Boston College Law Review

Volume 59
Issue 9 *Annual Survey of Federal En Banc and Other Significant Cases*

Article 22

4-26-2018

Unfaithful but Not Without Privacy Protections: The Seventh Circuit Addresses When Courts Should Consider an E-Mail Interception Unlawful in *Epstein v. Epstein*

Joseph Noreña
Boston College Law School, joseph.norena@bc.edu

UNFAITHFUL BUT NOT WITHOUT PRIVACY PROTECTIONS: THE SEVENTH CIRCUIT ADDRESSES WHEN COURTS SHOULD CONSIDER AN E-MAIL INTERCEPTION UNLAWFUL IN *EPSTEIN v. EPSTEIN*

Abstract: On December 14, 2016, the United States Court of Appeals for the Seventh Circuit, in *Epstein v. Epstein*, held that contemporaneousness is not a determinative factor at the pleadings stage of a claim for the unlawful interception of electronic communications under the Federal Wiretap Act ("FWA"). In so doing, the Seventh Circuit partly departed from the way in which other Federal Circuit Courts had previously considered the statutory language of the FWA, specifically the definitions of "electronic communication" and "intercept" under 18 U.S.C. § 2510(4), (12). This Comment argues that the Seventh Circuit's holding that contemporaneousness is not a determinative factor at the pleadings stage stands more in line with the congressional intent of the Electronic Communications Privacy Act of 1986 ("ECPA"), which aims to provide privacy protections to electronic communications.

INTRODUCTION

When Congress passed the Electronic Communications Privacy Act of 1986 ("ECPA"), it amended the Federal Wiretap Act ("FWA") in order to provide privacy protections to electronic communications.[1] One of the driving forces behind the ECPA was to provide greater privacy protections to e-mail and other computer-to-computer communications, which had rapidly become popular forms of electronic communication.[2] Title I of the ECPA allows a

[1] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, 1848–50 [hereinafter ECPA] (amending various sections of Title 18 the United States Code—which read together are considered the FWA—to cover the interception of electronic communications); *see also* S. REP. NO. 99-541, at 3–4 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3556–58 (clarifying that the ECPA added the protection of electronic communications because Congress sought to protect the privacy of electronic communications). Electronic communication is the transfer of sensory materials by a wire or electronic system that has an effect on interstate or foreign commerce, such as the transfer of e-mail. 18 U.S.C. § 2510(12) (2012); *see also* Tatsuya Akamine, Note, *Proposal for a Fair Statutory Interpretation: E-Mail Stored in a Service Provider Computer Is Subject to an Interception Under the Federal Wiretap Act*, 7 J.L. & POL'Y 519, 521–22 (1999) (arguing that the ECPA, enacted to extend coverage of the FWA to e-mails, is the most important piece of legislation that protects e-mail privacy interests).

[2] S. REP. NO. 99-541, at 4 (citing a letter written in 1984 from Senator Patrick Leahy to the Department of Justice in which Senator Leahy inquired as to whether current federal law protected e-mail and computer-to-computer communications); H.R. REP. NO. 99-647, at 21–22, 34 (1986) (elaborating on the expansion of the ECPA to cover electronic communications); *see also* Ariana R. Levin-

plaintiff or the U.S. Attorney General to sue for injunctive relief and civil damages if a plaintiff can show that a defendant unlawfully intercepted their wire, oral, or electronic communications.[3] A plaintiff must establish that an interception, defined as the "aural or other acquisition," of wire, oral, or electronic communication by some type of device, has occurred.[4] Consistent with Congress's goal, the FWA, as amended by the ECPA, is used to protect the privacy of wire, oral, and electronic communications.[5] In 2015, Barry Epstein asked the U.S. District Court for the Northern District of Illinois, and later the U.S. Court of Appeals for the Seventh Circuit, to assess whether he could use the ECPA as a "tactical weapon" in a divorce to effectively quash his spouse's surreptitiously obtained e-mail evidence of his extramarital affairs.[6]

In *Epstein v. Epstein*, in 2016, the U.S. District Court for the Northern District of Illinois dismissed Barry Epstein's ECPA claims against his wife, Paula Epstein, and her lawyer, Jay Frank.[7] The claims arose out of Paula's alleged unlawful interception of Barry's e-mails and Frank's alleged unlawful disclosure of those e-mails when Frank disclosed them during divorce proceedings between Barry and Paula.[8] The District Court granted Paula's motion to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6) because Barry

---

son, *Toward a Cohesive Interpretation of the Electronic Communications Privacy Act for the Electronic Monitoring of Employees*, 114 W. VA. L. REV. 461, 480 (2012) (citing S. REP. NO. 99-541 and H.R. REP. NO. 99-647 to explain the legislative intent of the ECPA).

[3] *See* 18 U.S.C. § 2520 (authorizing injunctive relief and the recovery of civil damages for any plaintiff whose wire, oral, or electronic communication is intercepted in violation of the ECPA); *see also id.* § 2521 (authorizing the Attorney General to bring a civil action in which a court may grant injunctive relief against a person engaging in or about to engage in activity illegal under the ECPA). Wire communication is the transfer of any communication that is able to be heard with the help of a wire, cable, or other like connection. *Id.* § 2510(1). Oral communication is any communication uttered by a person with the expectation of privacy. *Id.* § 2510(2).

[4] *See id.* § 2510(4) (defining intercept under the FWA); *id.* § 2511(1)(a) (explaining that Title 18 of the United States Code prohibits the intentional interception of wire, oral, or electronic communications).

[5] *See, e.g.*, Luis v. Zang, 833 F.3d 619, 629–30 (6th Cir. 2016) (reversing a district court's dismissal of an ECPA claim because the claim sought to protect private e-mail and other Internet communications, both classified as electronic communication); United States v. Smith, 155 F.3d 1051, 1059 (9th Cir. 1998) (holding that a third party unlawfully intercepted a voicemail on a private phone, classified as a wire communication); *see also* Michael D. Roundy, Note, *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, 415 (2006) (explaining that Congress passed the ECPA in part to provide the same privacy protections to electronic communications that were already in place for wire and oral communications).

[6] Epstein v. Epstein, 843 F.3d 1147, 1148 (7th Cir. 2016); *see* Epstein v. Epstein, No. 14 C 8431, 2015 WL 1840650, at *2 (N.D. Ill. Apr. 20, 2015) (explaining that Barry Epstein's amended complaint alleged ECPA violations against his wife, Paula Epstein, for unlawfully intercepting his e-mails).

[7] *Epstein*, 843 F.3d at 1148–49.

[8] *Id.* at 1149.

had failed to allege that Paula intercepted his e-mails contemporaneously with transmission of those e-mails.[9] The District Court reached this conclusion based on the decisions of several Federal Circuits, which have held that contemporaneousness is a determinative factor in considering whether an interception is unlawful under the ECPA.[10] Federal Circuit courts have defined a contemporaneous interception of electronic communications as an interception that occurs at the same time that electronic communication is being transmitted.[11] Nevertheless, the Seventh Circuit reversed the dismissal.[12] Even if contemporaneousness were a determinative factor later on at trial, contemporaneousness was not a determinative factor at the pleadings stage because of the ambiguity surrounding when exactly an e-mail is in transit.[13]

This Comment argues that the Seventh Circuit correctly held in *Epstein* that contemporaneousness is not a determinative factor in considering whether a plaintiff has made a plausible claim for an unlawful interception under the

---

[9] *Id.* (explaining the district court's reasoning and defining a contemporaneous interception as obtaining an electronic communication in transit); *see also* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003) (requiring that an interception actionable under the ECPA must occur contemporaneously, meaning intercepted at the initial transmission of the e-mail).

