Damages Is the Gatekeeper Issue for Federal Computer Fraud

George Roach*
William J. Michiels†

As the role of the personal computer and the usage of computer networks have grown, Congress has tried to keep pace with the related developments, especially pertaining to those protecting property rights. While the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, proscribes computer fraud, its overarching purpose seems more focused on shoring up commercial property rights for tangible and intangible property located on computers or computer networks.[1] The legislative

* George P. Roach is the founder of a Dallas litigation consulting and valuation firm, Multi Discipline Consultants, and is a senior advisor to the litigation consulting firm of Freeman & Mills, Inc., in Los Angeles. His background includes an M.B.A., J.D., and A.B. in economics. See www.multidisciplineconsultants.com for more information.

† William J. Michiels is a vice president at Freeman & Mills, Inc. His credentials include an M.B.A., and he is a C.P.A. in California. The authors wish to acknowledge the expert assistance of Jim Addams, Esq., without whom this Article would not be possible.

1. Perhaps the statute's original name in 1984 was less misleading: Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98 Stat. 2190 (1984).

history of the statute expresses equal concern for the privacy rights of individuals, but those rights fail to register significant commercial value and are effectively excluded from protection.

Two congressional priorities are in conflict and the resulting compromise yields a double standard: Congress wants to discourage significant damage to hardware or data files, yet it also wants to avoid criminalizing or overreacting to some insignificant activities that could be regarded as juvenile pranks. As a result, economic value has been established by the statute to distinguish between the significant and insignificant activities. Damage issues and even the calculation of damages therefore assume a much more important role than under most statutes, as the existence and amount of economic damages determine which intangible property rights warrant jurisdiction. Data files without economic value (e.g., only of personal value) are excluded from protection.

The scope of this Article focuses mainly on civil litigation, but most of the provisions of the statute are interpreted in the same manner in criminal and civil cases. The essential role of damages in making claims under this statute can be demonstrated by briefly recounting a recent criminal case. Convicted by a jury of feloniously introducing a computer virus into his employer's computer, the defendant moved for acquittal from the bench, claiming that the prosecution's inclusion of the employer's lost profits should not be admitted as evidence of damages. The judge reversed the jury, granting the motion, on the basis that the terms "loss" and "damage" were ambiguous under the CFAA[2] and found insufficient evidence in the statute's legislative history to justify the inclusion of lost profits, especially in light of the rule of lenity.[3]

A review of existing case law shows that damage issues are significant or determine the opinion in sixty percent of the cases. The majority of those cases were resolved as questions of law rather than as questions of fact for a jury. In a significant number of cases, claims were dismissed even before the plaintiff had submitted a damages report or provided testimony on damages. In twenty-four of the fifty opinions, the defendant prevailed on the motion to dismiss or for summary judgment.

---

2. The definition of loss now provided in Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 (2000), *amended by* 18 U.S.C. § 1030(e)(11) (Supp. II 2002), was not in effect for this case.

3. United States v. Pierre-Louis, No. 00-434-CR-GOLD, 2002 WL 1268396, at *3-4 (S.D. Fla. Mar. 22, 2002), *aff'd without published opinion*, 54 Fed. App'x 691 (11th Cir. 2002). *But see* Shaw v. Toshiba Am. Info. Sys., Inc., 91 F. Supp. 2d 926, 936 (E.D. Tex. 1999) (quoting Singer v. United States, 323 U.S. 338, 341-42 (1945) ("The principle of strict construction of criminal statutes does not mean that they must be given their narrowest possible meaning.")).

Equally important, however, is that the case statistics vary dramatically by the type of activity alleged and therefore warrant some categorization.

I. A STATUTE SUBJECT TO FURTHER CHANGE

The CFAA has been amended eight times since 1984[4] and further amendments seem likely as the role of computers in the American way of life continues to change. A 1986 congressional speech estimated that there existed 56,000 large general purpose computers, 213,000 smaller business computers, 570,000 minicomputers, and 2.4 million desktop computers in use in the private business sector in addition to 6 million home computers.[5] In comparison, it was recently estimated that more than 200 million Americans use computers to access the Internet today. In the United States, more Americans use computers than drive cars.

A. CFAA Claims

The statute provides for felony or misdemeanor indictments, injunctions, and civil claims. To date, the statute has been applied to claims for product liability, minor and major "trespassing," unfair competition, and various types of employment disputes. Civil claims relating to "spam" and computer "cookies" have also been frequently made.

