguments only helps illustrate the ECPA's growing datedness and inadequacy.

Moreover, the nature of the law enforcement practice in *Facebook* supports an argument that prospective electronic communications ought to have more, if not the same, privacy protections as traditional wiretapping.[204] Ongoing surveillance of communications that have not yet happened resembles the type of privacy threat that courts have firmly acknowledged with wiretapping.[205] For instance, *Berger* established requirements later codified in the Wiretap Act, like minimizing the duration of a wiretap, to provide Fourth Amendment safeguards beyond probable cause because the court recognized how harmful collecting large swaths of communications

197. *Id.*

198. Rob Nussbaum, *A Communication Data Warrant or Wiretap Order – Which is needed for Law Enforcement to Obtain ESI from Facebook?*, TRENDING L. BLOG (Apr. 18, 2022), https://trendinglawblog.com/2022/04/18/a-communication-data-warrant-or-wiretap-order-which-is-needed-for-law-enforcement-to-obtain-esi-from-facebook/.

199. Brief of New Jersey State Bar Association (NJSBA) as Amicus Curiae Supporting Movant at 14, Facebook, Inc. v. State of New Jersey, *rev'd*, 471 N.J. Super. 430 (2022) (No. 087054), https://tcms.njsba.com/personifyebusiness/Portals/0/Amicus%20Cases/NJSBA%20Amicus%20Brief%20-%20Facebook%20v%20NJ%20-%20Docket%20087054.pdf. [hereinafter NJSBA Amicus Brief]

200. *Id.*

201. Fraser v. Nationwide Mut. Ins., 352 F.3d 107, 114 (3rd Cir. 2004) (explaining that they adopt the reasoning of their sister circuits in holding that there has been no "intercept" under the Wiretap Act).

202. NJSBA Amicus Brief, *supra* note 199, at 14.

203. Facebook Inc. v. State, 471 N.J. Super. 430, 458–59 (Super. Ct. App. Div. 2022), *rev'd*, 254 N.J. 329 (2023).

204. EPIC Amicus Brief, *supra* note 13, at 8–9.

205. *Id.*

could be to one's privacy.[206] Justice Douglas' concurrence in *Berger* condemns wiretapping as "a dragnet, sweeping in all conversations within its scope – without regard to the participants or the nature of the conversations. It intrudes upon the privacy of those not even suspected of crime and intercepts the most intimate of conversations."[207] Despite not involving traditional wiretapping, it is easy to imagine how the law enforcement practice in *Facebook* equally presents privacy threats that implicate people irrelevant to the investigation who nevertheless communicate with the subject. Without additional safeguards for prospective electronic communications, law enforcement could easily run the Fourth Amendment afoul.[208]

To make matters more alarming, law enforcement could obtain the same level of information as they would through unfettered interception of communications via a traditional wiretap by engaging in the law enforcement practice in *Facebook*.[209] Again, no safeguards are in place to minimize the acquisition scope or limit potentially implicating persons unrelated to the investigation.[210] Law enforcement is also free to collect prospective electronic communications in a wider range of circumstances because there are no limitations on the type of crimes where such practice is permissible.[211] Further, the appellate court's decision to afford lesser privacy protections to prospective electronic communications and allow for the extended acquisition of such upon only one showing of probable cause rests on the shaky distinction between communications that are in storage and transit.

The fact that electronic communications are capable of being simultaneously in storage and transit[212] obscures the Storage/Transit Dichotomy, insinuating its increased inappropriateness today.[213] As explained above, "packets" of data comprising the electronic communication are often stored along intermediate routers until they reach their intended recipients.[214] This structure is inherent to communication via email (as was the case in *Councilman*) and messaging apps like Facebook Messenger—the

206. Berger v. New York, 388 U.S. 41, 55 (1967).

207. *Id.* at 65.

208. The fear that might overcome someone if they fear or suspect law enforcement is surveilling their electronic communications could also lead to a chilling effect, inhibiting free speech. This is more so the case with prospective communications than stored communications because people maintain control of their actions. Thus, prospective communications ought to have more privacy protections. NJSBA Amicus Brief, *supra* note 19, at 10.