[10] *See Epstein*, 2015 WL 1840650, at *2–3 (citing to four different Circuit Courts of Appeal to support its proposition that a defendant must intercept e-mails contemporaneously in order to violate the ECPA). The Fifth Circuit was the first appellate court to decide the specific issue in *Epstein*. *See* Steve Jackson Games, Inc. v. Secret Serv., 36 F.3d 457, 458 (5th Cir. 1994) (affirming a district court's final judgment that the Secret Service's seizure of a computer hard disk drive that held private e-mails was not an unlawful interception under the ECPA because those e-mails were stored and not intercepted contemporaneously).

[11] *See Fraser*, 352 F.3d at 113 (defining a contemporaneous interception of electronic communications as an interception that occurs "at the initial time of transmission"); United States v. Steiger, 318 F.3d 1039, 1150 (11th Cir. 2003) (defining a contemporaneous interception of electronic communications as an interception that occurs while the electronic communication is "in flight," or in the course of being transmitted).

[12] *Epstein*, 843 F.3d at 1150–51.

[13] *See id.* at 1150 (holding that the Seventh Circuit would not take a position on whether interceptions of electronic communication must occur contemporaneously, but even if interceptions must occur contemporaneously, Barry had stated a valid claim against Paula); *see also id.* at 1149 (defining a contemporaneous interception of electronic communications as an interception that occurs "during transmission" instead of after the electronic communication has reached its destination, or an interception while the electronic communication is "in transit"). "Determinative factor" in the context of this Comment means a factor that ultimately determines whether a court will dismiss an action for failure to state a claim. *See* Arthur R. Miller, *From* Conley *to* Twombly *to* Iqbal*: A Double Play on the Federal Rules of Civil Procedure*, 60 DUKE L.J. 1, 33 (2010) (arguing that because *Ashcroft v. Iqbal* held that a judge must consider subjective factors when deciding whether to dismiss a case for failure to state a claim, judicial discretion had now become the "determinative factor" in deciding whether a plaintiff can survive a motion to dismiss). Consequently, even though the Seventh Circuit did not use the phrase determinative factor, the court effectively held that contemporaneousness was not a determinative factor to state a plausible claim for the interception of electronic communication under the FWA as amended by the ECPA. *See Epstein*, 843 F.3d at 1150–51 (holding that even if the FWA only covers contemporaneous interceptions, Barry stated a plausible claim because the allegedly intercepted e-mails may have been intercepted while in transmission).

ECPA, thus facilitating the ability of plaintiffs to make ECPA claims.[14] The Seventh Circuit's interpretation of contemporaneousness at the pleadings stage is more in line with the Congressional intent of the ECPA since Congress intended to afford greater privacy protections to e-mails.[15] Part I of this Comment examines the emergence of contemporaneousness as a determinative factor in considering unlawful interception claims as well as the Seventh Circuit's interpretation of the husband's claim in *Epstein*.[16] Part II discusses the different interpretations of contemporaneousness as a determinative factor in a claim for the unlawful interception of electronic communications under the ECPA.[17] Finally, Part III argues that the Seventh Circuit's view that contemporaneousness is not a determinative factor at the pleadings stage is more in line with the Congressional intent of the ECPA because it helps plaintiffs protect the privacy of their e-mails.[18]

I. The History of the ECPA and Contemporaneousness as a Determinative Factor in Unlawful Interception Claims

The ECPA was enacted in 1986 to expand protections afforded by the Omnibus Crime Control and Safe Streets Act of 1968 ("OCCSSA").[19] The OCCSSA provided privacy protections for wire and oral communications, most notably by allowing an individual to bring a private cause of action for the unlawful interception of their wire and oral communications.[20] As an expansion to the OCCSSA's protections against the interception of wire and oral

---

[14] *See infra* notes 95–110 and accompanying text.

[15] *See infra* notes 95–110 and accompanying text.

[16] *See infra* notes 19–54 and accompanying text.

[17] *See infra* notes 55–94 and accompanying text.

[18] *See infra* notes 95–110 and accompanying text.

[19] S. Rep. No. 99-541, at 1. The ECPA amended several sections of Chapter 119 of Title 18 of the United States Code, which contains the laws that control the interception of wire, oral, and electronic communications. 18 U.S.C. §§ 2510–2522 (2012). Judges also refer to 18 U.S.C. §§ 2510–2522—the codification of the ECPA, the laws which the ECPA amended, and successive amendments after the ECPA—as the Federal Wiretap Act or the Wiretap Act. *See, e.g.*, *Steve Jackson Games*, 36 F.3d at 458 (referring to the FWA). The ECPA itself has been amended several times since its passage in 1986. *See* Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. Rev. 609, 626 (2007) (explaining how the ECPA has been amended significantly since it was passed in 1986). Most notably, in 2001, the USA PATRIOT Act amended the ECPA. *Id.* Nevertheless, the USA PATRIOT Act did not affect the definitions of electronic communication or interception. *See* USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272, 290–91 (2001) (explaining precisely which definitions the USA PATRIOT Act would change); *see also* 18 U.S.C. § 2510 (containing the updated definitions).

[20] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, 213, 223 (establishing a cause of action for those individuals who have had their wire or oral communications unlawfully intercepted, without any mention of electronic communication). Oral communication was defined as any type of communication orally uttered by a person who has the expectation that their communication will not be intercepted. *Id.* at 212. Wire communication was defined as any communication made at least partly through transmission by wire, cable, or other similar connection. *Id.*

communications, Congress passed Title I of the ECPA to protect against the interception of electronic communications in transmission, such as e-mail.[21] The statute does not define precisely when that unlawful interception must occur.[22] Section A of this part examines how courts, primarily the U.S. Court of Appeals for the Fifth Circuit, have interpreted the contemporaneousness factor under the OCCSSA and later under the ECPA.[23] Section B of this part examines the facts and procedural history of *Epstein v. Epstein*, in which the Seventh Circuit held that contemporaneousness is a not determinative factor in unlawful interception claims under the ECPA.[24]

A. The Evolution of an Unlawful Interception and the Contemporaneousness Factor

Before the passage of the ECPA, the Fifth Circuit decided that an unlawful interception of oral communication under the OCCSSA must occur contemporaneously with the utterance of that oral communication.[25] In *United States v. Turk*, the defendant involved in narcotics investigations alleged that Miami police officers had unlawfully intercepted his oral communication when

---

[21] *See* ECPA, 100 Stat. at 1848–50 (amending the OCCSA to cover the interception of electronic communications); *see also* 18 U.S.C. § 2510(12) (defining electronic communication as any the transfer of sensory materials by a wire or electronic system that has an effect on interstate or foreign commerce). When electronic communications are intercepted in transmission, the interception occurs at the time when a wire or electronic system is transferring sensory materials. ECPA, 100 Stat. at 1848–49; *see* S. REP. NO. 99-541, at 4, 8 (recognizing that the ECPA aims to protect against the interception of e-mail and defining e-mail as private communication typed into a computer system and then transferred via public and private telephone lines); *see also* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1557, 1561 (2004) (arguing that privacy concerns related to personal e-mails drove the passage of the ECPA). Title II of the ECPA, otherwise known as the Stored Communications Act, protects against the unlawful acquisition of stored electronic communications. ECPA, 100 Stat. at 1860 (making it illegal to acquire stored electronic communication). Although beyond the scope of this Comment, the Stored Communications Act also plays a major role in policing government surveillance of electronic communications. *See* Alexander Porter, Note, *"Time Works Changes": Modernizing Fourth Amendment Law to Protect Cell Site Location Information*, 57 B.C. L. REV. 1781, 1792 (2016) (explaining how Congress intended for the Stored Communications Act to allow judicial oversight of the government surveillance of cell phone communications).