Proscribed actions include the following categories that are listed in the statute as subsections (a)(1) through (a)(7):

1. Obtaining government-protected information;
2. Obtaining information from a protected computer by means of interstate communication;
3. Accessing a government computer;
4. Obtaining anything of value by fraudulent means from a protected computer except for computer use worth less than $5,000 in a one-year period;
5. Causing damage to a protected computer and/or its data or programming;
6. Trafficking in passwords in some situations; and

---

4. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98 Stat. 1837, *amended by* Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213, *amended by* Computer Abuse Amendments Act of 1994, Pub. L. No. 103-322, 108 Stat. 1796, *amended by* National Information Infrastructure Protection Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488, *amended by* Criminal Law Technical Amendments Act of 2002, Pub. L. No. 107-273, 116 Stat. 1806, *amended by* Cyber Security Enhancement Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (codified as amended at 18 U.S.C. § 1030 (2000)).

5. 132 CONG. REC. H3275, H3277-78 (daily ed. June 3, 1986) (statement of Rep. Nelson).

7. Threatening to damage a protected computer and/or its data or programming for purposes of extortion.[6]

Such proscribed actions must be the result of the defendant having intentionally accessed a computer without authorization or in excess of authorization where accessing the computer furthers a wrongful activity. The term "protected computer" includes computers used by the federal government, major financial institutions, and computers which are used in interstate or foreign commerce.

B. Basic Precepts of the Statute

1. Think Intangible and Tangible Assets

Since 1984, when it passed the original statute, Congress asserted that existing law did not adequately protect computer programming and data. Congress's initial solution was to ensure that computerized information was included within the definition of "property" for federal law.[7] For the purposes of the statute, Congress also developed a working definition of "obtain," which largely means to misappropriate files without otherwise changing them:

> The Department of Justice has expressed concerns that the term "obtains information" in 18 U.S.C. § 1030(a)(2) makes that subsection more than an unauthorized access offense, i.e., that it might require the prosecution to prove asportation of the data in question. Because the premise of this subsection is privacy protection, the Committee wishes to make clear that "obtaining information" in this context includes mere observation of the data. Actual asportation, in the sense of physically removing the data from its original location or transcribing the data, need not be proved in order to establish a violation of this subsection.[8]

According to an analysis reported by the Department of Justice, the 1996 amendments sought to specifically include the theft of intangible information in subsection (a)(2) at least in partial response to the opinion rendered by the United States Court of Appeals for the Tenth Circuit in *United States v. Brown*.[9] That opinion held that the provisions of 18 U.S.C. § 2314, relating to interstate transportation of stolen property, do

---

6. 18 U.S.C. § 1030 (Supp. II 2002).
7. 132 CONG. REC. H3275, H3278 (daily ed. June 3, 1986) (statement of Rep. Rodino).
8. S. REP. NO. 99-432, at 6-7 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2484.
9. Computer Crime & Intellectual Prop. Section, U.S. Dep't of Justice Criminal Div., *Legislative Analysis of the 1996 National Information Infrastructure Protection Act*, 2 ELECTRONIC INFO. POL'Y & L. REP. 240, 240 (1997), *available at* http://www.usdoj.gov/criminal/cybercrime/1030_anal.html.

not cover intangible property such as data stored on an electronic format.[10]

In its 1986 amendments, Congress added subsection (a)(5), which was intended to further protect data from theft or sabotage: "The new subsection 1030(a)(5) to be created by the bill is designed to penalize those who intentionally alter, damage, or destroy certain computerized data belonging to another."[11] In 1996, Congress also revised the definition of damage to specifically include a broad range of harm that befalls the data of a computer system. Damage was defined as: "any impairment to the integrity or availability of data, a program, a system, or information that,—(A) causes loss aggregating at least $5,000 in value during any 1-year period to one in one or more individuals."[12] However, these damages are limited to economic damages.[13]

The full impact of this congressional concept or intent has been constrained by judicial interpretation. Some courts have denied plaintiffs' claims for losses in value of their data.[14] It seems difficult to achieve the deterrent effect that Congress envisioned for the protection of data files and programming with the advent of liability to civil claims without taking into account the loss in value of the data or programming. Intellectual property cannot be adequately protected unless copying is deterred. In particular, Congress's specific inclusion of observing data in the definition of "obtaining data" would be totally superfluous without allowing for the change in the economic value of the data, if any, to be included as damage or loss.

