



United States District Court,
D. Delaware.

WESLEY COLLEGE, Plaintiff,
v.

Leslie PITTS, Bettina Ferguson, and Keith Hudson,
Defendants.

Civil Action No. 95-536 MMS.

Argued May 20, 1997.
Decided Aug. 11, 1997.

College sued former clerical employee, current faculty member and former faculty member, alleging violations of Title I and Title II of Electronic Communications Privacy Act (ECPA) and various state statutes arising out of compromise of security of college's e-mail system. On current and former faculty members' motion for summary judgment, the District Court, Murray M. Schwartz, Senior District Judge, held that: (1) reasonable factfinder could not infer that faculty members made affirmative attempt to intercept, or persuade another person to intercept, electronic communications; (2) faculty members did not violate ECPA in disclosing contents of e-mail divulged to them by former employee; (3) former employee's inadvertent glimpse of e-mail on computer screen could not constitute "interception" of such e-mail within meaning of ECPA; (4) assuming that former employee engaged in unauthorized access of e-mail in electronic storage in college's mainframe, such access was not unlawful "interception" of electronic communication within meaning of ECPA; (5) reasonable factfinder could not infer that faculty members themselves accessed college's mainframe and electronic communications system without authorization; (6) under Delaware law, faculty members did not share in any liability of former employee for unauthorized access; and (7) under Delaware law, faculty members lacked scienter necessary for liability for misuse of computer system information.

Motion granted.

West Headnotes

[1] Telecommunications **498**
[372k498 Most Cited Cases](#)

Liability under intentional interception provision of

Title I of Electronic Communications Privacy Act (ECPA) is predicated on affirmative attempt by defendant to intercept, or persuade another to intercept, electronic communication. [18 U.S.C.A. § 2511\(1\)\(a\)](#).

[2] Telecommunications **498**
[372k498 Most Cited Cases](#)

Reasonable factfinder in civil action under Electronic Communications Privacy act (ECPA) could not infer that faculty defendants made affirmative attempt to intercept, or persuade another person to intercept, electronic communications, as required for finding of liability under Title I of ECPA, based upon evidence that faculty members had motive to intercept e-mail and that college president received hard copies of e-mails in campus mail, and upon apparent discrepancy between testimony of former college employee and one faculty member, absent any evidence of interception in violation of Title I. [18 U.S.C.A. § 2511\(1\)\(a\)](#).

[3] Civil Rights **377.1**
[78k377.1 Most Cited Cases](#)

If trier of fact in employment discrimination case concludes defendant's testimony is not credible, it is free to infer defendant committed illegal act; whether employer has taken an adverse employment action against plaintiff is not generally at issue, sole issue is employer's motive for taking such action, and it is fair under such circumstances to infer from discrepancy in testimony or implausible denial by defendant ultimate fact of discriminatory motive.

[4] Telecommunications **498**
[372k498 Most Cited Cases](#)

Liability under use or disclosure provision of Title I of Electronic Communications Privacy Act (ECPA) requires proof that: defendant used or disclosed contents of an electronic communication such as e-mail; and sufficient facts existed concerning circumstances of interception of such communication that defendant could, with presumed knowledge of law, know or have reason to know that interception was prohibited by ECPA. [18 U.S.C.A. § 2511\(1\)\(a\)](#).

[5] Telecommunications **498**
[372k498 Most Cited Cases](#)

Liability under either "intentional interception" or "use or disclosure" provision of Title I of Electronic

Communications Privacy Act (ECPA) must be premised on interception of electronic communication; absent interception, there can be neither intentional interception nor knowledge of interception occurring in violation of law. [18 U.S.C.A. § 2511\(1\)\(a\)](#).

[6] Telecommunications  **494.1**
[372k494.1 Most Cited Cases](#)

Assuming that former college employee inadvertently saw e-mail on computer screen and then informed faculty members of its contents, faculty members did not violate Electronic Communications Privacy Act (ECPA) in disclosing contents of such e-mail, as no unlawful interception could have resulted from inadvertent glimpse of screen. [18 U.S.C.A. § 2511\(1\)\(a\)](#).

[7] Telecommunications  **494.1**
[372k494.1 Most Cited Cases](#)

Assuming that college employee inadvertently glimpsed e-mail displayed on college president's computer screen, such inadvertent glimpse could not constitute "interception" of e-mail within meaning of Electronic Communications Privacy Act (ECPA), as computer screen was medium for information rather than "electronic device" capable of being used to "intercept" e-mail within meaning of ECPA. [18 U.S.C.A. § 2511\(1\)\(a\)](#).

[8] Telecommunications  **494.1**
[372k494.1 Most Cited Cases](#)

Assuming that former college employee engaged in unauthorized access of e-mail in electronic storage in college's mainframe, such access was not unlawful "interception" of electronic communication within meaning of Electronic Communications Privacy Act (ECPA), as it was not contemporaneous with transmission of communications at issue. [18 U.S.C.A. § 2511\(1\)\(a\)](#).

[9] Telecommunications  **494.1**
[372k494.1 Most Cited Cases](#)

No "interception" of electronic communication, within meaning of Title I of Electronic Communications Privacy Act (ECPA), can occur if acquisition of contents of communication is not contemporaneous with its transmission. [18 U.S.C.A. § 2511\(1\)\(a\)](#).

[10] Telecommunications  **494.1**
[372k494.1 Most Cited Cases](#)

No violation of Title I of Electronic Communications Privacy Act (ECPA) results from acquisition of contents of electronic communication after communication has been placed in electronic storage. [18 U.S.C.A. § 2511\(1\)\(a\)](#).

[11] Telecommunications  **494.1**
[372k494.1 Most Cited Cases](#)

In context of electronic communications such as e-mail, prohibition against unauthorized access to stored wire or electronic communications articulated in Title II of Electronic Communications Privacy Act (ECPA) is separate from prohibition against unauthorized interception of such communications articulated in Title I thereof and is not lesser included offense. [18 U.S.C.A. § 2511\(1\)\(a\)](#), [2701\(a\)](#).

[12] Telecommunications  **494.1**
[372k494.1 Most Cited Cases](#)

Even assuming that former college employee who described to faculty members contents of e-mail generated by college president lied when he told faculty members that he had inadvertently seen e-mail on computer screen, and that he had in fact unlawfully intercepted such communications in violation of Electronic Communications Privacy Act (ECPA), subsequent disclosure of contents of such e-mail by faculty members did not violate ECPA, absent any evidence that faculty members knew or should have known that former employee was lying. [18 U.S.C.A. § 2511\(1\)\(a\)](#).

[13] Telecommunications  **498**
[372k498 Most Cited Cases](#)

Reasonable factfinder in civil action under Electronic Communications Privacy act (ECPA) could not conclude that faculty members accessed college's mainframe and electronic communications system without authorization and accessed e-mails in electronic storage, as required for finding of liability under Title II of ECPA, based upon evidence that faculty members had motive to intercept e-mail and that college president received hard copies of e-mails in campus mail, and upon apparent discrepancy between testimony of former college employee and one faculty member, absent any indication that faculty members had access to computer system or expertise to engage in unauthorized access. [18](#)

[U.S.C.A. § 2701\(a\)](#).

[14] Telecommunications  **498**
[372k498 Most Cited Cases](#)

Under Delaware law, faculty members who neither accessed college's mainframe themselves for purpose of obtaining private e-mail nor persuaded third party to do so on their behalf did not share in any liability of such third party for unauthorized access. [11 Del.C. § 932](#).

[15] Telecommunications  **498**
[372k498 Most Cited Cases](#)

Under Delaware law, college faculty members who were told by former college employee about contents of e-mail that employee told them he had seen on computer screen lacked scienter necessary for liability for misuse of computer system information, absent any indication that they were aware that employee was lying, or of high probability that he was lying, as to how he obtained information, or that they were aware that he had probably or actually obtained information via unauthorized access of college's computer system. [11 Del.C. § 935](#).