[22] *See* 18 U.S.C. § 2510(4) (defining intercept without explaining precisely when an interception must occur in order to constitute an unlawful interception); *see also* ECPA, 100 Stat. at 1848–49 (amending 18 U.S.C. § 2510 to include the phrase electronic communication and its accompanying definition).

[23] *See infra* notes 25–44 and accompanying text.

[24] *See infra* notes 45–54 and accompanying text.

[25] United States v. Turk, 526 F.2d 654, 659 (5th Cir. 1976). In *United States v. Turk*, the court defined a contemporaneous interception as an interception of communication that occurs at the actual time that the communication is happening. *Id.* at 658. In fact, the Fifth Circuit was the only court to address the contemporaneous factor before the passage of the ECPA. *See* Levinson, *supra* note 2, at 493 n.180 (explaining that *United States v. Turk* was the only pre-ECPA case that required interceptions to occur contemporaneously).

they seized the cassette tapes of his recorded phone conversations without a warrant.[26] The Fifth Circuit concluded that the police officers' seizure of the cassette tapes was not unlawful because their conduct did not fall under the OCCSSA definition of interception, which is defined as "aural acquisition."[27] Congress had previously explained that an aural acquisition means the action of physically hearing some wire or oral communication through some kind of listening device.[28]

The defendant argued that the actions of the police officers constituted an interception because they listened to the seized cassette tapes.[29] He argued that listening to the cassette tapes constituted an interception because a new aural acquisition occurs every time someone listens to a prior recording of oral communication.[30] The Fifth Circuit disagreed, interpreting the plain language of the statute to reflect Congress's intent that an interception of oral communication must occur at the time that communication is happening.[31] In other words, the interception must occur contemporaneously with the utterance of that communication.[32] If contemporaneousness was not a determinative factor for an unlawful interception, then the OCCSSA would cover every type of surveillance, and the Fifth Circuit held that Congress did not intend such broad coverage.[33]

Ten years after the Fifth Circuit's decision in *Turk*, Congress passed the ECPA in 1986, and in doing so it added protections to electronic communications but did not specify whether an unlawful interception of electronic com-

---

[26] *Turk*, 526 F.2d at 657. The police officers obtained the cassette tapes by stopping a car after receiving a tip that the passengers in that car were illegally possessing cocaine and firearms. *Id.* at 656. Among other objects, the police officers found in the car cassette tapes containing recorded telephone conversations. *Id.* The police officers took the cassette tapes back to the police station, listened to the tapes (all without a warrant or the car owner's permission), and eventually found out that one of the tapes implicated the defendant in narcotics violations. *Id.* at 656–57. The defendant wanted to classify the actions of the police officers as an unlawful interception in an attempt to exclude the illegally obtained evidence from his trial. *Id.* at 657.

[27] *Id.* at 659 (quoting S. REP. NO. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2178).

[28] *See id.* at 657 (explaining that the statutory language "aural acquisition" means the action of physically hearing some wire or oral communication through some kind of device); *see also* 18 U.S.C § 2510(18) (defining "aural transfer" as a transfer of the human voice between the original utterance of that voice and the hearing of that voice by someone else).

[29] *Turk*, 526 F.2d at 658.

[30] *Id.*

[31] *Id.* at 659 (quoting S. REP. NO. 90-1097) (ruling that the interception of wire and oral communication is unlawful but that other forms of surveillance are not unlawful); *see also id.* at 658 (reasoning that if Congress had intended for each new aural acquisition of a wire or oral communication to constitute a new interception, Congress would have written that into the statute).

[32] *See id.* at 658 & n.3 (concluding that, at the very least, an interception requires some type of involvement by the interceptor while the communication is happening).

[33] *See id.* at 658–59 (explaining that an interception of oral communications could not occur unless the interception happened at the utterance of that oral communication). In explaining the congressional intent behind passing the OCCSSA, the Fifth Circuit cited the OCCSSA's corresponding congressional report. *See generally* S. REP. NO. 90-1097 (stating explicitly that the OCCSSA does not cover all forms of surveillance).

munications had to occur contemporaneously with transmission of that communication.[34] As a result, several Federal Circuit Courts, including the Fifth Circuit, held that such an interception must occur at the same time the electronic communication is being transmitted.[35]

In 1994, in *Steve Jackson Games, Inc. v. Secret Service*, the Fifth Circuit was the first appellate court to decide that contemporaneousness is a determinative factor as to whether or not the interception of electronic communications is unlawful under the ECPA.[36] The court held that even though the Secret Service seized a computer hard disk drive that contained private e-mails, the Secret Service did not unlawfully intercept those e-mails under the ECPA.[37] Those e-mails were stored on a hard disk drive and therefore not intercepted at the time those e-mails were being transmitted.[38] The Fifth Circuit further explained that Congress maintained the FWA's definition of intercept—the acquisition of communication through some type of mechanical device—when it enacted the ECPA.[39]

The Fifth Circuit reasoned that Congress intended to distinguish electronic communications in storage from electronic communications in transit, because Congress defined electronic communication and electronic storage separately under the ECPA.[40] On the other hand, the definition of wire communica-

---

[34] *See also* Levinson, *supra* note 2, at 493 (pointing out that no congressional materials indicate that the legislators took notice of *Turk*). *See generally* ECPA, 100 Stat. 1848.

[35] *See, e.g.*, *Steve Jackson Games*, 36 F.3d at 462 (holding that Congress, when it wrote the ECPA, intended that an unlawful interception of electronic communication must occur at the same time the electronic communication is being transmitted). The Third, Sixth, Ninth, and the Eleventh Circuit have also held that such an interception must occur contemporaneously with transmission. *Luis*, 833 F.3d at 629; *Fraser*, 352 F.3d at 113; *Steiger*, 318 F.3d at 1048–49; Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002); *Smith*, 155 F.3d at 1059.

[36] *See Steve Jackson Games*, 36 F.3d at 462 (holding that an interception of electronic communication under the ECPA must occur contemporaneously with transmission of that electronic communication).

[37] *Id.* at 463.

[38] *Id.* Just as the interception of oral communication in *Turk* needed to occur contemporaneously with the utterance of oral communication, the interception of private e-mails in *Steve Jackson Games* needed to occur contemporaneously with transmission of those e-mails. *See id.* at 460–61 (affirming a district court's holding, which cited *Turk*, that the Secret Service did not intercept electronic communications because the interception did not occur contemporaneously with the transmission of those e-mails); *see also* Mulligan, *supra* note 21, at 1565 (citing *Turk* and *Steve Jackson Games* as support for the idea that the FWA—as amended by the ECPA—aims to regulate surveillance of Internet communications "in transit").