In the related area of mail fraud, the United States Supreme Court spoke of the need to protect such intangible property rights:

> Here, the object of the scheme was to take the Journal's confidential business information—the publication schedule and contents of the "Heard" column—and its intangible nature does not make it any less "property" protected by the mail and wire fraud statutes. *McNally* did not limit the scope of § 1341 to tangible as distinguished from intangible property rights.[15]

---

10. United States v. Brown, 925 F.2d 1301, 1308 (10th Cir. 1991).

11. S. REP. NO. 99-432, at 10 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2488.

12. National Information Infrastructure Protection Act of 1996, sec. 201, § 1030(e)(8), 110 Stat. 3491, 3493 (1996).

13. *Id.*

14. Moulton v. VC3, No. 1:00CV434-TWT, 2000 WL 33310901, at *6 (N.D. Ga. Nov. 7, 2000).

15. Carpenter v. United States, 484 U.S. 19, 25 (1987).

The Court's view of the law in general, however, does not override the statute's minimum, but rather it should encourage courts to admit evidence of damages and losses that are somewhat more intangible.

2. Unauthorized Access

The meaning of "unauthorized access," a necessary element under almost all of the alternative claims provided under subsections (a)(1) through (a)(7), has been developed by case law. The term is generally used to imply "virtual trespassing" within the context of the accessor's intended use for the data obtained by the access. Whether an act exceeds authorized access is subject to the change in the defendant's relationship with the owner of the protected computer and to the defendant's intended end use for the data accessed.[16] Therefore, the executive in charge of a company's information system would not have authorized access for an unauthorized end use or purpose. Similarly, a subscriber to an Internet service is not authorized to access the Internet Web site to pursue activities outside the site's terms of use.[17] At times, courts rely on existing employment or confidentiality agreements to preclude uses that would breach confidentiality, or on the fact that an employee is deemed to have lost authorization when he switches his loyalty to an alternative employer or principal.[18] Thus, an IRS agent who views the tax returns of acquaintances or an employer that reads an employee's personal e-mail file for evidence of correspondence with minors are relieved of any civil liability for their clear violations of privacy because the economic loss to the plaintiffs is not significant.[19]

Courts are sensitive to sudden changes in the defendant's authorization. Thus, if a current employee redirects his loyalties to a competitor, his prior authorization from his existing employer is deemed

16. *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582-83 (1st Cir. 2001).

17. *See* EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 63 (1st Cir. 2003) (rejecting the district court's notion that any party visiting a Web site without appropriate advisory language should have the reasonable expectations that the owner of the Web site does not give the visitor authority to harvest data from the site).

18. It is unnecessary to go to such lengths to prove that an employee's access was unauthorized in such circumstances. Plaintiffs might consider asserting the federal common law fiduciary duty of an employee to protect the confidentiality of the employer's data and documents as voiced by the United States Supreme Court. *See Carpenter*, 484 U.S. at 27 (quoting Snepp v. United States, 444 U.S. 507, 515 n.11 (1980) (per curiam) ("[E]ven in the absence of a written contract, an employee has a fiduciary obligation to protect confidential information obtained during the course of his employment.")).

19. *See* United States v. Czubinski, 106 F.3d 1069, 1078 (1st Cir. 1997); Fischer v. Mt. Olive Lutheran Church, 207 F. Supp. 2d 914, 926-27 (W.D. Wis. 2002). *But see In re* Toys R Us, Inc., Privacy Litig. No. 00-CV-2746, 2001 WL 34517252, at *9-12 (N.D. Cal. Oct. 9, 2001).

to have been effectively revoked.[20] This can also, however, work to the benefit of the defendant who accesses the computer before his authorization is deemed to have changed. In such a case, even where the defendant subsequently utilizes the accessed information after the change in authority, he is not liable for a claim under the CFAA.[21] Authorization is determined at the time the computer is accessed.

3. CFAA's "Fraud" Requirement

In constructing the CFAA, Congress borrowed a broad interpretation of "fraud" from the federal statutes on mail and wire fraud,[22] yet it intended that the protected computer have a close connection to the fraud alleged. The CFAA requires that the role of the computer in defendant's alleged actions be significant, not just tangential, to the defendant's obtaining or harming computer files that are used in an overall scheme or "fraud." Thus, the mere theft of computer hardware that has no specific data files does not fall under the statute. Furthermore, recent opinions have interpreted the statute to not require that the plaintiff own the computer that has been accessed;[23] ownership of the files is sufficient.