209. NJSBA Amicus Brief, *supra* note 199, at 15–16.

210. *Id.*

211. *Id.*

212. EPIC Amicus Brief, *supra* note 13, at 17; Ovide, *supra* note 149; Wang, *supra* note 148, at 1945–46.

213. Roundy, *supra* note 3, at 426.

214. EPIC Amicus Brief, *supra* note 13, at 17; Ovide, *supra* note 149; Wang, *supra* note 148, at 1945–46.

most popular messaging app in the United States.[215] In *Facebook*, Facebook stated that its servers did not have the technological capacity to provide perfectly contemporaneous access to the prospective communications via the duplicate accounts maintained by law enforcement.[216] Thus, even if law enforcement had sought to acquire electronic communications contemporaneously, the likely result would be the acquisition of stored data still potentially in transit due to technological necessity.[217] The appellate court's ease in categorizing these communications as in storage fails to acknowledge this critical point.

The appellate court's decision becomes increasingly concerning when one imagines how this practice might evolve to closer resemble traditional wiretapping. For instance, consider the logic of the appellate court: law enforcement was not engaged in interception because they requested disclosure of prospective electronic communications stored on Facebook's servers in fifteen-minute intervals.[218] As *amici curiae* point out, "By this logic, the police would not need a wiretap order to demand Facebook to send them users' messages every 15 milliseconds because that is not interception."[219] Even on a near-contemporaneous basis, the law enforcement practice would not trigger the Wiretap Act's heightened protections because of the effect the rigidity of the Storage/Transit Dichotomy has on the appellate court's analysis, as well as the Fifth and Ninth Circuits' analyses. Thus, the appellate court's decision, underscores the "existential oddity" described by the *Councilman* court when rejecting the Storage/Transit Dichotomy—the idea that electronic communications do not briefly cease to be electronic communications and then suddenly become electronic communications again.[220]

Lastly, any jurisdiction that might mirror the appellate court's reasoning in permitting this law enforcement practice would effectively render wiretapping futile and potentially open the floodgates for future abuse.[221] Specifically, law enforcement could obtain the same level of information as they would get through a wiretap without ever needing to apply for a wiretap warrant by simply seeking out prospective electronic communications instead.[222] Any such jurisdiction would effectively provide law enforcement with the comfort that comes with an understanding that courts will likely find that most, if not all, of those communications are in storage and incapable of

215. Beveridge, *supra* note 154; SPECTRM, *supra* note 148.

216. Facebook, Inc. v. State, 471 N.J. Super. 430, 440–41 (Super. Ct. App. Div. 2022), rev'd, 254 N.J. 329 (2023).

217. *See id.*

218. *Amicus Briefs: Facebook v. New Jersey*, ELEC. PRIV. INFO. CTR., https://epic.org/documents/facebook-v-new-jersey/ (last visited May 10, 2023).

219. *Id.*

220. United States v. Councilman, 418 F.3d 67, 78 (1st Cir. 2005).

221. NJSBA Amicus Brief, *supra* note 199, at 15–16.

222. *Id.*

interception under the Wiretap Act. Instead, the less rigorous protections that the SCA affords stored communications will likely govern any issues involving prospective electronic communications. The fact that New Jersey is the first state to address such a practice emphasizes the need to modify the ECPA to protect against the dangers posed by other jurisdictions possibly agreeing with the appellate court's reasoning—*Facebook* may only be the beginning.[223]

### D. ANALYSIS OF THE NEW JERSEY SUPREME COURT'S DECISION AND HOW IT SUPPORTS THAT CHANGE IS NEEDED TO THE ECPA'S CURRENT FRAMEWORK

Although this Note was initially drafted before the New Jersey Supreme Court barred the law enforcement practice at issue by reversing the Appellate Division's holding, their decision supports this Note's argument that change is needed to the ECPA current framework.[224] In its opinion, the New Jersey Supreme Court held that near contemporaneous acquisition of electronic communications is the "functional equivalent" of wiretapping, warranting heightened protections.[225] Much like the Appellate Division, the court came to its holding after analyzing the language and structure of the ECPA and NJWESCA, plus key federal precedent addressing the acquisition contemporaneous with transit requirement and the Storage/Transit Dichotomy.

First, the court held that the language and structure of the ECPA and NJWESCA do not support authorizing access to future, prospective electronic communications via a CDW rather than a wiretap warrant.[226] Regarding the ECPA, the court agreed with Facebook that the SCA was not designed to apply to future events or communications.[227] As Facebook pointed out, the amended Wiretap Act (Title I of the ECPA) contains forward-looking provisions that apply to and limit prospective surveillance activities, such as interception of future conversations, but the SCA (Title II of the ECPA) does not.[228] The court also noted that other caselaw supports their argument the SCA covers past rather than future communications.[229] Since the NJWESCA reflects the ECPA's structure, only the equivalent wiretap sections of the NJWESCA contain forward-looking provisions too.[230] Thus, it did not make sense to apply the SCA—or the NJWESCA's

223. *See generally* ELEC. PRIV. INFO. CTR., *supra* note 218.
224. Facebook, Inc. v. State, 254 N.J. 329, 341 (2023).
225. *Id.*
226. *Id.* at 357.
227. *Id.* at 355–57.
228. *Id.*
229. *Id.*
230. *Id.*

equivalent sections—when law enforcement seeks to acquire prospective electronic communications.

Second, the court held that the NJWESCA's equivalent Wiretap Act sections apply to near real-time acquisition of prospective electronic communications.[231] The court distinguished the facts at hand from the facts in federal cases that adopted the acquisition contemporaneous with transit requirement like *Turk*, *Steve Jackson Games*, and *Konop.*[232] Namely, the court pointed out that the communications acquired in those cases were historical communications rather than communications that were in transit or nearly contemporaneous to transit.[233] To the court, requiring contemporaneity would be inappropriate:

> Imagine instead an attempt by law enforcement to gain broad access to future electronic communications, including private messages, within 15 minutes, the earliest possible moment they are available, for 30 days – the very situation this case presents. A strict contemporaneity rule adopted before the advent of the Internet would not be a good fit to address that or other situations technology presents today. Nor would such a rule be consistent with the underlying purpose of the wiretap statutes – to protect individual privacy.[234]

The court rejected the logic present in the New Jersey Appellate Division's opinion, which discounted the law enforcement practice's close resemblance to traditional wiretapping.[235] Further, the court warned of the danger posed by this type of reasoning, given that technological advancements may continue to shorten the required time that data must be stored before disclosure to the point where such a law enforcement practice would resemble traditional wiretapping even more.[236]

Overall, *Facebook* is a clear example of new privacy threats in modern contexts. The New Jersey Supreme Court itself emphasized that the privacy interests at stake and the level of intrusion are substantial when presented with facts like those in *Facebook.*[237] Without some degree of change, new threats like the law enforcement practice in *Facebook* will continue to test the strength of the ECPA's current framework. Given the extent to which technology has already advanced since the ECPA's enactment and last amendment twenty-two years ago, the ECPA's current framework may very soon prove to be wholly inadequate in carrying out its initial purpose to ensure privacy protections.

231. *Id.* at 361.
232. *Id.* at 360.
233. *Id.*
234. *Id.*
235. *Id.* at 361.
236. *Id.*
237. *Id.*

### E. JUDICIAL SOLUTION: ADOPTING A BROAD CONTEMPORANEITY STANDARD

So, what can courts do when presented with situations like *Facebook* that necessitate squaring "intercept" under the Wiretap Act with prospective electronic communications (and electronic communications more generally)? Michael Roundy suggests rejecting the Storage/Transit Dichotomy like the First Circuit in *Councilman*.[238] While Roundy concedes that requiring acquisition contemporaneous to transit is the most appropriate standard to apply when assessing "intercept," Roundy advocates for a broader contemporaneity standard.[239] A broader contemporaneity standard would evaluate contemporaneity holistically and on a case-by-case basis instead of evaluating it based on the answer to whether acquisition occurred contemporaneous to transit.[240]

Roundy lists three factors for a broader evaluation of contemporaneous acquisition and interception of electronic communications: (1) whether the acquisition of the electronic communication is from electronic storage, (2) whether the intended recipient received the electronic communication before the acquisition, and (3) whether the acquisition of the electronic communication occurred simultaneous to the transmission.[241] The first factor weighs against a finding of interception if the acquisition is from electronic storage.[242] The second and third factors acknowledge the virtually instantaneous nature of modern electronic communications.[243] The second factor weighs in favor of a finding of interception if the acquisition occurred before the electronic communication reached its intended recipient.[244] An example of this second factor might be rerouting competitor emails to a separate mailbox like in *Councilman*.[245] Lastly, the third factor weighs in favor of a finding of interception if the acquisition occurred simultaneous to transmission, regardless of whether the contents were technically from storage.[246] Nevertheless, Roundy emphasizes that the premise behind adopting a broad contemporaneity standard Is that no single factor should be dispositive.[247]

The utility of adopting a broad contemporaneity standard is discernible when applying it to the facts of *Facebook*. In *Facebook*, law enforcement technically acquired the electronic communications from storage on the

238. Roundy, *supra* note 3, at 433.
239. *Id.*
240. *Id.* at 438.
241. *Id.*
242. *Id.* at 436.
243. *Id.*
244. *Id.* at 437.
245. The court alluded to this despite not providing a direct answer to the contemporaneity standard question. United States v. Councilman, 418 F.3d 67, 80 (1st Cir. 2005).
246. Roundy, *supra* note 3, at 437.
247. *Id.*

duplicate accounts, which initially weighs against finding "interception" (as the appellate court found).[248] Under a broad contemporaneity standard, however, this factor is not dispositive. Contrary to the appellate court's holding, the third factor would support a finding of "interception" because the electronic communications were placed on the duplicate accounts virtually at the same time the communications occurred, notwithstanding the fifteen-minute delay in disclosure.[249] If this were the analysis applied, it is likely that the appellate court's holding would have been that the law enforcement's practice constituted interception of the prospective electronic communications sought, necessitating a wiretap warrant and implying that the SCA would not apply.

Overall, a broad contemporaneity standard is appealing because it addresses the ECPA's inadequacy in the context of modern electronic communications. Notably, the standard does not completely dispose of the Storage/Transit Dichotomy. Rather, it eases the Storage/Transit Dichotomy's rigidness to account for the reality of electronic communications often in storage and transit simultaneously by rendering such classifications non-dispositive.[250] Moreover, the standard remains consistent with the Wiretap Act's central concern, as iterated by the Fifth Circuit in *Turk*, which established requiring contemporaneous acquisition for interception.[251] The Fifth Circuit noted that the Wiretap Act is concerned with surveillance at the time of the communication, and that is precisely what Roundy's third factor helps bring into the fray.[252]

### F. LEGISLATIVE SOLUTION: REVISING THE ECPA'S "INTERCEPT" AND "ELECTRONIC STORAGE" DEFINITIONS

An alternative or complementary solution is for Congress to codify the broader contemporaneity standard Roundy supports. Theodore McDonough suggests that a starting point for legislation could be the E-Mail Privacy Act of 2005, introduced by Senator Leahy (D-VT) and Senator Sununu (R-MA) following the *Councilman* decision.[253] The E-Mail Privacy Act sought to amend the definition of "intercept" to include the aural or other acquisition of the contents of any wire, electronic, or oral communication contemporaneous with transit *or on an ongoing basis during transit*, through the use of any electronic, mechanical, or other device or process, *notwithstanding that the communication may simultaneously be in*

248. Facebook, Inc v. State, N.J. Super. 430, 438 (Super. Ct. App. Div. 2022), *rev'd*, 254 N.J. 329 (2023).

249. *Id.* at 438–39.