[39] *Steve Jackson Games*, 36 F.3d at 462 (citing to S. REP. NO. 99-541, at 13). Congress changed the phrase aural acquisition to "aural or other acquisition," signifying that the interpretation of aural acquisition as interpreted under *Turk* should remain the same under the ECPA. *Id.* at 461 (citing 18 U.S.C. § 2510(4) (1986);18 U.S.C. § 2510(4) (1968)).

[40] *See id.* at 461–62 (defining electronic communication and electronic storage by citing the ECPA amendments to the FWA); *see also* 18 U.S.C. § 2510(12), (17) (2012) (containing the codified definitions from the amendments); Mulligan, *supra* note 21, at 1565 (breaking down the ECPA as covering both electronic communications in transit and electronic communications in storage). Electronic communication is defined as the "transfer" of any signals, images, or data transmitted through some type of electronic device. 18 U.S.C. § 2510(12). On the other hand, electronic storage is defined

tion includes both wire communication in transit as well as any wire communication in storage.[41] Thus, the Fifth Circuit held that because Congress distinguished electronic communications in storage from electronic communications in transit, an unlawful interception of electronic communication had to occur contemporaneously with transmission.[42]

The decision in *Steven Jackson Games* and subsequent decisions from the various Circuit Courts of Appeals stand for the proposition that contemporaneousness is a determinative factor in establishing whether an e-mail has been intercepted in violation of the ECPA.[43] The Seventh Circuit partly departed from this practice when it held that contemporaneousness is not a determinative factor at the pleadings stage, and thus should not automatically prevent a complainant from successfully pleading a claim for the unlawful interception of electronic communications under the ECPA.[44]

B. The Seventh Circuit Addresses the Contemporaneousness Factor

In May of 2011, Paula Epstein filed for divorce in the Circuit Court of Cook County, Illinois, after accusing her husband, Barry Epstein, of serial infi-

---

as any type of "storage" of a wire or electronic communication that can be transmitted electronically. *Id.* § 2510(17). In *Steve Jackson Games*, the e-mails stored on a hard drive were a form of stored communications covered by Title II of the ECPA (the Stored Communications Act), and acquiring stored e-mail does not constitute a contemporaneous interception. 36 F.3d at 463. Plaintiffs prefer to bring an action for the interception of electronic communication as opposed to the seizure of stored electronic communication because statutory damages are at least ten times greater for interceptions of electronic communication. *See* 18 U.S.C. § 2520(c)(2)(B) (setting statutory damages for electronic communication interception violations at the greater of ten thousand dollars or one hundred dollars a day for each day of violation); *Id.* § 2707 (setting statutory damages for the seizure of stored electronic communication at a minimum of one thousand dollars and more than that if the actual damages are greater than one thousand dollars); *see also* Sarah Salter, *Storage and Privacy in the Cloud: Enduring Access to Ephemeral Messages*, 32 HASTINGS COMM. & ENT. L.J. 365, 378 (2010) (arguing that Congress places a higher value in protecting electronic communication in transit than electronic communication in storage).

[41] *See Steve Jackson Games*, 36 F.3d at 461 (citing 18 U.S.C. § 2510(1)). Wire communication is defined as any communication made at least partly through transmission by wire, cable, or other similar connection. 18 U.S.C. § 2510(1).

[42] *See Steve Jackson Games*, 36 F.3d at 461–62 (holding that electronic communication in storage cannot be intercepted because only electronic communication in transit can be intercepted such that it would violate the FWA); *see also* Roundy, *supra* note 5, at 418–20 (explaining how the *Steve Jackson Games* court created a distinction between electronic communication in storage and electronic communication in transit based on the statutory definitions of electronic storage, electronic communication, and wire communication).

[43] *See, e.g.*, *Fraser*, 352 F.3d at 113 (citing *Steve Jackson Games*, 36 F.3d at 461–62) (holding that the interception of an e-mail must occur contemporaneously to be unlawful under the ECPA); *Steiger*, 318 F.3d at 1050 (holding that e-mails intercepted contemporaneously are e-mails intercepted while "in flight").

[44] *See Epstein*, 843 F.3d at 1150–51 (listing three independent reasons the district court erred in ruling that the complaint definitively failed to plead a contemporaneous interception of electronic communication).

delity.[45] Barry subsequently served a discovery request on Paula's attorney asking for all potential evidence of his infidelity.[46] After receiving copies of incriminating e-mails from Paula's lawyer, Barry filed suit in the District Court of Northern Illinois pursuant to 18 U.S.C. § 2520 alleging, among other things, that Paula had unlawfully intercepted his e-mails in violation of the ECPA.[47] Purportedly, Paula had installed a program on Barry's computer that automatically forwarded the e-mails received and sent from Barry's e-mail accounts to her e-mail accounts.[48]

After Barry filed his complaint, Paula filed a motion to dismiss in which she asserted that Barry's claims failed because he did not allege that Paula had contemporaneously intercepted the e-mails.[49] Pending the motions to dismiss, Barry amended his complaint to allege that Paula had in fact intercepted his e-mails contemporaneously.[50] Barry's amended complaint alleged that the e-mails were forwarded to Paula at the same time the intended recipient e-mail servers received them.[51] Still, Judge Thomas M. Durkin of the District Court of Northern Illinois granted Paula's motions to dismiss.[52]

On appeal, the Seventh Circuit held that contemporaneousness was not a determinative factor as to whether or not a plaintiff has successfully pled an unlawful interception.[53] The court held that even if the FWA only covered contem-

---

[45] *Id.* at 1148.

[46] *Id.* at 1148–49.

[47] *Id.* Barry also alleged in his complaint that Paula's lawyer had unlawfully disclosed those e-mails by delivering the e-mails to Barry in response to Barry's discovery request. *Id.* This claim was dismissed by the Northern District of Illinois, and the dismissal was affirmed by the Seventh Circuit. *Id.* An unlawful disclosure of electronic communications is actionable under the ECPA, but this is a separate claim from an unlawful interception. *See* 18 U.S.C. § 2511(1)(c) (unlawful to intentionally disclose or attempt to disclose one's wire, oral, or electronic communication). Here, Barry consented to the disclosure of his e-mails by Paula's lawyer when he made the discovery request. *See Epstein*, 843 F.3d at 1151–52 (holding that Barry's claim against Paula's lawyer failed because the FWA does not cover a disclosure that occurs with consent). The e-mails were incriminating because, although rarely prosecuted, adultery is still a crime in the state of Illinois. *Epstein*, 843 F.3d at 1153 (Posner, J., concurring).

[48] *Epstein*, 2015 WL 1840650, at *1.

[49] *Id.*; *Epstein*, 843 F.3d at 1149; *see also Fraser*, 352 F.3d at 113 (requiring that an e-mail interception actionable under the ECPA must occur contemporaneously with transmission of that e-mail). Though not relevant to the interception issue, Barry also alleged that Paula's lawyer, Jay Frank, had unlawfully disclosed intercepted electronic communications. *Epstein*, 2015 WL 1840650, at *1. Frank also moved to dismiss Barry's unlawful disclosure claim. *Id.* at *2.

[50] *Epstein*, 2015 WL 1840650, at *1–2.

[51] *Id.*

[52] *Id.* at *3. Further, Judge Durkin granted Paula's attorney's motion to dismiss on the grounds that Barry had consented to the disclosure of e-mails. *Id.* at *4.

[53] *See Epstein*, 843 F.3d at 1150–51 (holding that even if the FWA only covers contemporaneous interceptions, the allegedly intercepted e-mails do not conclusively defeat Barry's claim that Paula unlawfully intercepted his e-mails); *see also* Patricia Manson, *Man Gets OK to Sue Wife Over Hacking*, CHI. DAILY L. BULL. (Dec. 15, 2016), http://www.chicagolawbulletin.com/archives/2016/12/15/wife-husband-email-hack-12-15-16 [https://perma.cc/7CXF-2QUA] (explaining the court's holding

poraneous interceptions, the time-stamped e-mails attached to Barry's complaint did not defeat his claim against Paula for three reasons: 1) the District Court misunderstood when an interception actually occurs; 2) the District Court mixed up the e-mails the husband had received and the e-mails the husband had sent; 3) and discovery may bring forward other e-mails with different timestamps.[54]

II. JUDGES DECIDE WHEN CONTEMPORANEOUSNESS IS A DETERMINATIVE FACTOR FOR AN UNLAWFUL INTERCEPTION OF ELECTRONIC COMMUNICATIONS UNDER THE ECPA

The U.S. Court of Appeals for the Third, Fifth, Sixth, Ninth, and Eleventh Circuits have all held that an unlawful interception of electronic communication must occur contemporaneously with the transmission of that electronic communication.[55] The Eleventh Circuit defined contemporaneous with transmission as "in flight," or the seconds in between the communication being sent (i.e. pressing the send button to transmit an e-mail) and the communication being placed in some kind of temporary storage (i.e. an e-mail inbox).[56] Other courts have adopted this definition as well.[57] Section A of this Part examines how and why courts have found contemporaneousness to be a determinative factor at final judgment, summary judgment, and at the pleadings stage.[58] Section B of this Part examines how and why the U.S. Court of Appeals for the Seventh Circuit departed from the other Federal Circuit Courts in *Epstein v. Epstein*.[59]

---

that the timestamps on Barry's e-mails that were forwarded to Paula's e-mail address do not close off the possibility that the e-mails were intercepted by Paula at the time they were transmitted). Interestingly, the Seventh Circuit effectually also overturned another case out of the Northern District of Illinois that had been decided in between Judge Durkin's order and the appeal. *See* Owen v. Cigna, 188 F. Supp. 3d 790, 792 (N.D. Ill. 2016) (citing Judge Durkin's order in *Epstein* to support the court's dismissal of a claim for the unlawful interception of e-mails on the basis that the plaintiff had not shown his e-mails were intercepted contemporaneously). *But see* Vasil v. Kiip, Inc., No. 16-CV-09937, 2018 WL 1156328, at *4 (N.D. Ill. Mar. 5, 2018) (dismissing a claim for the unlawful interception of electronic communication because the interception did not occur contemporaneously).

[54] *Epstein*, 843 F.3d at 1150–51.

[55] Luis v. Zang, 833 F.3d 619, 629 (6th Cir. 2016); Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003); United States v. Steiger, 318 F.3d 1039, 1048–49 (11th Cir. 2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002); Steve Jackson Games, Inc. v. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994).

[56] *Steiger*, 318 F.3d at 1050 (quoting Jarrod J. White, *E-Mail@Work.com: Employer Monitoring of Employee E-Mail*, 48 ALA. L. REV. 1079, 1083 (1997)).

[57] *See Luis*, 833 F.3d at 629 (agreeing with the Eleventh Circuit's reasoning that a contemporaneous interception is an interception of an electronic communication in flight, or intercepted while the communication is being transmitted); Krise v. Sei/Aaron's Inc., No. 1:14-CV-1209-TWT, 2017 WL 3608189, at *10 (N.D. Ga. Aug. 22, 2017) (quoting *Steiger* when defining a contemporaneous interception as an interception of electronic communication in flight).

[58] *See infra* notes 60–86 and accompanying text.

[59] *See infra* notes 87–94 and accompanying text.

A. Contemporaneousness as a Determinative Factor for an Unlawful Interception

The Eleventh Circuit in *United States v. Steiger*, in line with the Fifth Circuit in *Steve Jackson Games, Inc. v. Secret Service*, held at final judgment that contemporaneousness is a determinative factor for an unlawful interception of electronic communication under the Electronic Communications Privacy Act ("ECPA").[60] In 2003, in *Steiger*, a defendant-child abuser attempted to suppress the evidence contained in his personal computer data (a form of electronic communication) because those data were acquired via an unlawful interception under the ECPA.[61] The District Court did not address the defendant's argument that the personal computer data evidence should be suppressed under the ECPA.[62] Nevertheless, on appeal the Eleventh Circuit held that retrieving the computer data was not an unlawful interception of electronic communication because, in order to constitute an unlawful interception, the acquisition of that data needed to occur contemporaneously with transmission of that data.[63] In other words, the communication had to have been intercepted while in flight.[64] Like the Fifth Circuit in *Steve Jackson Games*, the Eleventh Circuit

---

[60] *Steiger*, 318 F.3d at 1047–48 (citing to *Steve Jackson Games*, 36 F.3d at 463 in its conclusion that unlawful interceptions of electronic communication under the ECPA must occur contemporaneously with transmission of that electronic communication). As previously discussed, the Fifth Circuit in *Steve Jackson Games* upheld the final judgment of the District Court for the Western District of Texas that the Secret Service did not unlawfully intercept private e-mails stored on an electronic bulletin board where those e-mails were not acquired contemporaneously with transmission and instead constituted stored communications. *Steve Jackson Games*, 36 F.3d at 458. As previously noted, the Fifth Circuit reasoned that Congress had intended to distinguish between electronic communications in storage and electronic communications in transit because Congress separately defined electronic communication and electronic storage. *See id.* at 461 (defining electronic communication and electronic storage separately by citing 18 U.S.C. § 2510(12), (17) (2012)).

[61] *Steiger*, 318 F.3d at 1046. The defendant sought to suppress the evidence found on his computer because the government proffered that evidence in criminal proceedings against him for alleged child sex abuse as well as possession and receipt of child pornography. *Id.* at 1041, 1046. Importantly, the defendant argued that where a third party had used a computer virus to surveil the defendant's personal computer data, the computer virus constituted an interception. *Id.* at 1044.

[62] *Id.* at 1046. Even if the evidence was unlawfully intercepted, the FWA only allows a criminal defendant to suppress unlawfully intercepted wire and oral communications and not electronic communications. *Id.* Interestingly, and beyond the scope of this Comment, the Eleventh Circuit upheld that the FWA, as codified under 18 U.S.C. §§ 2511, 2520, does not permit a defendant to suppress unlawfully intercepted electronic communications from evidence. *Id.*; *see also* United States v. Jones, 364 F. Supp. 2d 1303, 1305–06 (D. Utah, 2005) (holding that the FWA's suppression remedy under 18 U.S.C. § 2515 extends only to wire and oral communications and not electronic communications); Salter, *supra* note 40, at 378–79 (explaining that the FWA's suppression remedy is not available for communications in transit that were not communicated by voice).

[63] *Steiger*, 318 F.3d at 1048–49.

[64] *Id.* The Eleventh Circuit derived the phrase "in flight" from the dictionary definition of intercept, defined as the stopping or interrupting while in progress and before arrival. *Id.* As previously noted, "in flight" in the context of e-mail interceptions means the seconds in between the communica-

reasoned that unless the electronic communication is acquired while in flight, that electronic communication is in storage and thus no interception has occurred.[65]

The Third Circuit and Ninth Circuits previously held that contemporaneousness is a determinative factor for an unlawful interception of electronic communication under the ECPA at summary judgment.[66] In 2002, in *Konop v. Hawaiian Airlines, Inc.*, the Ninth Circuit concluded that contemporaneousness is a determinative factor at the summary judgment stage.[67] In *Konop*, a supervisor used an account under someone else's name to access and then distribute the contents of a plaintiff-employee's website, where the plaintiff-employee published posts criticizing the defendant-employer.[68] The Ninth Circuit affirmed a grant of summary judgment for the defendant-employer as to the unlawful interception claim because the contents of the website were not obtained while in transmission.[69] Thus, as a matter of law, no unlawful interception existed.[70] The Ninth Circuit affirmed, and further explained that Congress in 2001 had implicitly adopted contemporaneousness as a determinative factor when considering unlawful interceptions of electronic communication.[71] Significantly, the Ninth Circuit distinguished *Konop* from *United States v.*

---

tion being sent and the communication being placed in some kind of temporary storage. *See id.* at 1050 (quoting White, *supra* note 56, at 1083).

[65] *See id.* at 1048–49 (citing to the Fifth and Ninth Circuits to support its proposition that stored communications cannot be intercepted and that an interception of electronic communication can only occur contemporaneously with transmission of that electronic communication); *see also* Salter, *supra* note 40, at 378 (explaining the different treatment of electronic communication in transit and electronic communication in storage in civil and criminal cases).

[66] *Fraser*, 352 F.3d at 113, *Konop*, 302 F.3d at 879.

[67] *Konop*, 302 F.3d at 879.

[68] *Id.* at 873.

[69] *Id.* at 878–79. Just as other courts distinguished between electronic communications in transit and electronic communications in storage, the Ninth Circuit in *Konop* explained that no interception occurred because the contents of the website were obtained while in storage. *Id.*; *see also* Roundy, *supra* note 5, at 420 (explaining the distinction between electronic communication in transit and electronic communication in storage).

[70] *See Konop*, 302 F.3d at 878–79 (affirming summary judgment because no interception could have occurred unless the interception occurred contemporaneously with transmission).

[71] *Id.* Specifically, the court explained that Congress had accepted the decisions of the Federal Circuit Courts that held contemporaneousness to be a determinative factor because Congress amended the FWA without addressing the issue. *Id.* (referring to, generally, the USA PATRIOT Act, which amended the FWA without changing the definition of "intercept"); *see also Steve Jackson Games*, 36 F.3d at 458 (concluding, before 2001, that contemporaneousness was a requisite element in unlawful interception claims). Separately, the court established the secure website as a form of electronic communication because an Internet server sends documents from the website to the computer of someone accessing those documents from the secure website. *Konop*, 302 F.3d at 876. Thus, the secure website is itself the transfer of information by an electronic system. *Id.*

Smith, a 1998 Ninth Circuit decision that held interceptions of *wire* communications do not need to occur contemporaneously.[72]

Similarly, in June of 2003, the Third Circuit affirmed a grant of summary judgment in favor of an employer who allegedly intercepted an employee's e-mails in violation of the Federal Wiretap Act ("FWA").[73] Evidence reflected that the employer's acquisition of the employee's previously sent and received e-mails did not constitute a contemporaneous interception under the ECPA.[74] The employer's searching and subsequent acquisition of the employee's stored e-mails could not constitute an unlawful interception because the employer did not acquire the e-mails contemporaneously with any type of transmission of those e-mails.[75] The court based its holding on the fact that it was adopting the definition of contemporaneous used by other Federal Circuit Courts.[76]

Most recently, and three months before the Seventh Circuit decided *Epstein v. Epstein*, the Sixth Circuit allowed a complainant to plead that his e-mails were unlawfully intercepted for the express reason that his complaint sufficiently alleged that his e-mails had been intercepted contemporaneously with transmission.[77] Here, a husband suspicious of his wife's online activity, used a software program called WebWatcher to allegedly intercept e-mails and online instant messages sent between his wife and the complainant.[78] The complainant claimed that the suspicious husband and Awareness, the company that produced the WebWatcher software, had unlawfully intercepted his electronic communications under the FWA.[79]

---

[72] *See Konop*, 302 F.3d at 877–78 (noting that *United States v. Smith* stands for the proposition that wire communications do not need to be intercepted contemporaneously with transmission); *see also* United States v. Smith, 155 F.3d 1051, 1056–58 (9th Cir. 1998) (holding that an interception of wire communications does not need to occur contemporaneously with transmission, but the FWA does require the interception of oral or electronic communications to occur contemporaneously with transmission).

[73] *Fraser*, 352 F.3d at 113.

[74] *Id.*

[75] *Id.* Just as the courts before it had done, the Third Circuit distinguished between electronic communications in transit and electronic communications in storage. *Id.* at 114. Since the employee's e-mails had been obtained while stored in the employee's e-mail inbox, no interception could have occurred. *Id.*

[76] *Id.* at 113–14; *see also Steiger*, 318 F.3d at 1048–49 (defining a contemporaneous interception of electronic communication as an acquisition of electronic communication in flight); *Konop*, 302 F.3d at 878 (defining a contemporaneous interception of electronic communication as an acquisition of electronic communication during transmission and not while in storage); *Steve Jackson Games*, 36 F.3d at 458 (defining a contemporaneous interception of electronic communication as an acquisition of electronic communication during transmission of that communication).

[77] *Luis*, 833 F.3d at 625.

[78] *Id.* at 624.

[79] *Id.* The complainant settled his unlawful interception claim against the suspicious husband. *Id.* at 623. As support for his unlawful interception claim against Awareness, the complainant pointed to advertising materials in which Awareness had advertised Web Watcher as a program allowing users to

The District Court for the Southern District of Ohio, on the recommendation of a magistrate judge, granted Awareness' motion to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6).[80] The court held that the complainant had failed to allege a plausible unlawful interception claim against Awareness, and the court defined an unlawful interception as an interception occurring contemporaneously with transmission.[81] The Sixth Circuit reversed and remanded the case, with two important holdings: first, a complainant must plead that an unlawful interception under 18 U.S.C. § 2511 must occur contemporaneously with transmission.[82] Second, the complainant here did sufficiently plead that Awareness contemporaneously intercepted his e-mails and other online messages.[83]

The Sixth Circuit inferred that because Awareness had advertised WebWatcher as a software that could acquire electronic communication "in near real-time," Awareness was likely acquiring the complainant's e-mails and instant messages as soon as those electronic communications were sent.[84] In other words, the electronic communications were intercepted contemporaneously with transmission.[85] By reversing the grant of a motion to dismiss *because* the complainant pled a contemporaneous interception, the Sixth Circuit implied that contemporaneousness is a determinative factor at the pleadings stage of a claim for the unlawful interception of electronic communications under the ECPA.[86]

---

view someone's electronic communications "in near real-time." *See id.* at 631 (exposing the contents of certain Awareness advertising materials).