*[377 Charlene D. Davis](#), Daniel P. Bennett, Bayard, Handelman and Murdoch, P.A., Wilmington, DE ([Charles P. Roberts III](#), Haynsworth, Baldwin, Johnson and Greaves, P.A., Greensboro, NC, of counsel), for plaintiff.

[Frederick L. Cottrell](#), Luke E. Dembosky, Richards, Layton & Finger, Wilmington, DE ([Jeffrey Grossman](#), and Stuart Race, Fine and Staud, Philadelphia, PA, of counsel), for defendant Pitts.

Bettina Ferguson, Dover, DE, defendant pro se.

[Michael J. Malkiewicz](#), Barros, McNamara, Scanlon, Malkiewicz & Taylor, P.A., Dover, DE, for defendant Hudson.

OPINION

[MURRAY M. SCHWARTZ](#), Senior District Judge.

I. INTRODUCTION

Plaintiff Wesley College ("Wesley") filed this civil suit against three defendants, Leslie Pitts, Bettina Ferguson, and Keith Hudson, alleging violations of Title I and Title II of the Electronic Communications

Privacy Act of 1986 ("ECPA") and [Del. Code tit. 11, § § 932 and 935](#). While these are criminal statutes, civil actions are permitted under [18 U.S.C. § § 2520, 2707](#), and [Del. Code tit. 11, § 939](#), respectively. Jurisdiction is invoked pursuant to [28 U.S.C. § 1331](#) and [28 U.S.C. § 1367\(a\)](#).

Ferguson and Hudson have brought motions for summary judgment on all of Wesley's claims. For the following reasons, their motions for summary judgment will be granted.

II. FACTUAL BACKGROUND

A. The E-mail that Kept Coming Back

1. The Chancery Court Lawsuit and its Revelations

This case had its genesis over six years ago, in March of 1991, when Keith Hudson, an English teacher at Wesley College of Dover, Delaware, was denied tenure. Docket Item ("D.I.") 113 at B-3, ¶ 7. Instead, he was *[378](#) offered a terminal contract, which ended in May of 1992. After his contract expired, Hudson filed suit for breach of contract against Wesley, its Board of Trustees and Reed M. Stewart ("Stewart"), the former president of Wesley, in the Delaware Chancery Court.

Hudson was not deposed until June of 1995. His deposition began routinely enough; then Hudson was asked, by his attorney, if he was "familiar with any communications with anyone that worked or previously worked in the computer center of Wesley College relating to" an advertisement for a position as an English teacher that Wesley College had placed in a trade journal. Hudson's reply:

Yes, I am. It was--I was told by a current faculty member at Wesley that Leslie Pitts, who worked in the computer center and has subsequently left Wesley, had said that he had seen an e-mail from the president, which directed the English department when they were advertising for an English position not to advertise it in such a way that it would suit me.

D.I. 113 at B-139. After further questioning by Wesley's counsel, Hudson revealed that name of the "current faculty member": Bettina Ferguson, who taught paralegal studies at Wesley and allegedly had been told by Pitts about the e-mail. *Id.*

2. Wesley's Computer System

At this point, Wesley became concerned about security leaks in its computer system. D.I. 112 at 7. Wesley uses a networked computer system ("NCS").

The NCS is anchored by a mainframe computer, which, as Wesley puts it, "is utilized to transmit and store virtually all of the information and knowledge on which the College operates." D.I. 95 at ¶ 8. The mainframe is located in the computer center in the basement of the campus library. D.I. 113 at 1, ¶ 2. The computer center is protected by a security system and access to the computer center is limited. D.I. 95 at ¶ 8. So-called "dumb" terminals are connected to and communicate with the mainframe and are available throughout the Wesley campus; the terminals are "dumb" because they do not store information independently.

A user must have an account number and a password to utilize one of the dumb terminals; passwords are assigned by computer center personnel to faculty members, administrators, and students. D.I. 95 at 29. One of the services the terminals offered was private electronic mail ("e-mail"). Stewart, the former president of Wesley, was a particularly avid user of e-mail; he sent over 1000 e-mails a month. D.I. 113 at 2, ¶ 4.

3. *The Unmarked Envelopes*

Wesley's concerns about leaks in the NCS--specifically, the e-mail system-- were heightened when on July 17, 1995, a little less than a month after Hudson's deposition, Stewart received an unmarked envelope at his home. The envelope contained hard copies of three private e-mails authored by Stewart. D.I. 113 at 7, ¶ 3. One e-mail was dated February 15, 1995 and addressed matters regarding Hudson's suit against Wesley. So, too, another e-mail dated August 16, 1994. *Id.* The third e-mail, dated February 22, 1995, concerned new hiring. *Id.* The envelope also included a headline torn from the *Delaware State News*, a local newspaper; the flip side of the headline carried a portion of the Obituaries section of the paper. *Id.* [\[FN1\]](#)

[\[FN1\]](#). This latter observation may not be as sinister as it sounds; Pitts, who admitted sending an envelope to Stewart, explained that he included the headline to mark the date he sent the envelope.

Four days later, on July 21, 1995, Stewart was greeted with another unmarked envelope containing two more private e-mails, this time sent through campus mail. *Id.* at B-8, ¶ 4. Each e-mail concerned a truck that Stewart had purchased from

Wesley. *Id.* One e-mail was dated August 4, 1991, and the other was dated December 9, 1991. *Id.*

Now convinced that its computer system had been infiltrated, Wesley filed suit against Pitts, Ferguson, and Hudson on September 1, 1995. D.I. 1. Pitts and Hudson were deposed on October 1, 1996; approximately one day later, Stewart received yet another envelope through campus mail. D.I. 113 at 8, ¶ 5. This envelope contained another copy of the December 9, 1991 e-mail which had been *379 sent to Stewart on July 21, 1995. *Id.* On the back of this e-mail, a typed message warned, "You are falling apart. See there are more." *Id.* at 21. Two days later, Ferguson and another Wesley professor, Linda Pelzer, were deposed.

B. The Suspects

1. *Leslie Pitts*

Pitts was employed as a computer programmer by Wesley from 1993 until his discharge in March of 1995. D.I. 113 at 26. As a computer programmer, Pitts had the capability to obtain any information, "in one form or another," that was on the mainframe. *Id.* at 35. In his deposition, Pitts testified that Stewart often mistakenly printed out e-mails in the computer center, where Pitts worked, instead of his office. *Id.* at 39. Pitts said he returned some e-mails to Stewart's assistant; others he placed in a folder beside the printer in the computer center. *Id.* Stewart has flatly denied printing his e-mails. In fact, while Stewart was proficient at composing e-mails, he was yet an interactive novice in some respects; the print command on his computer remained a mystery to him. D.I. 113 at 5, ¶ 14.

After he was terminated, Pitts took the folder home. *Id.* at 38, 45. Dover police found the folder in a search of Pitts' house; most, if not all, of the e-mails in the folder mentioned Pitts by name. *Id.* at 60. If Pitts is to be believed, this is pure coincidence; he denied reading any of the e-mails until after his termination. *Id.* at 61-62. The e-mails indicate the dates and times they were created, but not the times they were printed. Several of the e-mails were created outside Pitt's working hours of 8:30 a.m. to 4:30 p.m. *See id.* at 70-76.

In his deposition, Pitts admitted he sent to Stewart at his home an unmarked envelope containing one e-mail and a headline from the *Delaware State News*. [\[FN2\]](#) This e-mail, Pitts explained, was one he "needed to return to him [Stewart] because of its

content." *Id.* at 48. Pitts further admitted he sent a copy of the same e-mail to Linda Pelzer, a Wesley professor in the English department, because she was mentioned in it. *Id.* at 53. He denied any knowledge of the e-mails sent to Stewart through the campus mail, and denied discussing with Ferguson or Hudson any of the e-mails sent to Stewart or confiscated by the Dover police. *Id.* at 64-65.