The term "fraud" is not used in five of the seven alternative subsections, namely subsections (a)(1), (a)(2), (a)(3), (a)(5), and (a)(7). For the remaining two subsections, (a)(4) and (a)(6), "fraud" has been interpreted to mean a course of wrongdoing that does not require the common law elements of fraud. Thus, the *Shurgard* court held that the plaintiff stated a claim when he alleged that "the defendant participated

---

20. *See* Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000) (quoting RESTATEMENT (SECOND) OF AGENCY § 112 (1958) ("Unless otherwise agreed, the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal.")).

21. *See* LeBlanc v. Allstate Ins. Co., No. 99-2724, 2000 U.S. Dist. LEXIS 9351, at *8 (E.D. La. June 22, 2000) ("That is, even if Allstate used the reports in litigation, Allstate could not have intentionally exceeded its authorization at the time the databases were accessed. Plaintiffs therefore cannot establish that Allstate intentionally . . . obtained information without authorization."); *see also* Edge v. Prof'l Claims Bureau, Inc., 64 F. Supp. 2d 115, 118 (E.D.N.Y. 1999), *aff'd without published opinion*, 234 F.3d 1261 (2d Cir. 2000).

22. Pac. Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1194-95 (E.D. Wash. 2003) (citing Deborah F. Buckman, Annotation, *Validity, Construction, and Application of Computer Fraud and Abuse Act (18 U.S.C.A. § 1030)*, 174 A.L.R. FED. 101, 112 (2001)).

23. Theofel v. Farey Jones, 341 F.3d 978, 986 (9th Cir. 2003); *see* Nexans Wires S.A. v. Sark-USA, Inc., 319 F. Supp. 2d 468, 472 (S.D.N.Y. 2004).

in dishonest methods to obtain the plaintiff's secret information" under subsection (a)(4).[24]

One of the more unusual claims under the statute demonstrates these principles in a case against a lawyer for abusive discovery tactics. The United States Court of Appeals for the Ninth Circuit reversed a district court which held that a plaintiff that did not own the computer could not, as a matter of law, state a claim under the statute.[25] The defendant sent a subpoena, unapproved by the court, to a fact witness for the production of various computer files existing on that witness' computer.[26] The subpoena was later held to have overreached for such production and the defendant was sanctioned by the trial court.[27] The owners of the files, unaffiliated with the fact witness, filed a claim under the CFAA against the defendant which sent the subpoena.[28] The Ninth Circuit held that a computer had been accessed without appropriate authority and files had been obtained, reversing the district court's holding that causes of action can only be brought by owners of a computer.[29]

4. What Is an "Act"?

One of the more difficult issues for a prosecutor or plaintiff to determine can be how to distinguish the various acts of the defendant and how at least one of the acts must be shown to have caused damages or losses of at least $5000.[30] Defendants in cases relating to Internet "cookies" have been especially successful in attacking the opposing side's inability to either distinguish acts or show how one seemingly

---

24. *Shurgard Storage*, 119 F. Supp. 2d at 1125-26 ("CFAA's use of 'fraud' simply means wrongdoing and not proof of the common law elements of fraud."); *see Carpenter*, 484 U.S. at 27 ("As we observed last Term in *McNally*, the words 'to defraud' in the mail fraud statute have the 'common understanding' of 'wronging one in his property rights by dishonest methods or schemes,' and "'usually signify the deprivation of something of value by trick, deceit, chicane or overreaching.'" . . . The concept of 'fraud' includes the act of embezzlement, which is '"the fraudulent appropriation to one's own use of the money or goods entrusted to one's care by another."'" (quoting Grin v. Shine, 187 U.S. 181, 189 (1902))); *see also* S. REP. NO. 99-432, at 9 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2483-87 (asserting that subsection (a)(4) was intended to "penalize thefts of property via computer that occur as part of a scheme to defraud").

25. *Theofel*, 341 F.3d at 986.

26. *Id.*

27. *Id.*

28. *Id.* at 978, 986.

29. *Id.*; *see* Shaw v. Toshiba Am. Info. Sys., Inc. 91 F. Supp. 2d 926, 938 (E.D. