MARITAL CYBERTORT: THE LIMITS OF PRIVACY IN THE FAMILY COMPUTER

by
Laura W. Morgan[#]

I. INTRODUCTION

John and Mary have been married for 10 years. Mary has begun to suspect that John is having an affair. Rather than hire a private detective and take the risk that she will be held accountable for any torts the private detective might commit,[1] she decides to engage in a little "self-help discovery."

Mary goes through all the papers in John's desk which is in the family study, and she finds some unfamiliar bank statements, reflecting charges on a credit card she didn't know John had. She also finds a little black book that appears to have passwords for on-line accounts. Armed with this information, she decides to find whatever she can on the various computers in the home.

[#] Laura W. Morgan is the owner and operator of Family Law Consulting in Charlottesville, Virginia, which provides research and writing services to family law attorneys nationwide.

[1] *See* Laura W. Morgan, *Liability of An Attorney or Spouse for Torts Committed by a Private Detective*, 11 DIVORCE LITIG. 247 (1999).

First, Mary boots up the computer both she and John have used since they purchased it. She looks at all the directories on Windows, but she finds nothing that would pique her interest. She logs onto John's e-mail by trying every password she found in John's little black book until one works. There she finds numerous e-mails to and from Susan, one of John's co-workers; the e-mails are intimate and of an obviously romantic nature. Using John's little black book of passwords, she also finds an internet-based e-mail account in John's name on Hushmail.[2]

Mary is furious. She goes onto the internet, and using the words "catch your cheating spouse" finds E-blaster, a software program which promises to "capture their incoming and outgoing email, chats and instant messages - then immediately forward you an exact copy."[3]

A few weeks later, after Mary has received via her own Hotmail address numerous

---

[2] http://www.hushmail.com/ (last visited February 28, 2007). Similar web-based e-mail systems include Hotmail, Gmail, and Yahoo! mail. Unlike e-mail programs such as Outlook, Pegasus, or Thunderbird, which downloads e-mail from the server to the user's computer, with web-based e-mail reaches the server, it is stored and viewed on the server. As described by one authority, "Web-based e-mail systems such as Gmail, Hotmail, and Yahoo e-mail, [are] where people's e-mail remains stored at the server and not deleted after it is read." Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 Fordham L. Rev. 747 (2005). The obvious advantage of webmail is that e-mail can be accessed from any computer, anywhere in the world, so long as the computer has internet access. *See* Free Web-Based E-mail Services, at http:// www.emailaddresses.com/email_webl.htm (last visited March 3, 2006) (providing lengthy list of free web-based e-mail services around the world).

[3] http://www.spectorsoft.com/products/eBlaster_Windows/index.html (last visited February 28, 2007).

E-Blaster has the capability of monitoring computer keystrokes, including passwords and deleted words, and can either store the information on the computer for later retrieval or send it to a remote site, another computer.

e-mails sent by John to Susan, Mary decides to take the family computer to a forensic computer firm. The firm makes a copy of the hard-drive, and gives Mary a copy of all the e-mails and the documents stored on the hard-drive in the alternate data stream[4] which reflect John's Swiss bank account numbers.

Mary decides that enough is enough. She goes back home, picks up John's laptop which he uses mostly for work but also for pleasure (he takes it on family vacations), and brings the laptop to the forensic computer firm for analysis. She then goes to a divorce lawyer with all the e-mails and documents she has gathered.

Just how much trouble, if any, is Mary in?

II. THE FEDERAL LAW FRAMEWORK

A. *Title III of the Omnibus Crime Control and Safe Streets Act of 1968: The Wiretap Act*

[4] Alternate Data Streamn (ADS) is the ability to fork file data into existing files without affecting their functionality, size, or display to traditional file browsing utilities like dir or Windows Explorer.

In 1968, Congress enacted the first comprehensive federal statute regulating the surveillance of oral conversations: Title III of the Omnibus Crime Control and Safe Street Acts of 1968. This was commonly referred to as The Wiretap Act or Title III.[5]

The Wiretap Act was enacted for the purpose of protecting private individuals against wiretapping in domestic disputes and to protect against various forms of wiretapping in the business sector.[6] "The extension of The Wiretap Act's prohibition against intercepting conversations to 'any person,' by providing for minimal liquidated damages, a strong exclusionary rule, and the right to recover attorneys' fees and court costs for all violations, reflected concern for protecting conversational privacy in the private sphere."[7]

---

[5] 28 U.S.C. § 2510 et seq. (2000). *See* James G. Carr & Patricia L. Bellia, THE LAW OF ELECTRONIC SURVEILLANCE (West 2001).