[FN2](#). There is a discrepancy between the number of e-mails Pitts admits he sent to Stewart in the envelope which also contained the *Delaware State News* headline (one) and the number Stewart states he received in that envelope (three).

2. Bettina Ferguson

Ferguson was a teacher in paralegal studies at Wesley from August 1991 until May 31, 1996. [FN3](#) Ferguson never had an e-mail account on the NCS. D.I. 107 at 41-42. According to Ferguson, she knew of Pitts and his position at Wesley, but did not know him particularly well. D.I. 107 at 38. In fact, Ferguson stated she held what she "believed to be the overall faculty opinion about his [computer] skills; that they were not very good." D.I. 107 at 78. ¶ 6.

[FN3](#). Ferguson was also an attorney. She is appearing *pro se* in this action.

Sometime in March or April of 1995, Pitts approached Ferguson on a portico on the college center and requested a meeting with her. D.I. 107 at 35. Ferguson knew Pitts had been recently terminated and warned him she could not give him any legal advice. *Id.* Pitts persisted, however, and, about twenty minutes later, entered her office.

According to Ferguson, Pitts first told her he was having difficulty finding a lawyer who charged a reasonable fee. Ferguson replied that she could not help him with that. *Id.* Then, states Ferguson, Pitts told her how "stupid" the college was to fire him, because he "knew things." *Id.* He explained to Ferguson that his job entailed counseling Wesley faculty on use of the NCS. Consequently, he said, he "saw things" on the computer screens. *Id.* at 36. In particular, he said, he saw an e-mail on a computer screen while working with someone that was relevant to Hudson's lawsuit against Wesley. *Id.*

According to Ferguson, Pitts said he could not help but read the e-mail on the screen. *Id.* In Ferguson's words, Pitts "said--in *380 fact, he showed how his eyes got big when he saw it [the e-mail], and that it said something about being careful how the English position was advertised because it might hurt the college in the Hudson case." *Id.* As Ferguson relates it, Pitts said "something about how hard it is to ignore something that's right in front of you." *Id.* at 78, ¶ 7. Without much further ado, Pitts left. *Id.* at 36.

Ferguson knew about Hudson's suit against Wesley, so she immediately called Hudson and recounted the conversation she had with Pitts. *Id.* at 36- 37. Hudson is a minister in Ferguson's church, and Hudson and Ferguson have discussed the e-mail, Pitts' story, and Hudson's suit against Wesley on a number of occasions. *Id.* at 77-78. Ferguson and Hudson had something else in common; they were both disconcerted about treatment they had received at Wesley. Hudson, of course, had filed suit against Wesley, while Ferguson had utilized the internal grievance procedure to appeal a denial of promotion. *Id.* at 99-100.

Ferguson testified she had never seen a hard copy of the e-mail message she discussed with Pitts until her deposition. *Id.* at 37. Indeed, she states she is still not certain that any one of the e-mails she was shown during her deposition was the one mentioned by Pitts. *Id.* at 79.

3. Keith Hudson

Hudson was an English and drama professor at Wesley from the fall of 1985 until the spring of 1992, when he was terminated. D.I. 107 at 43-44. Hudson has a lawsuit pending against Wesley arising out of that termination. Hudson did not have access to the e-mail system on the NCS; in fact, he testified he was never a user of the Wesley computer system at all. *Id.* at 48. Hudson testified he received a phone call from Ferguson and Ferguson told him Pitts had seen an e-mail while working in Stewart's office. After hearing the contents of the e-mail from Ferguson, Hudson thought it would be helpful in his lawsuit against Wesley because it would refute Wesley's contention that his dismissal was a purely economic decision. Hudson discussed the e-mail in very general terms with his church members, and in more detail with his attorney, his wife, and his children. D.I. 113 at 126, 131-32.

4. Linda Pelzer

Pelzer is a professor in the English department of Wesley. D.I. 113 at 133. She received an unmarked envelope postmarked July 21, 1995. The envelope contained a February 15, 1995 e-mail authored by Stewart. The portion of the e-mail that mentioned Pelzer was highlighted. The e-mail pertained to Hudson's lawsuit against Wesley and the need for another faculty member with expertise in British Literature. [\[FN4\]](#) Pelzer placed the e-mail in her cabinet, and discussed it only with her husband. *Id.* at 134.

[FN4.](#) The February 15, 1995 e-mail (which, recall, was sent in an unmarked envelope to Stewart at his home) was addressed to his administrative assistant, Nancy Steigerwald (now Nancy Best), his wife, Beverly Stewart, and Dixie Norris, a Wesley employee. The e-mail stated:

I think Dale Dubay in Wilm and Terry Hickey in Dover (Schmittinger and Rodriguez) must answer this for you/me. I believe Linda is an advocate for Hudson. You/I DARE NOT say anything to her which could get back to Hudson and his lawyer. One slip and my life and this college is ruined. I also personally disagree that we need a faculty person in Brit Lit and cannot support it. We need someone with expertise in English Composition. We also have someone in Brit Lit! Isn't that is special capability of Raleigh.

Let us not say ANYTHING to Pelzer which could endanger me or this case. Please. We need a generalist in that English position and I would rather have Linda angry about that than me ruined in court and the college crippled. I know/trust you understand.

Please delete this from the E-mail and call Dale and Terry. Identify yourself and explain to them what is happening. However, you yourself have told me of the vote of that division on drama as a minor and you mentioned you thought it was motivated to support Hudson. These people either don't realize or don't care that my life and that of my family could be ruined or this college, with a stupid misstep, could sustain damages which would cripple the very future.

Please acknowledge and delete.

D.I. 113 at 11 (all typographical and grammatical errors in original).

Pelzer is not a party to this lawsuit. In fact, Wesley has described her behavior as "innocent[]." D.I. 112 at 20.

*381 III. DISCUSSION

A. Summary Judgment Standards

[Rule 56 of the Federal Rules of Civil Procedure](#) allows summary judgment when "there is no genuine issue as to any material fact and ... the moving party is entitled to a judgment as a matter of law." "[A]n issue is genuine only if a reasonable jury, considering the evidence presented, could find for the non-moving party." [Surace v. Caterpillar, Inc.](#), 111 F.3d 1039, 1043 (3d Cir.1997) (quoting [Childers v. Joseph](#), 842 F.2d 689, 693-94 (3d Cir.1988)). In addition, the nonmoving party receives the benefit of all reasonable inferences from the record. [Bray v. Marriott Hotels](#), 110 F.3d 986, 989 (3d Cir.1997).

B. Title I of the ECPA

1. The discrepancy

The case against Ferguson and Hudson under Title I is principally based on the discrepancy in the respective testimony of Pitts and Ferguson. To recap, Pitts denied discussing with anyone any of the sixteen e-mails shown to him at his deposition which were confiscated from his house or sent to Stewart through the mail. D.I. 113 at 61. Ferguson, on the other hand, testified she was told by Pitts that he saw an e-mail on a computer screen; the e-mail Pitts told her about resembles in content one of the sixteen e-mails produced at Pitts' deposition--specifically, the February 15, 1995 e-mail. [\[FN5\]](#) D.I. 113 at 77.

[FN5.](#) Pitts allegedly told Ferguson he saw an e-mail from Stewart which directed the Wesley English department not to advertise a position in such a way that would fit Hudson's qualifications. D.I. 113 at 139. Hudson's testimony reinforces Ferguson's tale, except that Hudson testified he was told by Ferguson that Pitts saw the email on *Stewart's* computer screen, while Ferguson testified Pitts told her only he saw the e-mail on *someone's* computer screen. Compare what Pitts allegedly related to Ferguson with the February 15, 1995 e-mail, which is excerpted *supra* in note 4.

The two stories are not necessarily irreconcilable. Pitt only testified he never discussed any of the e-mails he was shown at his deposition with anybody else; it is possible, Ferguson and Hudson posit, that Pitts told Ferguson about an e-mail similar to the February 15, 1995 e-mail, but not shown to Pitts at his deposition. After all, Stewart states he produces on average 1000 e-mails per month; it is unlikely that each of Stewart's e-mails covers a novel topic. Indeed, several of the e-mails produced in this litigation cover the same topic. Further, Pitts allegedly told Ferguson he saw the incriminating e-mail on a computer screen, and Pitts was asked only if he had discussed e-mails which had been printed as hard copies.