250. Roundy, *supra* note 3, at 437.

251. *Id.* at 417; United States v. Turk, 526 F.2d 654, 658 (5th Cir. 1976).

252. *Turk*, 526 F.2d at 658–59 (5th Cir. 1976).

253. McDonough, *supra* note 2, at 1072; E-Mail Privacy Act, S. 936, 109th Cong. (2005).

*storage*.[254] McDonough also suggests amending the definition of "electronic storage" to include any storage of a wire or electronic communication after transmission and by an electronic communication service for backup protection of such communication and *exclude temporary storage incidental to electronic communication transmissions employing electronic communication system*.[255]

Revising the definitions of "intercept" and "electronic storage" this way would have the same effect on *Facebook*'s outcome as a reexamination of *Facebook* under a broad contemporaneity standard. Prospective electronic communications would be excluded under the new definition of "electronic storage," consistent with *Councilman*. Moreover, the law enforcement practice would fall under the section of the new definition of "intercept" that addresses an ongoing basis during transit, given that the stored data is inherent to transmission and law enforcement had "real-time" access through the users' duplicate account. Considering the contrasting approaches already developed across the federal circuits, a legislative solution might be more viable than relying on courts to universally adopt a broad contemporaneity standard.[256]

### G. LEGISLATIVE SOLUTION: IMPLEMENTING SAFEGUARDS FOR PROSPECTIVE ELECTRONIC COMMUNICATIONS

An alternative solution to adopting a broad contemporaneity standard is adopting a new statute or an amendment to the ECPA that creates explicit safeguards against law enforcement seeking prospective electronic communications to circumvent the Wiretap Act. In their amicus brief, the New Jersey State Bar Association proposed implementing the following three requirements for law enforcement to satisfy when they seek a CDW to acquire prospective electronic communications:

> (i) There is evidence that normal investigative procedures have failed or less intrusive means cannot be employed; (ii) minimization efforts are utilized, including, perhaps, a monitor who will receive the communications covered by the warrant—before providing them to investigators on the case—to ensure that unrelated or privileged communications, or communications about other crimes, are sealed and not provided to other investigators on the case without judicial approval; and (iii) the timeframe for which the warrant is offered is limited to a reasonable amount of time necessary to collect the information.[257]

254. E-Mail Privacy Act, S. 936, 109th Cong. (2005).
255. McDonough, *supra* note 2, at 1073–74.
256. Campbell, *supra* note 19, at 545.
257. NJSBA Amicus Brief, *supra* note 199, at 16–17.

Congress could implement similar requirements at the federal level with respect to standard search warrants.

While this legislative solution does not address the existing challenges the Storage/Transit Dichotomy and the requirement of contemporaneous acquisition, it at least acknowledges that the facts in *Facebook* present a new and substantial privacy threat. *Facebook* necessitates granting at least some, if not the same, heightened privacy protections against wiretapping because of the alarming similarities between seeking prospective electronic communications and traditional wiretapping, as discussed above. Ultimately, establishing similar requirements to the *Berger* requirements codified in the Wiretap Act could help maintain adherence to the Fourth Amendment's privacy guarantees. Not applying all the *Berger* requirements would help balance the utility of electronic surveillance to law enforcement and their legitimate needs, as recognized by the original Wiretap Act, against the need to protect against collecting vast amounts of communications and implicating the privacy of those who are irrelevant to any ongoing investigation.[258]

## VI. CONCLUSION

The ECPA's infamous lack of clarity has led to different interpretations and applications across courts, many of which fail to recognize the realities of modern electronic communication. As a result, some electronic communications receive lesser levels of privacy protection and are left more vulnerable to intrusion. The law enforcement practice in *Facebook* is one example of an emerging privacy threat today, but more importantly, the case itself highlights the ECPA's growing inadequacy in protecting against new threats. Without some change to the ECPA, new privacy threats will continue to chip away at the ECPA's current framework until it proves wholly inadequate. *Facebook* should serve as a wake-up call for the judiciary or Congress to take some action to protect the integrity of the ECPA and the Fourth Amendment.

258. Roundy, *supra* note 3, at 411.

***