[80] *Id.* at 625.

[81] *Id.*; *see also* Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (holding that a claim is plausible and can survive a 12(b)(6) motion to dismiss where the facts in the plaintiff's pleading "allow[] the court to draw [a] reasonable inference" that the plaintiff would win on their claim). The district court granted the motion to dismiss on the grounds that it was the suspicious husband and not Awareness that had intercepted the complainant's e-mails. *Luis*, 833 F.3d at 625. The Sixth Circuit reversed this particular holding for reasons not relevant to this discussion. *Id.* at 627.

[82] *Luis*, 833 F.3d at 629. The FWA establishes that an intentional interception of electronic communication is an unlawful interception. 18 U.S.C. § 2511(1)(a) (2012).

[83] *Luis*, 833 F.3d at 630. The court's reference to a sufficient pleading refers to the heightened pleading standard necessary to overcome a motion to dismiss. *See Iqbal*, 556 U.S. at 678 (establishing that a complaint puts forth a plausible claim when the facts in the plaintiff's complaint "allow[] the court to draw [a] reasonable inference" that the plaintiff would win on their claim).

[84] *Luis*, 833 F.3d at 631.

[85] *See id.* at 629–31 (describing Awareness's acquisition of the complainant's electronic communication as a contemporaneous interception because WebWatcher was advertised as a program that captures communications at the same time the communications are transmitted). The Sixth Circuit also pointed to the complaint, which specifically stated that the e-mails and instant messages were not previously stored by the complainant. *Id.* at 630. The complaint further stated that Awareness had acquired the e-mails and instant messages as they were being written and sent. *Id.*

[86] *See id.* at 630–31 (reversing the dismissal because the complainant's allegation that WebWatcher "instantaneously" routed communications to its servers, combined with Awareness's advertising materials, allowed the court to infer that Awareness had contemporaneously intercepted the complainant's electronic communications).

B. The Application of Contemporaneousness as a Determinative Factor at the Pleadings Stage of an Unlawful Interception Claim Under the ECPA in Epstein v. Epstein

In *Epstein v. Epstein*, the Seventh Circuit did not decide whether or not interceptions of electronic communication had to occur contemporaneously with transmission.[87] Instead, the court decided that contemporaneousness was not a determinative factor that would automatically dismiss a plaintiff's unlawful interception claim.[88] In other words, a court could make the reasonable inference that a plaintiff would succeed in his or her claim even without a complaint that lays out the specifics of when the interception of electronic communication occurred.[89] Printed versions of the allegedly intercepted e-mails attached to Barry's complaint suggested that Paula received the e-mails well after Barry had sent those e-mails.[90] Nevertheless, the court explained that an interception occurs at the e-mail server, not when the interceptor (in this case, Paula) receives those e-mails.[91]

Consequently, the Seventh Circuit decided it could reasonably infer (based on Barry's complaint) that Barry would successfully prove Paula *contemporaneously* intercepted his e-mails.[92] In sum, the Seventh Circuit held that making the reasonable inference that a plaintiff would succeed in an unlawful interception claim does not require a court to decide at the pleadings stage that

---

[87] Epstein v. Epstein, 843 F.3d 1147, 1150 (7th Cir. 2016). Significantly, the court pointed to another Seventh Circuit case that dealt with the alleged unlawful interception of e-mails. *See* United States v. Szymuszkiewicz, 622 F.3d 701, 705–06 (7th Cir. 2010) (holding that an employee unlawfully intercepted his supervisor's e-mails because the employee could access the intercepted e-mails almost immediately after transmission). The Seventh Circuit explained that, in *United States v. Szymuszkiewicz*, it did not decide whether contemporaneousness was a factor to consider in unlawful interception claims. *Epstein*, 843 F.3d at 1150. Rather, *Szymuszkiewicz* left that question open. *Id.*

[88] *See Epstein*, 843 F.3d at 1150–51 (holding that even if the FWA only covers contemporaneous interceptions, the allegedly intercepted e-mails do not defeat Barry's claim that Paula unlawfully intercepted his e-mails).

[89] *Id.*; *see also Iqbal*, 556 U.S. at 678 (holding that a claim is plausible when a court can "draw a reasonable inference" that the plaintiff would win on his or her claim based on the facts in the complaint).

[90] *See Epstein*, 843 F.3d at 1150 (explaining that the shortest interval of time in between Barry sending or receiving an e-mail and that same e-mail being forwarded to Paula's e-mail account was three hours).

[91] *Id.*; *see also Szymuszkiewicz*, 622 F.3d at 704 (explaining that an unlawful interception of e-mail communications occurs when the e-mails are "copied at the server"). An e-mail server is a centralized computer system that transfers e-mails in between e-mail accounts. *Mail Server*, COMPUTER HOPE (Dec. 29, 2017), https://www.computerhope.com/jargon/m/mailserv.htm [https://perma.cc/7XU3-386K].

[92] *See Epstein*, 843 F.3d at 1150 (containing the court's explicit holding that Barry's complaint could withstand a 12(b)(6) motion to dismiss). In fact, the Seventh Circuit's inference seems more like the standard of getting past the "speculative level" that the Sixth Circuit points to in *Luis v. Zang*. *See id.* (establishing that Barry Epstein pled a viable ECPA claim); *see also Luis*, 833 F.3d at 630 (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555 (2007)) (holding that factual allegations must go beyond the "speculative level" in order to survive a motion to dismiss).

the interception occurred contemporaneously with transmission.[93] The Seventh Circuit's holding that contemporaneousness is not a determinative factor at the pleadings stage of an unlawful interception claim reflects the Congressional intent of the ECPA.[94]

III. The Seventh Circuit's Holding in *Epstein v. Epstein* Is More in Line with the Congressional Intent of the ECPA

The U.S. Court of Appeals for the Seventh Circuit's holding in *Epstein v. Epstein* reflects Congress' intent in drafting the Electronic Communications Privacy Act ("ECPA").[95] Congress passed the ECPA in large part to protect the privacy of electronic communications, such as e-mail.[96] Despite several amendments to the Federal Wiretap Act ("FWA") since the passage of the ECPA, Congress has not altered the ECPA provisions that aimed to protect the privacy of electronic communications.[97]

In 1986, Congress amended the FWA by passing the ECPA because members of Congress were particularly concerned with protecting the privacy of e-mail communications.[98] The FWA has been amended several times since 1986, but no amendments have affected the definitions of electronic communication or unlawful interception.[99] Even though Congress has amended certain

---

[93] *See supra* notes 87–92 and accompanying text. The Seventh Circuit used a line of reasoning similar to the line of reasoning used by the Sixth Circuit in *Luis*. *See Epstein*, 843 F.3d at 1150–51 (laying out the three elements of the court's reasoning); *cf.* 833 F.3d at 630–31 (holding that potential evidence attached to a complaint and the plaintiff's allegations allowed the court to make a reasonable inference that the plaintiff would succeed in his claim). In *Luis*, the Sixth Circuit overturned a 12(b)(6) dismissal because the relationship between the defendant's marketing materials and the plaintiff's allegations allowed the court to make a reasonable inference that the plaintiff would succeed on his claim. 833 F.3d at 630. Similarly, by laying out the three reasons it did in *Epstein*, the Seventh Circuit overturned a 12(b)(6) dismissal because the relationship between the defendant's time stamped e-mails and the plaintiff's allegations allowed the court to make a reasonable inference that Barry could succeed on his claim. *See* 843 F.3d at 1150–51 (reversing the judgment of the District Court with regard to Paula's 12(b)(6) motion).