But at summary judgment, where all reasonable inferences must be drawn in favor of the nonmovant, the Court cannot say a reasonable finder of fact could not find Pitts' testimony and Ferguson's testimony are inconsistent. The key question is whether a reasonable fact finder can infer from this discrepancy that either Ferguson or Hudson violated the ECPA.

2. The first avenue of Title I liability--"intentionally intercepts, endeavors to intercept or procures any other person to intercept"

[\[1\]\[2\]](#) Title I of the Electronic Communications Privacy Act subjects to suit any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any ... electronic communication." [18 U.S.C. § 2511\(1\)\(a\)](#). Liability under this aspect of Title I is predicated, then, on an affirmative attempt by the defendant to intercept, or persuade another to intercept, an electronic communication. The only way Ferguson or Hudson could be found liable, then, would be if a factfinder endorses Pitts' testimony and concludes Ferguson is lying. [\[FN6\]](#) Wesley argues a factfinder could then envision one of two scenarios:

[FN6](#). This is because if Ferguson's testimony is credited, then she merely heard Pitts relate how he saw an e-mail; there is nothing in her testimony to indicate she intercepted an e-mail herself, or persuaded Pitts to intercept an e-mail on her behalf.

(1) Ferguson, by herself or with Hudson and perhaps others, illegally acquired Stewart's e-mails. One of these e-mails was the February 15, 1995 e-mail; this

would explain, [*382](#) argues Wesley, how Ferguson had independent knowledge of the contents of the February 15, 1995 e-mail when Pitts never told her about it. Ferguson, again by herself or with Hudson and perhaps others, delivered the two envelopes containing e-mails to Stewart through campus mail.

(2) Ferguson and Hudson collaborated with Pitts to acquire the e-mails. Pitts used his computer know-how to access NCS and obtain Stewart's e-mails. Pitts sent the envelope containing three e-mails to Stewart at home. Ferguson, perhaps with assistance from her alleged sinister cohorts, delivered the other two envelopes to Stewart through campus mail.

Further, Wesley provides a motive for all three defendants; each had a record of animosity toward Wesley and Stewart, argues Wesley. Ferguson was challenging a denial of promotion through internal grievance hearings. Hudson and Pitts had been terminated. Hudson was litigating the legality of his termination, Pitts was considering doing the same.

Aside from a potential motive, however, neither scenario is supported by a shred of admissible evidence. As for the first scenario, Ferguson has testified she never had any "kind of account" on the NCS, the system Stewart used. D.I. 107 at 41-42. Further, Wesley--who, as a plaintiff bears the burden of proving its allegations by a preponderance of evidence--has either adduced no evidence or failed to point to any evidence to show Ferguson had the opportunity or technological capability to "intercept" the NCS and peruse Stewart's e-mails.

The evidence is just as infirm with regard to Hudson. Hudson, like Ferguson, testified he was "never" a user of NCS and he never had an e-mail account. D.I. 107 at 47-48. This testimony is un rebutted. Further, Hudson was no longer even employed by Wesley when the e-mails were allegedly "intercepted." There is simply no record evidence to support a conclusion Hudson had the computer skills or opportunity to infiltrate the NCS system and pinch Stewart's e-mails, ostensibly for use in his lawsuit.

The second plot outlined by Wesley--that of a collaborative effort by the three defendants--is even more fanciful. The record shows one chance meeting of any length between Pitts and Ferguson--a meeting which, if Pitts is to be believed, never even occurred. Hudson, on the other hand, testified he had never met Pitts until the day of Hudson's deposition. D.I. 110 at 153. Wesley has not pointed to any statements by Pitts which would suggest

anything more occurred between the three--much less a shadowy conspiracy.

At bottom, a factfinder would be asked to determine liability on the above bases from three things: (1) motive, (2) an apparent discrepancy in the testimony of Pitts and Ferguson, and (3) e-mails sent to Stewart through campus mail which nobody has of yet owned up to. This is not enough; a reasonable factfinder could not conclude, without more, that either Ferguson or Hudson took affirmative steps to intercept or access Stewart's e-mail when there is no evidence they possessed the capability to take those steps or joined forces with somebody who did.

[3] Nevertheless, Wesley argues this case is akin to employment discrimination cases, where if a trier of fact concludes the testimony of a defendant is not credible, it is free to infer the defendant committed an illegal act. See *St. Mary's Honor Ctr. v. Hicks*, 509 U.S. 502, 511, 113 S.Ct. 2742, 2749, 125 L.Ed.2d 407 (1993); *Marzano v. Computer Science Corp.*, 91 F.3d 497, 509 (3d Cir.1996). This case is different, however. In employment discrimination cases, there is no question the employer has taken an adverse employment action against the plaintiff; for example, the employer rarely contests a plaintiff was not actually fired, or denied a promotion, or demoted. The only issue left is motive--did the employer take that adverse action because the plaintiff belonged to a protected class? It is fair, then, to infer from a discrepancy in testimony, or an implausible denial by the defendant, the ultimate fact of discriminatory motive.

Here, though, Wesley would ask the finder of fact to do more. Wesley wants the factfinder to infer from the discrepancy in Pitts' testimony and Ferguson's testimony not just that one of the two is lying, but that Ferguson took an affirmative, adverse action (i.e., intercepted or accessed the e-mail). *383 *Scutieri v. Paige*, 808 F.2d 785, 790 (11th Cir.1987), a case Wesley relies upon for the proposition that summary judgment is inappropriate because "[d]irect evidence may not be available based on the stealthiness of the invasion" and "[t]he success of a wiretap ultimately depends upon secrecy and concealment" is illustrative of this distinction.

In *Scutieri*, the Eleventh Circuit Court of Appeals reversed a grant of a directed verdict in favor of Marquez, a co-owner of a burglar alarm company, who was accused of installing wiretaps and bugging devices in the plaintiff's apartment. The evidence was much more substantial against Marquez in

Scutieri than against Ferguson and Hudson in this case, however. For example, Marquez, as the co-owner of a burglar alarm company, certainly had the capability to install an illegal wiretap. Further, Marquez was seen and admitted working in areas and with devices that contained illegal wiretaps. *Id.* at 789-90. Finally, security guards, who were under strict orders to log-in each person that entered the apartment complex, were instructed by another defendant, Paige, not to log-in Marquez; "[i]t seems odd," the *Scutieri* court concluded, "that Paige, who the evidence clearly established was responsible for the wiretapping, would conceal Marquez's presence on the premises if Marquez was there for a purely legitimate and proper reason." *Id.* at 790.

Thus, several key factors were present in *Scutieri* which are glaringly absent here--capability of the defendant to commit the alleged act, ample opportunity to commit the act, evidence fixing the defendant at the scene of the illegal interception, and concrete evidence of irregular behavior which would suggest a conspiracy. What Wesley has presented is insufficient; no rational jury could find either Ferguson or Hudson liable under the first aspect of Title I.

3. *The second avenue of Title I liability--disclosure of the contents of an electronic communication while knowing or having reason to know of an illegal interception*
(a) *The two elements of Title I disclosure liability*

[4] Title I also makes it unlawful for any person to use or disclose to any other person the contents of any electronic communication while knowing or having reason to know the information was obtained through the illegal interception of an electronic communication. 18 U.S.C. § 2511(1)(c) & (d). Thus, to prevail under this Title I theory against Ferguson and Hudson, Wesley would have to prove two elements: (1) Ferguson and/or Hudson used or disclosed the contents of an electronic communication, in this case, an e-mail, and (2) sufficient facts existed concerning the circumstances of the interception such that Ferguson and/or Hudson could, with presumed knowledge of the law, know or have reason to know the interception was prohibited by the ECPA. See *Forsyth v. Barr*, 19 F.3d 1527 (5th Cir.1994); *Williams v. Poulos*, 11 F.3d 271, 284 (1st Cir.1993).