[6] Richard Turkington, *Protection for Invasions of Conversational and Communication Privacy by Electronic Surveillance in Family, Marriage, and Domestic Disputes under Federal and State Wiretap and Store Communications Acts and the Common Law Privacy Intrusion Tort*, 82 NEB. L. REV. 693, 702 (2004).

[7] *Id.*

The 1968 Act prohibited the interception of "wire or oral" communications unless one party to the communication consented to the interception.[8] The original 1968 Wiretap Act restricted "wire communications" to those transmitted by telephone companies licensed by the FCC,[9] while "oral communications" were those that take place face-to-face.

B. *The Electronic Communications Privacy Act: The Amended Wiretap Act and the Stored Communications Act.*

As new methods of communication became increasingly commonplace, such as cellular phones, cordless phones and electronic communications transmitted in digital form, Congress amended the Wiretap Act with the Electronic Communications and Privacy Act of 1986 (ECPA) to also prohibit the intentional interception of electronic communications.[10] Congress also to address other privacy concerns in new technologies.

---

[8] 18 U.S.C. §§ 2511(2)(c)-(d) (2000).

[9] Wiretap Act, tit. III, § 2510, 82 Stat. 197 (1968).

[10] 100 Stat. 1848 (1986).

Briefly, the ECPA is divided into three titles.[11] Title I is the former Wiretap Act. The ECPA amended the Wiretap Act by, inter alia, adding the word "electronic" to the types of communications protected from interception,[12] as well as by amending the definition of interception to include more than just aural forms of interception.[13] Title II of the ECPA, generally referred to as the Stored Communications Act,[14] is an entirely new title that prohibits anyone but an authorized user from accessing stored electronic communications, including e-mail and voice mail.[15]

Thus, the ECPA Amendments now divide the former Wiretap Act into Title I, II, and III. The former Title III of the Omnibus Crime Control and Safe Streets Act is now Title I of the ECPA. Title I of the ECPA now regulates the interception of any conversation, including electronic conversations. Title II of the ECPA regulates access to stored e-mail, fax communications, and voicemail.

1. The Wiretap Act under Title I of ECPA

Title I of ECPA, the amended Wiretap Act, "prohibits the intentional interception of wire, oral or electronic communications and the intentional disclosure of the contents . . . by one knowing or having reason to know that the information was obtained through an

---

[11] Title III of the ECPA regulates call-tracing devices such as caller ID and pen registers. This title is not relevant to the present discussion and will not be examined.

[12] 18 U.S.C. § 2511(1) (2000). *See* Committee on the Judiciary, The Electronic Communications Privacy Act of 1986, H.R. Rep. No. 99-647, at 2 (1986).

[13] 18 U.S.C. § 2510(4) (2000).

[14] 18 U.S.C. §§ 2701-2711 (2000).

[15] The Stored Communications Act was amended by the USA PATRIOT Act, but the amendments concern government monitoring of e-mail.

interception that violates the act. . . . [The] ECPA amended the Wiretap Act by extending to data and electronic transmissions the same protection already afforded to oral and wire communications."[16] This Act now provides a private right of action "against one who intentionally intercepts, [or] endeavors to intercept ... any wire, oral, or electronic communication."[17]

[16] Fischer v. Mt. Olive Lutheran Church, Inc., 207 F. Supp. 2d 914, 922 (W.D. Wis. 2002).

[17] *Id.*

To violate the Wiretap Act provisions of the ECPA with regard to e-mail on a computer, the acquisition of the communication must occur during the transmission, not after the e-mail is received and stored on the computer.[18] In one of the first cases to address the issue, *Steve Jackson Games, Inc. v. U.S. Secret Service*,[19] the Fifth Circuit held that once an e-mail has reached any sort of electronic storage, it is no longer capable of being intercepted, as defined by the Wiretap Act, and so any access is subject only to the Stored Communications Act. The Ninth Circuit, in *Konop v. Hawaiian Airlines*,[20] initially held that "the Wiretap Act protects electronic communications from interception when stored to the same extent as when in transit."[21] The court, however, subsequently withdrew that opinion, issuing a revised opinion that accords with the analysis in *Steve Jackson Games*.[22] Other cases that have addressed the issue are in agreement: once e-mail is stored, there is no "interception" within the meaning of the Wiretap Act.[23] The only remedy

---

[18] *See generally* 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 (2006).

[19] 36 F.3d 457, 461-64 (5th Cir. 1994).

[20] 236 F.3d 1035 (9th Cir. 2001).

[21] 236 F.3d at 1046.

[22] Konop v. Hawaiian Airlines, 302 F.3d 868, 878 (9th Cir. 2002), *cert. denied,* 537 U.S. 1193, 123 S.Ct. 1292 (2003) ("We therefore hold that for a website such as Konop's to be 'intercepted' in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage.").

[23] *E.g.*, U.S. v. Councilman, 418 F.3d 67 (1st Cir. 2005); United States v. Steiger, 318 F.3d 1039, 1048-49 (11th Cir.2003), *cert. denied,* 538 U.S. 1051, 123 S.Ct. 2120 (2003) ("[W]e hold that a contemporaneous interception--*i.e.*, an acquisition during 'flight'--is required to implicate the Wiretap Act with respect to electronic communications.");

for accessing stored e-mails is Title II of ECPA, the Stored Communications Act, and even that remedy may be unavailing (see discussion below).

The application of these principles to husband and wives looking at e-mail on the family computer is scant but noteworthy.[24] On point to this discussion is *Evans v. Evans*:[25]

> In defendant's last argument, she contends the trial court committed reversible error in overruling timely and continuing objections to the admission into evidence of intercepted sexually explicit e-mails between defendant and Dr. Mark Johnson, a Chapel Hill physician. Defendant claims the e-mails, private communications received from Dr. Johnson, were illegally intercepted pursuant to 18 U.S.C. § 2511(1)(c) and (d) (2000), which prohibits the disclosure or use of any electronic communication that was intercepted in violation of the Electronic Communications Privacy Act (ECPA). However, most courts examining this issue have determined that interception "under the ECPA must occur contemporaneously with transmission." *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 (3d Cir., 2003). Here, the e-mails were stored on, and recovered from, the hard drive of the family computer. The e-mails were not intercepted at the time of transmission. Therefore, we hold the trial court did not admit the evidence in violation of the ECPA.[26]

Wesley College v. Pitts, 974 F. Supp. 375 (D. Del.1997), summarily aff'd, 172 F.3d 861 (3d Cir.1998); Garrity v. John Hancock Mut. Life Ins. Co., No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343, at *8 (D. Mass. May 7, 2002) (Electronic Communications Privacy Act "requires that the acquisition of electronic communications occur during transmission"); Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 635 (E.D. Pa. 2001) (noting that accessing an e-mail post receipt is not intercepting it and thus does not violate the ECPA and comparing this post receipt viewing to finding an already opened letter sent via the U.S. Postal Service on a co-worker's desk and reading it, which would not amount to interception).

[24] For a discussion of the Wiretap Act in relation to more traditional eavesdropping in matrimonial litigation, see Allan H. Zerman & Cary J. Mogerman, *Wiretapping and Divorce: A Survey and Analysis of the Federal and State Laws Relating to Electronic Eavesdropping and Their Application in Matrimonial Cases*, 12 J. AM. ACAD. MATRIM. LAW 227, 228 (1994).

[25] 610 S.E.2d 264 (N.C. App. 2005).

[26] 610 S.E.2d at 270-71.

Thus, because the e-mails were already in storage, there was no interception during transmission.

White v. White[27] offers a similar lesson. In *White*, the husband and wife lived in the same house. The husband occupied the sunroom of the home where the family computer, television, and stereo were located. The sun room was also the only way to get to the grill on the deck of the house. As a result, all of the members of the family were in and out of the room. After the wife discovered a letter from the husband to his girlfriend, allegedly in plain view, she hired a computer forensic expert to explore the hard-drive. The expert, at the wife's direction and without using the husband's password, copied his e-mails that were stored on the hard drive. The court held there was no violation of the New Jersey Wiretap Act because the e-mail was not in transmission when it was accessed.

[27] 781 A.2d 85 (N.J. Super. Ch. Div. 2001).

O'Brien v. O'Brien[28] offers a contrast. In that case, when marital discord erupted between the Husband and the Wife, the Wife installed a spyware program called Spector on the Husband's computer. The Spector spyware secretly took snapshots of what appeared on the computer screen, and the frequency of these snapshots allowed Spector to capture and record all chat conversations, instant messages, e-mails sent and received, and the websites visited by the user of the computer. The Wife argued that the electronic communications did not fall under the umbra of the Wiretap Act because these communications were retrieved from storage and, therefore, were not "intercepted communications" as defined by the Act. In opposition, the Husband contended that the Spector spyware installed on the computer acquired his electronic communications real-time as they were in transmission and, therefore, were intercepts illegally obtained under the Act.

The court began by noting that the federal courts have consistently held that electronic communications, in order to be intercepted, must be acquired contemporaneously with transmission and that electronic communications are not intercepted within the meaning of the Federal Wiretap Act if they are retrieved from storage. The court concluded, "The Spector spyware program that the Wife surreptitiously installed on the computer used by the Husband intercepted and copied the electronic communications as they were transmitted. We believe that particular method constitutes interception within the meaning of the . . . Act[.]"[29]

---

[28] 899 So.2d 1133 (Fla. 5th DCA 2005).

[29] *Id.* at 1136. *See generally* Camille Calman, *Spy vs. Spouse: Regulating Surveillance Software on Shared Marital Computers*, 105 COLUM. L. REV. 2097 (2005);

Patricia L. Bellia, *Spyware and the Limits of Surveillance Law*, 20 BERKELEY TECH. L.J. 1283 (2005); Janine H. McNulty, *Who Is Watching Your Keystrokes? An Analysis of M.G.L. ch. 214 § 1b, Right to Privacy and its Effectiveness Against Computer Surveillance*, 2 J. HIGH TECH. L. 67 (2003); Shana K. Rahavy, *The Federal Wiretap Act: The Permissible Scope of Eavesdropping in the Family Home*, 2 J. HIGH TECH. L. 87 (2003).

It is noteworthy that the *O'Brien* does not distinguish between the interception of *received* messages and the interception of *sent* messages, and this distinction may spell the difference between a violation of the Act and no violation. Most courts have found that interception of *outgoing* messages cannot be a wiretap, since surveillance software receives its input for outgoing communications not from the modem but directly from the computer's keyboard; such communications are wholly within one computer and do not affect interstate or foreign commerce as required by the Wiretap Act.[30] The capture of *incoming* messages, by contrast, via screenshot might be a wiretap if capture is contemporaneous with transmission.

2. The Stored Communications Act Under Title II of ECPA

Title II of ECPA is the Stored Communications Act. This part of ECPA regulates the intentional access of stored electronic communications and records. Under this Act, it is a violation if a person "intentionally accesses without authorization a facility through which an

---

[30] *See* U.S. v. Scarfo, 180 F. Supp.2d 572 (D. N.J. 2001) (keystroke programs are not in violation of any law, because they do not intercept communications, they do not access the computer in an unauthorized manner, and they cause no harm to the computer or user). *Accord* United States v. Ropp, 347 F. Supp. 2d 831, 838 (C.D. Cal. 2004).

Moreover, copies of communications by keystroke programs may be impossible to authenticate. *See* Fenje v. Feld, 2003 U.S. Dist. LEXIS 24387 (N.D. Ill., Dec. 8, 2003) (holding authentication of e-mail "is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims," citing Fed. R. Evid. 901(a)). In Zepeda v. Zepeda, 632 N.W.2d 48 (S.D. 2001), the husband installed software on home computer to covertly monitor wife's keystrokes. He discovered that she engaged in highly erotic discussions in Internet chat rooms. Husband separated from wife and later accepted a job in Texas. Husband believed wife was an Internet addict and that this led her to have sex with a man in the family home while the child was sleeping. A temporary custody order prohibited wife from using the Internet unless required by her employment. At trial, husband introduced computer log-on records to show substantial use of the Internet in the household. The court pointed out that these records did not show which member of the household used the computer or whether it was just left logged on.

electronic communication service is provided .... and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system...."[31] Any person aggrieved by a violation of this Act may bring a civil action to recover from the person or entity which engaged in the violation.[32] Quite significantly, the Stored Communications Act does not have a provision similar to the Wiretap Act that provides for the exclusion of evidence obtained in violation of the Act.[33]

---

[31] 18 U.S.C. § 2701(a)(1) (2000).

[32] 18 U.S.C. § 2707 (2000).

[33] Unlike the Wiretap Act, the Stored Communications Act does *not* provide an exclusion remedy. It allows for civil damages, *see* 18 U.S.C. § 2707, and criminal punishment, *see* 18 U.S.C. § 2701(b), but nothing more. Indeed, the Stored Communications Act expressly rules out exclusion as a remedy; § 2708, entitled "Exclusivity of Remedies," states specifically that § 2707's civil cause of action and §§ 2701(b)'s criminal penalties "are the *only* judicial remedies and sanctions for violations of" the Stored Communications Act. 18 U.S.C. § 2708.

United States v. Smith, 155 F.3d 1051, 1056 (9th Cir. 1998).

The first requirement for a violation of the Stored Communications Act is that access to the files or e-mails is "without authorization." Thus, whether a spouse has segregated an e-mail account or other files by maintaining a private password is a key fact in evaluating whether access to e-mail stored on the hard drive of a family computer is "without authorization" within the meaning of the Stored Communications Act.[34] When access is full to both spouses and not password protected, there is no violation of the act, because the access was not "without authorization."[35]

---

[34] *See* Trulock v. Freeh, 275 F.3d 391 (4th Cir. 2001) (holding that the authority to generally access the computer hard drive did not include the authority to access password protected files of a joint computer user).

[35] *E.g.*, State v. Appleby, 2002 WL 1613716 (Del. Super. 2002) (after the husband and wife co-mingled their computer hardware, using it freely as each saw fit, its ownership and possession were joint, and each spouse was entitled to the equipment as much as the other; under the circumstances, where the hard drive was left broken, uninstalled and in the estranged wife's possession and where the hard drive once was installed in the estranged wife's computer, she had complete access to it while it was working and hundreds of her personal documents remained on it, the hard drive was "theirs" in every sense); White v. White, 781 A.2d 85 ((N.J. Super. Ch. Div. 2001) (wife's access was not without authorization where the husband had consented to his wife's access to the computer); Hazard v. Hazard, 833 S.W.2d 911 (Tenn. Ct. App. 1991) (copy of a letter from the husband to his former attorney stored in the husband's computer in the marital home, to which the wife had complete access, was not privileged); Stafford v. Stafford, 641 A.2d 348 (Vt. 1993) (where wife found on the family computer a file called "MY LIST" which was an inventory and description of the husband's sexual encounters with numerous women, wife testified she found it on the family computer and that it was similar to a notebook that she had discovered the husband's handwriting giving similar accounts, computer file was admissible).

The decision in White v. White raises some important questions. The court notes,

> Shortly after defendant discovered the letter, she hired Gamma Investigative Research, and unbeknownst to plaintiff-and without using plaintiff's password-Gamma copied plaintiff's files from the computer's hard drive. These files contained e-mail sent between plaintiff and his girlfriend; they also contained images that he viewed on Netscape. Gamma then prepared a written report detailing its findings and sent copies of all the above to

> defendant and her attorney. It was only while being deposed that plaintiff learned that defendant had accessed his e-mail. He had thought-incorrectly as it turns out-that his e-mail and attachments could not be read without his AOL password.

Thus, the husband had password protected his e-mail and attachments, but the forensic computer firm was able to retrieve the e-mails and attachments from the hard-drive without the husband's password. Does not the mere presence of a password denote the husband intended the wife not have access, and therefore her act in taking the computer to Gamma Investigative Research, and their retrieval of information from the hard-drive, constitutes access "without authorization" despite the fact that the wife had access to the computer generally?

More importantly, however, is the second requirement that only e-mail that is in "electronic storage" is protected from unauthorized access under § 2701 of the Stored Communications Act. Electronic storage is defined in the ECPA as "temporary, immediate storage incidental to the electronic transmission" or "backup" storage of an electronic communication.[36] In *Fraser v. Nationwide Mutual Insurance Co.*,[37] the court explained the journey an e-mail makes from sender to recipient, and concluded that once e-mail is downloaded to the recipient's computer, it is no longer in electronic storage under the ECPA:

---

[36] 18 U.S.C. § 2510(17) (2000).

[37] 135 F. Supp. 2d 623 (E.D. Pa. 2001).

> Transmission of e-mail from the sender to the recipient through an electronic communication system . . . is indirect. First, an individual authorized to use the system logs on the system to send a message. After a message is sent, the system stores the message in temporary or intermediate storage. I will refer to this storage as "intermediate storage." After a message is sent, the system also stores a copy of the message in a separate storage for back-up protection, in the event that the system crashes before transmission is completed. I will refer to this storage as "back-up protection storage." In the course of transmission from the sender to the recipient, a message passes through both intermediate and backup protection storage. Transmission is completed when the recipient, logs on to the system and retrieves the message from intermediate storage. After the message is retrieved by the intended recipient, the message is copied to a third type of storage, which I will call "post-transmission storage." A message may remain in post-transmission storage for several years.[38]

Thus, access to e-mail already downloaded from the e-mail server was not subject to the Stored Communications Act regulation because "post-transmission storage" is not "in electronic storage."

In *White v. White*,[39] the court reached the same conclusion: once the e-mail has been dowloaded from the e-mail server to the recipient's computer, it is not in "electronic storage" under the ECPA.

The implications for family law disputes is profound. "This construction of federal and state stored communications acts take wiretap statutes off the table in cases where

---

[38] *Id.* at 633-34 (citations and footnotes omitted).

[39] *Supra*, note 25.

spouses access e-mail stored on the hard drive of a computer in the family home."[40]

[40] Richard C. Turkington, *Protection for Invasions of Conversational and Communication Privacy by Electronic Surveillance in Family, Marriage, and Domestic Disputes under Federal and State Wiretap and Store Communications Acts and the Common Law Privacy Intrusion Tort*, 82 NEB. L. REV. 693, 722 (2004).

By contrast, accessing e-mail on a remote server may well be a violation of the Stored Communications Act. Recall that under this Act, it is a violation if a person "intentionally accesses without authorization a facility through which an electronic communication service is provided .... and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system...."[41]

The courts have held that the purpose of § 2701 is to prevent unauthorized access to a facility through which an electronic communication service is provided.[42] Thus,

---

[41] 18 U.S.C. § 2701(a)(1) (2000).

[42] *See In re* Northwest Airlines Privacy Litig., 2004 WL 1278459, at *2 (D. Minn.

unauthorized access to web-based e-mail servers can constitute a violation of the Act.[43]

June 6, 2004) (dismissing § 2701-based claim because "[p]laintiffs' complaint is not with how Northwest obtained the information, but with how Northwest subsequently used the information."); Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F.Supp.2d 817, 821 (E.D. Mich.2000) ("Because section 2701 of the ECPA prohibits only unauthorized access and not the misappropriation or disclosure of information, there is no violation of section 2701 for a person with authorized access to the database no matter how malicious or larcenous his intended use of that access. Section 2701 outlaws illegal entry, not larceny."); Educ. Testing Serv. v. Stanley H. Kaplan, Educ. Ctr., Ltd., 965 F.Supp. 731, 740 (D. Md.1997) ("[I]t appears evident that the sort of trespasses to which the [ECPA] applies are those in which the trespasser gains access to information to which he is not entitled to see, not those in which the trespasser uses the information in an unauthorized way."); State Wide Photocopy, Corp. v. Tokai Fin. Servs., Inc., 909 F.Supp. 137, 145 (S.D.N.Y.1995) ("[Section] 2701 is aimed at parties accessing facilities without authorization").

[43] There is law to the effect that "electronic storage" under the Act covers only *temporary* electronic storage of e-mails that are to be forwarded to a final destination, because Congress defined "electronic storage" as "any *temporary* intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof ..." 18 U.S.C. § 2510(17)(A). Since web-based e-mail is the *final* destination, it may possibly not

C. *The Computer Fraud and Abuse Act*

---

be in electronic storage, and thus the Electronic Storage Act is inapplicable. *See* Snow v. DIRECTV, Inc., 2005 WL 1226158, * 3 (M.D. Fla. May 9, 2005).

Unlike the Wiretap Act and Stored Communications Act, which relate to wrongfully appropriated content, the Computer Fraud and Abuse Act focuses more on the wrongfully appropriated access to a computer itself.[44] The Computer Fraud and Abuse Act of 1984[45] (CFAA) prohibited the unauthorized use of or access to a computer in three comparatively narrow areas: (1) to knowingly access a computer without authorization, or in excess of authorization, in order to obtain classified United States defense or foreign relations information with the intent or reason to believe that such information would be used to harm the United States or to advantage a foreign nation; (2) to knowingly to access a computer without authorization, or in excess of authorization, in order to obtain information contained in a financial record of a financial institution or in a consumer file of a consumer reporting agency; (3) to knowingly to access a computer without authorization, or in excess of authorization, in order to use, modify, destroy, or disclose information in, or prevent authorized use of, a computer operated for or on behalf of the United States if such conduct would affect the government's use of the computer.[46]

---

[44] *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1615-17 (2003).

[45] 18 U.S.C. § 1030 (2000).

[46] 18 U.S.C. § 1030(a)(1).

The CFAA was originally enacted to prosecute computer crimes of federal interest.[47] The CFAA was amended in 1986 and again in 1994 to provide for a private right of action on "private computers." For a private computer to be a protected computer under CFAA, it must be used "in interstate or foreign commerce or communication."[48] A computer located outside the U.S. can also be protected by the CFAA if it is "used in a manner that affects interstate or foreign commerce or communications of the United States."[49] Obviously, any computer hooked up to the internet or used for e-mail falls within the definition of protected computer. Thus, "All private computers infected with spyware are likely protected computers, since the process of contracting and the operation of spyware necessarily involve the Internet and interstate commerce."[50]

The CFAA punishes three different acts. First, it is unlawful if a person or entity "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information from any protected computer if the conduct involved an interstate or foreign communication."[51]

Second, it is unlawful if any person "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of

---

[47] S. Rep. No. 99-432, at 4 (1986).

[48] 18 U.S.C. § 1030(e)(2)(B) (2000).

[49] *Id.*

[50] Andrew T. Braff, *The Spy Act: Ditching Damages as an Element of Liability for On-line Conduct Between Private Parties?*, 2 SHIDLER J. L. COM. & TECH. 17, 20 (2000).

[51] 18 U.S.C. § 1030(a)(2)(c) (2000).

of such conduct furthers the intended fraud and obtains anything of value."[52] The "thing obtained" for value "may not merely be the unauthorized use" of the computer.[53] If the conduct consists only of the use of the computer, the value of such use must exceed $5,000 in any 1-year period for the government to bring an action.[54]

---

[52] 18 U.S.C. § 1030(a)(4) (2000).

[53] *Id.*

[54] *Id.*

Third, it is unlawful if a person "intentionally causes damage" by knowingly accessing or transmitting information or code to a protected computer.[55] Damage is defined as "any impairment to the integrity or availability of data, a program, a system, or information."[56] A civil action for violation of the CFAA may be brought only if the conduct falls under § 1030(a)(5) and involves $5,000 in "loss"[57] to one or more persons during a 1-year period; physical injury; threat to public health or safety; or impairment of a medical examination, diagnosis, treatment, or care of one or more individuals.[58]

Finally, there is no express provision stating that information obtained in violation of

---

[55] 18 U.S.C. § 1030(a)(5) (2000).

[56] 18 U.S.C. § 1030(e)(8) (2000).

[57] "Loss" is defined as any "reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." See USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 814(d), 115 Stat 272, 384 (2001).

[58] 18 U.S.C. § 1030(g) (2000).

the statute is inadmissible.[59]

[59] *See generally* Dodd S. Griffith, Note, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453 (1990); Annotation, *Validity, Construction, and Application of Computer Fraud and Abuse Act*, 174 A.L.R.FED. 101 ( ).

The law applying the CFAA to the installation of spyware (keystroke or screenshot programs) is also sparse but instructive.[60] In *In re DoubleClick Inc. Privacy Litig.*,[61] the court recognized the near impossibility of an individual proving $5,000 worth of damage resulting from the installation of spyware. After all, one can replace a computer for less than $2,000. The court thus interpreted 18 U.S.C. § 1030(e)(8)(A) to permit plaintiffs to aggregate damages "across victims and over time for a single act" that violated the statute, but not across all victims and all acts for any given year.

III. THE COMMON LAW FRAMEWORK

A. *Invasion of Privacy*

The common law tort of invasion of privacy is stated when someone intentionally intrudes upon the private affairs, seclusion, or solitude of another person by means that

---

[60] See also "Creator and Four Users of Loverspy Spyware Program Indicted" at http://www.cybercrime.gov/perezIndict.htm (last visited February 28, 2007), detailing the charges against creators of "Loverspy," a trojan horse keystroke program similar to e-blaster that records keystrokes and screenshots which are then sent to a remote location.

[61] 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

would be highly offensive to a person of ordinary sensibilities.[62]

[62] Restatement (Second) of Torts § 652B (1977). *See generally* Don Corbett, *Virtual Espionage: Spyware and the Common Law Privacy Torts*, 36 U. Balt. L. Rev. 1 (Fall 2006); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006); Alan F. Blakley, Daniel B. Garrie, Matthew J. Armstrong, *Coddling Spies: Why the Law Doesn't Adequately Address Computer Spyware*, 2005 DUKE L. & TECH. REV. 25 (2005).

The "right of privacy" traces its genesis to a law review article written by Samuel D. Warren and Louis D. Brandeis who recognized and shaped the common law right to privacy over a century ago.[63] The *Restatement of Torts* codified this right of autonomy. The *Restatement* contains four categories of invasion of privacy: (1) intrusion upon seclusion, (2) appropriation of identity, (3) disclosure of private facts, and (4) publicity that places another in a false light. The right of privacy protects against an "unreasonable intrusion upon the seclusion of another." The unreasonable intrusion alone is enough for a violation of a privacy right, yet it is not actionable until it becomes highly offensive. The intrusion must be substantial and reach the level where a reasonable man would "strongly object." Intrusion covers violations, such as opening another's mail or searching another's wallet, as well as those violations using mechanical means, such as tapping a phone to eavesdrop on private conversations.[64]

The reasonableness of privacy expectations in e-mail stored in computers in the home will depend upon whether the spouse has consented or authorized access to the e-mail by the other spouse. If separate e-mail accounts and separate passwords are maintained by spouses who jointly share a computer with joint access to the main drive, each spouse would have a reasonable expectation of privacy in their separate e-mail accounts. For example, in *White v. White*,[65] the New Jersey family court held that the tort of intrusion upon seclusion could apply to the access of computer records. The court held that

---

[63] Samuel Warren and Louis Brandeis, *The Right of Privacy*, 4 HARV. L. REV. 193, 220 (1890).

[64] *See* Restatement (Second) of Torts § 652B (1977).

[65] *Supra*, note 26.

that "[a] 'reasonable person' cannot conclude that an intrusion is 'highly offensive' when the actor intrudes into an area in which the victim has either a limited or no expectation of privacy."[66] The *White* court concluded there was no invasion, however, because the computer was open to both spouses.

---

[66] *Id.* at 92. *See also* Hamberger v. Eastman, 206 A.2d 239 (N.H. 1964) (finding a privacy intrusion violation when the defendant surreptitiously placed an audio tape recorder in the plaintiffs' bedroom, even though no one listened to the tape); Miller v. Brooks, 472 S.E.2d 350, 354 (N.C. Ct. App. 1996) (finding that husband had valid causes of action for invasion of privacy and intentional infliction of emotional distress against estranged wife who, among other behaviors, intercepted his postal mail).

B. *Trespass to Chattels*

Section 217 of the Restatement (Second) of Torts provides that "[a] trespass to a chattel may be committed by intentionally . . . using or intermeddling with a chattel in the possession of another."[67] Section 218 of the Restatement provides, in relevant part, that "[o]ne who commits a trespass to a chattel is subject to liability to the possessor of the chattel if, but only if . . . the chattel is impaired as to its condition, quality, or value, or . . . harm is caused to some person or thing in which the possessor has a legally protected interest."[68]

---

[67] Restatement (Second) of Torts § 217 (1965)