[94] *See infra* notes 98–110 and accompanying text (arguing that Congress passed the ECPA in part to facilitate the ability of complainants to plead plausible claims for the unlawful interception of electronic communication).

[95] *See infra* notes 98–110 and accompanying text.

[96] *See infra* notes 98–110 and accompanying text.

[97] *See infra* notes 98–110 and accompanying text.

[98] *See* S. Rep. No. 99-541, at 3–4 (1986) *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3556–58 (citing a letter written in 1984 from Senator Patrick Leahy to the Department of Justice in which Senator Leahy inquired as to whether current federal law protected e-mail and computer-to-computer communications); H.R. Rep. No. 99-647, at 21–22, 34 (1986) (elaborating on the expansion of the ECPA to cover electronic communications, which includes electronic mail).

[99] *See, e.g.*, USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272, 290–91 (2001) (amending the definitions section of Title 18 of the U.S. Code, § 2510, without changing certain definitions enacted by the ECPA, including those of "electronic communication" and "interception"); *see also* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002) (explaining that Congress chose

parts of the FWA since 1986, the ECPA was the last comprehensive set of amendments to the FWA.[100]

Contemporaneousness as a factor determinative of whether an interception of electronic communication ultimately occurred may still well be part of Congress' intent in passing the ECPA.[101] Nevertheless, the overarching goal of the ECPA was to protect the privacy of electronic communications, most notably e-mail.[102] More specifically, the ECPA was established to provide protections against the intentional interception of electronic communications.[103] Consequently, Congress likely did not intend for a plaintiff like Barry Epstein—whose e-mails were surreptitiously obtained—to be dismissed out of court because his complaint and affidavit arguably did not establish contemporaneousness.[104] The legislative history of the ECPA reflects that Congress intended for the law to expand access to civil actions for unlawful surveillance.[105]

Further, the Seventh Circuit's holding in *Epstein* is in line with a holding from an *en banc* U.S. Court of Appeals for the First Circuit that the ECPA does not necessarily require an interception of electronic communication to occur

---

not to change the definition of an unlawful interception of electronic communication when it amended the FWA in 2001).

[100] *See* Adam Gillaspie, Comment, *Extraterritorial Application of the Stored Communications Act: Why* Microsoft Corp. v. United States *Signals That Technology Has Surpassed Law*, 66 U. KAN. L. REV. 459, 466–67 (2017) (explaining that the ECPA was the last major amendment to the FWA).

[101] *See, e.g.*, Steve Jackson Games, Inc. v. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994) (holding that an interception must occur contemporaneously with transmission because that was Congress's intent when it separated the definitions of "electronic communication" and "stored communication"). Although, if stored e-mail is sent and then intercepted in transit, the First Circuit Court of Appeals has held that such e-mails are electronic communications and such an interception is unlawful under the ECPA. United States v. Councilman, 418 F.3d 67, 80 (1st Cir. 2005). This bolsters the claim that Congress intended for the ECPA definitions of "interception" and "electronic communication" to help, not hinder, the ability of plaintiffs to bring unlawful interception claims. *See id.* (holding that a plaintiff potentially had an unlawful interception claim where confusion existed concerning the classification between stored communication and transmitted electronic communication).

[102] *See* S. REP. NO. 99-541, at 3–4 (citing a letter written in 1984 from Senator Patrick Leahy to the Department of Justice in which Senator Leahy inquired as to whether current federal law protected e-mail and computer-to-computer communications); *see also* Roundy, *supra* note 5, at 403 (explaining that Congress intended to expand privacy protections to e-mail in passing the ECPA).

[103] H.R. REP. NO. 99-647, at 34–35 (making clear Congress's explicit intent to provide greater privacy protections to electronic communications by providing protections against the interception of those communications); *see also* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, 1853 (adding the word "intentionally" to 18 U.S.C. § 2511 in order to clarify the requisite state of mind necessary for an unlawful interception).

[104] *See* H.R. REP. NO. 99-647, at 34–35 (explaining that the ECPA's inclusion of "electronic communication" into the FWA was mean to provide protections against the interception of electronic communications).

[105] *See id.* at 40–41 (explaining that the privacy interests of U.S. citizens were a preeminent concern that led to the ECPA and urging intelligence agencies to keep Congress informed of their surveillance activities), *id*. at 50 (explaining that a plaintiff should be able to bring a civil action for an unlawful interception under 18 U.S.C. § 2520 regardless of whether the defendant is subject to a criminal prosecution for that interception).

contemporaneously.[106] The First Circuit affirmed the district court's denial of the defendant's motion to dismiss the government's indictment because the court believed that Congress did not necessarily intend to require interceptions of electronic communication to occur contemporaneously with transmission under the ECPA.[107] Given the lack of consistency among the various Circuit Courts that have interpreted the contemporaneousness factor, the Seventh Circuit in *Epstein* correctly held that the precise time when the electronic communication was intercepted should not determine the fate of a plaintiff's complaint.[108]

The Seventh Circuit's holding in *Epstein v. Epstein* helped an unfaithful husband, but the court's holding has the potential to facilitate the ability of all plaintiffs to protect the privacy of their personal e-mails.[109] Contemporaneousness may still be necessary to ultimately establish an unlawful interception under the ECPA, but it should not be the determinative factor that prohibits a plaintiff from having their day in court.[110]

CONCLUSION

Contemporaneousness is a court-interpreted factor used to determine whether an interception has actually occurred in a claim for the unlawful interception of electronic communications under the FWA. The U.S. Court of Appeals for the Seventh Circuit held in *Epstein v. Epstein* that contemporaneousness is not a determinative factor at the pleadings stage of an unlawful interception claim. A plausible claim for the unlawful interception of electronic communication does not need to show that the interception of electronic communication occurred at the precise time the electronic communication was in transit. Such a holding stands in line with the Congressional intent of the ECPA, which sought to increase the privacy protections afforded to electronic communications such as e-mails.

JOSEPH NOREÑA

Preferred cite: Joseph Noreña, Comment, *Unfaithful But Not Without Privacy Protections: The Seventh Circuit Addresses When Courts Should Consider an E-Mail Interception Unlawful in* Eptein v. Epstien, 59 B.C. L. REV. E. SUPP. 391 (2018), http://lawdigitalcommons.bc.edu/bclr/vol59/iss9/391/.

---

[106] *See Councilman*, 418 F.3d at 76, 79–80 (holding that a plain reading of the ECPA does not necessarily preclude electronic communication in storage from being intercepted contemporaneously).

[107] *See id.* at 71 (explaining that the defendant moved to dismiss the grand jury indictment on the grounds that the government had failed to state a claim that the defendant intercepted electronic communications), 76–77 (citing H.R. REP. NO. 99-647 at 35) (explaining how Congress, contrary to the recommendations of the Department of Justice, wanted to give electronic communication a broad definition).

[108] *See Epstein*, 843 F.3d at 1150–51 (ruling that to plead an unlawful interception of electronic communication under the ECPA, a complainant does not need to establish contemporaneousness at the pleadings stage).

[109] *Id.*

[110] *Id.*