As for the first element, Wesley observes that Ferguson disclosed the contents of the e-mail to

Hudson, and Hudson disclosed the contents to his wife and children. Further, Wesley argues, Hudson attempted to use the contents of the e-mail in the Chancery Court litigation; the information was elicited from him by his attorney during his deposition. See [In re Grand Jury](#), 111 F.3d 1066, 1077 (3d Cir.1997) (holding that disclosure of intercepted communications in compliance with subpoena duces tecum would be a violation of § 2511(1)(c)); [Poulos](#), 11 F.3d at 288 (holding that illegal interceptions cannot be introduced into evidence for impeachment purposes in civil cases); [Bess v. Bess](#), 929 F.2d 1332, 1334 (8th Cir.1991) (holding husband violated 18 U.S.C. § 2511 by reciting facts obtained from intercepted conversations in divorce proceeding in attempt to establish marital misconduct by wife). Ferguson and Hudson challenge whether there is enough evidence to satisfy the first element; they note they engaged in behavior similar to Pelzer, yet Pelzer has been described as "innocent" by Wesley and has not endured the hardship of being a named defendant in this case.

[5] The Court need not resolve the dispute over this first element, however. Insufficient facts exist from which a reasonable *384 fact finder could determine Ferguson and Hudson, with imputed knowledge of the law, should have known Pitts intercepted Stewart's e-mail in violation of the ECPA. To be more precise, liability under either aspect of Title I must be premised on an intercept as defined in that Title. As discussed with regard to the first aspect of Title I liability, there is no evidence Ferguson and Hudson, alone or together or with others, intercepted Stewart's e-mails.

(b) *Intercept--Use of a Device*

[6][7] If what Pitts allegedly told Ferguson is true--that is, Pitts inadvertently glimpsed an e-mail on a computer screen while helping someone-- then Ferguson and Hudson cannot be liable under the ECPA. This is so because the ECPA defines "intercept" as the "acquisition of the contents of any wire, electronic, or oral communication *through the use of any electronic, mechanical, or other device*[" 18 U.S.C. § 2510(4) (emphasis added). Wesley argues Pitts could still be guilty of an interception because the computer screen can be considered the electronic device by which he acquired his information. This contention is meritless. First, the computer screen was just the medium for the information, not an intermediary employed

by Pitts to receive the information. Wesley would conflate the two. Simply put, Congress had in mind more surreptitious threats to privacy than simply looking over one's shoulder at a computer screen when it passed the ECPA. [FN7] See [United States v. Meriwether](#), 917 F.2d 955, 960 (6th Cir.1990) (holding agent did not acquire contents of communication by "electronic, mechanical or other device" by pressing digital display button on pager and visually observing telephone numbers); [United States v. McLeod](#), 493 F.2d 1186, 1188 (7th Cir.1974) (holding no interception when government agent stood four feet from defendant and overheard conversations involving illicit gambling activities because agent did not use any "electronic, mechanical or other device" in obtaining evidence). Accordingly, if Pitts merely read the e-mail on the computer screen of the author or recipient, he did not violate the ECPA. Both Ferguson and Hudson would, of course, also be absolved of liability, as their liability must be premised on an unlawful intercept.

[FN7. This is exhibited in the statements made in the Senate in consideration of the amendments made to the ECPA in 1986:

[T]remendous advances in telecommunications and computer technologies have carried with them comparable technological advances in surveillance devices and techniques. Electronic hardware making it possible for overzealous law enforcement agencies, industrial spies and private parties to intercept the personal or proprietary communications of others are readily available in the American market today....

.

[T]he law must advance with technology to ensure the continued vitality of the Fourth Amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right. S. Rep. No. 541, 99th Cong., 2d Sess., 5

(1986) *reprinted in* 1986 U.S.C.C.A.N. 3557, 3559.

(c) *Intercept--Does it Cover Electronic Storage of Electronic Communications?*

Wesley argues a reasonable fact finder could conclude that while Ferguson's testimony may be true, when Pitts told Ferguson in her office that he acquired his information by mere casual observance of a computer screen, his tale came with a wink and a nod. In other words, Pitts was lying, and Ferguson either knew it or should have known it.

[8] This supposition only results in liability, of course, if a factfinder could infer Pitts actually had the capability to intercept Stewart's e-mails. After all, Ferguson and Hudson can only be liable under Title I if an intercept occurred. In *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 458 (5th Cir.1994), the Fifth Circuit Court of Appeals, interpreting the ECPA, held the seizure of a computer containing private e-mail which had been transmitted to and stored in an electronic bulletin *385 board system on that computer but had not yet been read by the intended recipients was not an unlawful intercept under Title I. Relying on *Steve Jackson Games*, Ferguson and Hudson argue Wesley cannot show the predicate unlawful intercept under Title I because there is no evidence Pitts acquired the e-mails contemporaneously with their transmission. Wesley, on the other hand, argues the *Steve Jackson Games* court erred in its interpretation of the ECPA, and Pitts' acquisition of e-mail need not have occurred simultaneously with Stewart's transmission to be an intercept under Title I of the ECPA.

(1) *The Statutory Language*

An intercept is defined in Title I as "the aural or other acquisition of the contents of any wire, electronic, or oral communication ..." 18 U.S.C. § 2510(4). [FN8] Two definitions contained within the definition of intercept are vital to the analysis here. Wire communication is defined in Title I 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 ... and such term includes any electronic storage of such communication." [FN9] 18 U.S.C. § 2510(1) (emphasis added). Electronic communication, such as an e-mail, is defined

differently, however. An electronic communication is "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 photooptical system but does not include ... any wire or oral communication." The definition of electronic communications, then, unlike the definition of wire communications, does not include the electronic storage of such communications. Electronic storage, in turn, is defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication[.] ..." 18 U.S.C. § 2510(17).

[FN8] Prior to its 1986 amendment, 18 U.S.C. § 2510(4) defined "intercept" as the "aural acquisition" of the contents of wire or oral communications through the use of a device. In 1986, the definition was changed to read the "aural or other acquisition of the contents of ... wire, electronic, or oral communications ..." The words "or other" were needed because electronic communications, as defined by the ECPA, cannot be acquired aurally.

[FN9] Title I of the ECPA also prohibits the intercept of oral communication, which is defined as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication[.]" 18 U.S.C. § 2510(2). Since the definition of oral communication does not amplify the issue of whether an acquisition of an electronic communication must be contemporaneous with its transmission, and for the sake of brevity, the Court does not address it in the text.

[9][10] Noting the omission of communications in electronic storage from the definition of electronic communications, the *Steve Jackson Games* court concluded electronic communications can only be "intercepted" in violation of Title I when they are in transit, not already in storage. 36 F.3d at 461-62. Indeed, each court to consider the question has

concluded there can be no interception under Title I if the acquisition of the contents of electronic communications is not contemporaneous with their transmissions. See [United States v. Moriarty, 962 F.Supp. 217, 221 \(D.Mass.1997\)](#) (recognizing temporal difference between Title I, which prohibits acquisition of contents of electronic communications contemporaneous with transmissions of those communications, and Title II, which governs once electronic messages are stored.); [Bohach v. City of Reno, 932 F.Supp. 1232, 1236-37 \(D.Nev.1996\)](#) ("An 'electronic communication,' by definition, cannot be 'intercepted' when it is in 'electronic storage,' because only 'communications' can be 'intercepted,' and, as the Fifth Circuit held in [Steve Jackson Games](#), the 'electronic storage' of an 'electronic communication' is by definition not part of the communication."); [United States v. Reyes, 922 F.Supp. 818, 836 \(S.D.N.Y.1996\)](#) ("[I]ntercepting an electronic communication essentially means acquiring the transfer of data.... [T]he *386 [ECPA] definitions thus imply a requirement that the acquisition of the data be simultaneous with the original transmission of the data."). See also [United States v. Turk, 526 F.2d 654, 658 \(5th Cir.1976\)](#) (holding that replaying a previously recorded conversation is not an intercept, because an intercept "require[s] participation by the one charged with an 'interception' in the contemporaneous acquisition of the communication through the use of the device."); [Payne v. Norwest Corp., 911 F.Supp. 1299, 1303 \(D.Mont.1995\)](#) (finding no "intercept" because defendant's "use of a handheld recorder to record voice mail messages did not occur contemporaneously with the leaving of the messages."), *aff'd in part, rev'd in part*, [113 F.3d 1079 \(9th Cir.1997\)](#).

Wesley attributes the omission of "electronic storage" from the definition of "electronic communications" to sloppy drafting by Congress. Instead, Wesley points to other evidence which, it asserts, demonstrates Congress intended Title I to protect e-mails even after they have been transmitted and are in electronic storage. First, Wesley notes, the terms "wire communication" and "electronic communication" do not focus on the meaning of a "communication" (the meaning of which Wesley submits is self-evident), but rather on the manner in which a communication is transmitted. This distinction is important, argues Wesley, because a communication does not cease being a communication after it is transmitted.

This point is related to the definition of "intercept"

under Title I, asserts Wesley. Intercept is defined as the "aural or other acquisition of the contents" of an electronic communication. There is no temporal limitation on the acquisition of a communication in the definition of intercept, notes Wesley; had Congress intended to limit Title I's coverage to acquisitions simultaneous with transmission, Wesley argues, it could have added the words "while in transit" after the word "acquisition."

Wesley is indeed correct Congress could have added those words had it so desired. But the omission of those words does not signify Congress intended to expand the definition of "intercept" to encompass the electronic storage of electronic communications. By distinguishing between wire communications and electronic communications--specifically, by including the electronic storage of wire communications within the definition of such communications but declining to do the same for electronic communications-- Congress sufficiently evinced its intent to make acquisitions of electronic communications unlawful under Title I only if they occur contemporaneously with their transmissions. Wesley's position cannot be adopted simply because Congress failed to take all possible measures to make the ECPA crystalline. [\[FN10\]](#)

[FN10](#). Wesley has pointed to other areas of the ECPA in which Congress has been less than precise. For example, the definition of "oral communication" excludes "any electronic communication," without any mention of wire communication, [18 U.S.C. § 2510\(2\)](#), while the definition of "electronic communication" excludes "any wire or oral communication," [18 U.S.C. § 2510\(12\)](#). It would be incongruous to equate wire communications and oral communications from this minor difference, argues Wesley, yet the Fifth Circuit Court of Appeals did just that when it gave substantive meaning to the term "electronic storage," found in "wire communication," but missing from the definition of "electronic communication."

Wesley's argument is misplaced. As will be discussed in the text, there is other evidence to indicate the omission of "electronic storage" from the definition of "electronic communication" was deliberate.

Wesley has a second argument that relates to the

definition of "intercept" under Title I. An intercept is defined as the acquisition of the *contents* of a communication, Wesley notes, it does not require the acquisition of the communication itself. See [18 U.S.C. § 2510\(4\)](#). If, as per [Steve Jackson Games](#), a communication can be intercepted only while in transit, Wesley argues, then "it is difficult to see how anyone could ever intercept the contents of an electronic communications[]" because the contents of an electronic communication cannot be known until after transmission has been completed. In making this argument, Wesley is separating the contents of an electronic communication from the communication itself. But this is an artificial separation. Title I is aimed not at when the contents of an electronic communication are discerned, but rather when the electronic *387 communication itself is intercepted *en route* to its intended recipient. The latter can be done by tapping a wire, much like the method used to tap a telephone call. See [Bohach, 932 F.Supp. at 1236](#) (finding no interception because "[a]fter all, no computer or phone lines have been tapped, ..."); Megan Connor Bertron, [Home Is Where Your Modem Is: An Appropriate Application of Search and Seizure Law to Electronic Mail](#), 34 AM. CRIM. L. REV. 163, 185 (1996) ("Both e-mail and telephone calls travel over the same wires ... [and] both forms of communication are transmitted, essentially, with the stroke of a few keys[.]"); Gregory L. Brown, [Steve Jackson Games, Inc. v. United States Secret Service: Seizure of Stored Electronic Mail Is Not An "Interception" Under the Federal Wiretap Act](#), 69 TUL. L. REV. 1381, 1391 n. 75 (1995) (comparing transmission of e-mail to transmission of telephone call). Thus, an interloper can obtain a communication and its contents simultaneously--during transmission.

Accordingly, the plain language of the ECPA reflects Congress did not intend for "intercept" to apply to electronic communications in "electronic storage." See [Steve Jackson Games, 36 F.3d at 461-62](#). In other words, under the text of Title I, Ferguson and Hudson could only be held liable if Pitts acquired the e-mails before they were placed in electronic storage, *i.e.*, during their transmission.

Nevertheless, the ECPA has been derided as being "famous (if not infamous) for its lack of clarity[.]" [Id. at 462](#). Accordingly, resort to the legislative history and statutory framework as a whole is necessary. Even after examining the legislative history and the framework of the ECPA, however, this Court, like the [Steve Jackson Games](#) court, concludes Congress did not intend to include the

acquisition of electronic communications in electronic storage within the definition of "intercept."

(2) Legislative History

Prior to its 1986 amendment, [18 U.S.C. § 2511](#) covered only wire and oral communications. Interpreting the pre-amendment [18 U.S.C. § 2511](#), the Fifth Circuit Court of Appeals held the Secret Service did not intercept communications by replaying a previously recorded conversation because an intercept "require[s] participation by the one charged with an 'interception' in the contemporaneous acquisition of the communication through the use of the device." [United States v. Turk, 526 F.2d 654, 658 \(5th Cir.1976\)](#). Title I of the ECPA extended coverage to electronic communications, of course, and Congress retained the definition of "intercept" as it existed at the time of the amendment. See [Steve Jackson Games, 36 F.3d at 462](#) (quoting S. REP. No. 99-541, 99th Cong., 2d Sess. 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3567). The Senate Report, quoted in [Steve Jackson Games](#), recounts:

Section 101(a)(3) of the [ECPA] amends the definition of the term "intercept" in current [section 2510\(4\) of title 18](#) to cover electronic communications. *The definition of "intercept" under current law is retained with respect to wire and oral communications except that the term "or other" is inserted after "aural."* This amendment clarifies that it is illegal to intercept the nonvoice portion of a wire communication. For example, it is illegal to intercept the data or digitized portion of a voice communication.

1986 U.S.C.C.A.N. at 3567 (emphasis added).

(3) Comparison to Title II

Further, this intent, and the concomitant temporal limitation on "intercept" in Title I, are reinforced upon scrutiny of Title II of the ECPA. Title II generally proscribes unauthorized access to stored wire or electronic communications. [Section 2701](#) provides:

[11] Except as provided in subsection (c) of this section whoever--

- (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
- (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication *388 while it is in electronic

storage in such system shall be punished....

[18 U.S.C. § 2701\(a\)](#). There are stark differences between the procedural and substantive requirements of Title I and Title II. While a governmental entity can obtain access to the contents of electronic communications that have been in storage less than 180 days with a warrant, see [18 U.S.C. § 2703\(a\)](#), there are additional requirements under Title I for the interception of electronic communications, see [18 U.S.C. § 2518](#). Title I imposes limitations on the types of crimes that may be investigated, see [18 U.S.C. § 2516](#), and the breadth and duration of the intrusion, see [18 U.S.C. § 2518\(5\)](#) (court order shall be executed "in such a way as to minimize the interception of communications not otherwise subject to interception"), and [18 U.S.C. § 2518\(5\)](#) (intercept not permitted "for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days"). [\[FN11\]](#) Title II does not.

[FN11](#). The *Steve Jackson Games* court elaborated on the minimization concern that is applicable to the interception of electronic communications, rather than to the access of stored electronic communications:

Obviously, when intercepting electronic communications, law enforcement officers cannot know in advance which, if any, of the intercepted communications will be relevant to the crime under investigation, and often will have to obtain access to the contents of the communications in order to make such a determination. Interception thus poses a significant risk that officers will obtain access to communications which have no relevance to the investigation they are conducting. That risk is present to a lesser degree, and can be controlled more easily, in the context of stored electronic communications, because, as the Secret Service advised the district court, technology exists by which relevant communications can be located without the necessity of reviewing the entire contents of all of the stored communications. For example, the Secret Service claimed (although the district court found otherwise) that it reviewed the private E-mail on the BBS [bulletin board] by use of key word searches.

[36 F.3d at 463](#).

Because of these substantial differences between Title I and Title II, the *Steve Jackson Games* court concluded "it is most unlikely that Congress intended to require law enforcement officers to satisfy the more stringent requirements for an intercept in order to gain access to the contents of stored electronic communications." [36 F.3d at 462](#). This Court agrees; Wesley's attempt to expand the definition of intercept to include electronic communications in electronic storage would conflate the differing sets of requirements of Title I and Title II. [\[FN12\]](#)

[FN12](#). This conclusion has been endorsed, either implicitly or otherwise, by commentators. For example, one student has written:

[T]he stored communications provisions of [\[Section\] 2701](#) prohibit the unauthorized accessing of wire or electronic communications once stored. While the distinction between the terms "intercept" and "access" has little significance for forms of communication that only exist as transmissions, and are never stored, the distinction is critical when a transmitted communication is later electronically stored, because it is at the time of storage that a communication becomes subject to different provisions of the ECPA. This is the case with both E-mail and voice-mail messages, both of which have a transmission phase and a storage phase. During the transmission phase, any protection against unlawful interception under [the ECPA] is governed by [\[Section\] 2511](#). On arrival in storage, the same messages are subject to [\[Section\] 2701](#).

Thomas R. Greenberg, Comment, *E-mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 AM. U.L. REV. 219, 248 (1994). See also Gregory L. Brown, *supra*, at 1390 (describing *Steve Jackson Games* as "correct in its reasoning and holding").

Wesley offers its own interpretation of the interplay between Title I and Title II. The abridged version of Wesley's argument is this: Title I outlaws the actual *acquisition* of the contents of an electronic communication, while Title II prohibits unauthorized *access* to--or the *mere opportunity to obtain*-- stored electronic communications. [\[FN13\]](#) Thus, *389

Wesley asserts, Congress intended Title II to serve as a lesser included offense; one can violate Title II without transgressing Title I, and if a defendant offended both, a plaintiff would be able to elect its remedies under either Title I or Title II.

[FN13](#). This same argument was made by the Government in [United States v. Moriarty](#), 962 F.Supp. 217, 219 (D.Mass.1997). In [Moriarty](#), the Government provided an example of the asserted distinction between "access," prohibited under Title II, and "intercept," prohibited under Title I: "a person could violate [Title II] by entering the Justice Department's computer system and altering the codes that would allow access to e-mail by authorized users. This would be a violation even though confidential e-mail messages were never intercepted. Such conduct would not violate [Title I]." *Id.* The court in [Moriarty](#) never addressed the validity of this asserted distinction, nor does this Court do so.

This may be true in some instances, but Wesley's view of Title II as a lesser included offense for stored electronic communications would nullify the difference in the procedural and substantive requirements of Title I and Title II. Under Wesley's view, the Government would be required to obtain a court order pursuant to [18 U.S.C. § 2518](#), with its concomitant limitations on the manner and duration of the intrusion, every time it acquired electronic communications in storage, such as on a computer disk. Title II's more lax requirements would only come into play when the Government wanted the opportunity to acquire a stored electronic communication. Wesley has pointed to no authority or legislative history to indicate Congress intended such a result.

Wesley also argues that, given the definition of wire communication, overlap between Title I and Title II is inevitable. The definition of wire communication in Title I includes the electronic storage of such communication. [18 U.S.C. § 2510\(1\)](#). But Title II also applies to the unauthorized access to a facility that results in access "to a wire or electronic communication while it is in storage." Therefore, concludes Wesley, it is futile to justify a temporal limitation on the term "intercept" from the differing substantive and procedural schemes of Title I and Title II. The short answer is while this argument

demonstrates there may be overlap between Title I and Title II with respect to wire communications, it does not show there is a similar overlap for the coverage of electronic communications.

Finally, Wesley laments the gap left in the ECPA if an intercept in Title I does not include stored electronic communications. Title I prohibits the disclosure or use of electronic communications, but says nothing about stored electronic communications. Title II prohibits unauthorized access to stored electronic communications, but does not censure the disclosure or use of the contents of those stored communications unless the disclosing or using party is the provider of an electronic communication service. See [18 U.S.C. § 2702\(a\)](#). Thus, a person who does not provide an electronic communication service (like Ferguson and Hudson) can disclose or use with impunity the contents of an electronic communication unlawfully obtained from electronic storage.

The Court agrees with Wesley that this gap in ECPA coverage is troubling. If it is to be bridged, however, it must be through the legislative power of Congress, not by the judiciary.

(4) *No evidence of "intercept"*

[\[12\]](#) As the preceding exercise in ECPA interpretation demonstrates, Wesley can only receive a favorable judgment against Ferguson and Hudson under Title I if it can show Pitts acquired Stewart's e-mails before they were placed in electronic storage, *i.e.*, while they were transmitted. Wesley has marshaled its evidence in an attempt to argue a rational jury could conclude Pitts acquired the e-mails while they were *en route* to their recipients. First, Wesley observes, many of the e-mails were created between 8:30 a.m. and 4:30 p.m., the hours in which Pitts was at work. As a computer programmer, Pitts admittedly had the capability to obtain any information, "in one form or another," that was on the mainframe. *Id.* at 35. Further, numerous e-mails authored by Stewart were found in Pitts' possession. While Pitts claims Stewart mistakenly printed them out in the computer center, and Pitts just coffered them in a folder for safekeeping, Stewart contradicted this by stating he was unfamiliar with the print command on his computer and it was not his practice to print or make hard copies of e-mail messages he received or sent. D.I. 113 at 5, ¶ 14. Finally, the fact that most, if not all, e-mails contained a reference to Pitts belies the notion that Stewart printed the e-mails out inadvertently. This

raises a substantial question as to how Pitts acquired the e-mails.

But asking a jury to resolve that question--at least on this summary judgment record--by concluding Pitts pinched the e-mails *390 during their transmission (and hence intercepted them in violation of Title I) would be soliciting guesswork. [FN14](#) Many of the e-mails were created by Stewart at times when Pitts was not scheduled to work. In fact, the e-mail vital to Wesley's theory of the case against Ferguson and Hudson--the February 15, 1995 e-mail that Wesley alleges was discussed by all three defendants--was created at 6:45 p.m., and thus outside of Pitts' working hours. It would have been impossible, then, for Pitts to acquire their contents at the same time as their transmission unless he had access to the NCS from a remote location. There is no evidence in this record that he did. Most important, however, Wesley has proffered no testimony and no evidence, expert or otherwise, to explain how Pitts would have acquired Stewart's e-mails contemporaneously with their transmission. Indeed, in its own answers to Hudson's interrogatories, Wesley averred that each e-mail involved in this litigation "was *not* intercepted contemporaneously with its transmission, but was intercepted at a later time." *See* D.I. 110 at 82-84, 86-93 (emphasis is Wesley's). Now, in opposing summary judgment, Wesley wants to depart from its own sworn assertion. It has offered no reason to support such a departure and will not be permitted to do so.

[FN14](#). The Court notes that while much of this discussion pertains to Pitts, Pitts has not joined in the motion for summary judgment. Accordingly the analysis and conclusions contained in this opinion are limited to this summary judgment record, and must not be construed as definitive on the issue of Pitts' alleged liability under Title I.

This would not be the only inferential leap required to affix liability on Ferguson and Hudson under Title I. Not only would a jury be forced to guess as to when and how Pitts obtained the e-mails, but a jury would also have to demonstrate Ferguson or Hudson knew or should have known Pitts was lying when he related his account about seeing a stray e-mail on the computer screen of an unwary Wesley faculty member. [FN15](#) Ferguson has produced a substantial amount of evidence to rebut the suggestion she should have known Pitts had

intercepted e-mail from Stewart. For instance, she testified she had little regard for Pitts' computer abilities, D.I. 107 at 78, ¶ 6, and described Pitts' tale, punctuated by animated facial expressions, as "completely credible." *Id.* at ¶ 8. In fact, Ferguson states, she had "no reason to doubt him." *Id.* The suggestion that Hudson knew or should have known Pitts was lying is even more tenuous. After all, Hudson never even spoke to Pitts; he merely heard the reproduction of his narrative through Ferguson.

[FN15](#). Recall, this is because if a factfinder credits Pitts over Ferguson, Title I liability would be premised on an intercept by Ferguson and/or Hudson or a shadowy conspiracy link including Ferguson, Hudson, Pitts, and perhaps others, who intercepted the e-mails. As discussed earlier, there is no evidence to support liability under this theory. If Ferguson is credited over Pitts, however, then Wesley can win a verdict if it shows Ferguson knew or should have known Pitts was lying when he allegedly described how he obtained the contents of Stewart's e-mail.

In short, Wesley's case against Ferguson and Hudson under Title I of the ECPA is built upon a series of innuendo and inferential leaps of faith. This is not enough to survive summary judgment; some cold, hard evidence of some sort is needed. Accordingly, the motions for summary judgment by Ferguson and Hudson will be granted as to Wesley's claims against them under Title I.

C. Title II of the ECPA

[18 U.S.C. § 2701\(a\)](#) provides that whoever--

- (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
 - (2) intentionally exceeds an authorization to access that facility;
- and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished....

[13](#) Wesley has alleged Ferguson and Hudson have violated Title II by accessing the NCS without authorization and pilfering *391 Stewart's e-mails from storage. [FN16](#) As stated earlier with regard to Wesley's claims under Title I, no rational factfinder

could conclude either Ferguson or Hudson had the know-how, or collaborated with someone who did, to commit such acts. Accordingly, summary judgment will also be granted as to Wesley's claims against Ferguson or Hudson under Title II.

[FN16. 18 U.S.C. § 2702](#) prohibits the disclosure of the contents of electronic communications obtained in violation of [18 U.S.C. § 2701](#); by its terms, however, [18 U.S.C. § 2702](#) applies only to persons or entities who provide an electronic communications service or a remote computing service to the public. See [18 U.S.C. § 2702\(a\)\(1\) & \(2\)](#). Wesley does not maintain either Hudson or Ferguson provides such a service to the public.

D. Delaware State Law Claims

1. [Section 932](#)

[14] Wesley has alleged violations of two Delaware statutes, [Del. Code tit. 11, § 932](#) ("[Section 932](#)") and [Del. Code tit. 11, § 935](#) ("[Section 935](#)"). [Section 932](#) is entitled "Unauthorized access" and provides that "[a] person is guilty of the computer crime of unauthorized access to a computer system when, knowing that he is not authorized to do so, he accesses or causes to be accessed any computer system without authorization." For reasons amply explored earlier in this opinion, there is no evidence Pitts accessed the Wesley NCS at the behest of Ferguson or Hudson, or that either Ferguson or Hudson accessed the NCS themselves. Summary judgment will therefore be granted in favor of Ferguson and Hudson on Wesley's [section 932](#) claim.

2. [Section 935](#)

[Section 935](#), entitled "Misuse of computer system information," is a bit lengthier. It provides:

A person is guilty of the computer crime of misuse of computer system information when:

- (1) As a result of his accessing or causing to be accessed a computer system, he intentionally makes or causes to be made an unauthorized display, use, disclosure, or copy, in any form, of data residing in, communicated by or produced by a computer system;
- (2) That person intentionally or recklessly and without authorization:
 - a. Alters, deletes, tampers with, damages, destroys

or takes data intended for use by a computer system, whether residing within or external to a computer system; or

b. Interrupts or adds data to data residing within a computer system;

(3) That person knowingly receives or retains data obtained in violation of subdivision (1) or (2) of this section; or

(4) That person uses or discloses any data which that person knows or believes was obtained in violation of subdivision (1) or (2) of this section.

[Section 935](#) is similar to [18 U.S.C. § 2511](#) in that it prohibits a person from disclosing information which that person knows was obtained by unauthorized means. But there are some important differences. For one, the scienter requirement for the Delaware statute is more stringent than its federal counterpart. The Delaware Code states that "[w]hen knowledge of the existence of a particular fact is an element of an offense, such knowledge is established if a person is aware of a high probability of its existence, unless he actually believes that it does not exist." [Del. Code tit. 11, § 255](#). Compare this to Title I of the ECPA, which requires a person only "know[] or hav[e] reason to know" the information was obtained illegally. [18 U.S.C. § 2511\(1\)\(c\) & \(d\)](#).

Further, unlike the ECPA, the Delaware statute defines "access." The Delaware Code states "access" means "to instruct, communicate with, store data in or retrieve data from a computer, computer system or computer network." [Del. Code tit. 11, § 931](#). Finally, [section 935](#) is broader than its federal analogue; [section 935](#) punishes the mere receipt of information where [18 U.S.C. § 2511](#) does not.

As rehearsed several times, there is no evidence either Ferguson or Hudson, alone or in league with others, accessed or otherwise tampered with the e-mail system on the *392 Wesley NCS. Subsections (3) & (4) must therefore provide the predicates for their liability under [Section 935](#). But as will be demonstrated, Wesley's [Section 935](#) claims against Ferguson and Hudson cannot survive summary judgment.

[15] There is an initial question whether Ferguson and Hudson received any "data" from Pitts, as that term is contemplated in the Delaware statute. While "data" is defined broadly--it "means information of any kind, in any form, including computer software[,]" [Del. Code tit. 11, § 931\(8\)](#)--it remains to be seen whether the Delaware courts would stretch the meaning of "data" so liberally as to cover the

gossip about an interoffice e-mail delivered by one loose tongue to another. But more important, there is no evidence to show either Ferguson or Hudson knew or believed Pitts acquired his knowledge about the e-mail as a result of conduct prohibited in the first two subsections of [Section 935](#). The more stringent scienter requirement of the Delaware statute becomes significant here. Wesley argues there is evidence Ferguson and Hudson should have known or assumed Pitts was lying about how he encountered the e-mail, but this is not enough under [Section 935](#). [Section 935](#) requires actual belief of wrongdoing or the cognizance of the "high probability" of existence of wrongdoing. There is no evidence Ferguson or Hudson had such a mental state.

Wesley trots out a familiar alternative argument. Similar to its assertion with regard to "intercept" in the ECPA, Wesley argues an unsanctioned glimpse at a computer screen can be considered "access" under [Section 935](#). Thus, even if Ferguson's testimony is accepted wholesale, Wesley suggests, she and Hudson can be held liable under [Section 935](#). As with its spin on "intercept," however, this would stretch the verb in the statute beyond its natural meaning. As noted earlier, access is defined under the Delaware Code as "to instruct, communicate with, store data in or retrieve data from a computer, computer system or computer network." [Del. Code tit. 11, § 931\(1\)](#). This contemplates something more technologically advanced than an untoward glance at the computer screen of a careless user. Accordingly, summary judgment will be granted against Wesley on its [Section 935](#) claims against Ferguson and Hudson.

Wesley has failed to highlight sufficient evidence to support any of its state or federal claims against Ferguson and Hudson to survive summary judgment. An appropriate order will issue.

END OF DOCUMENT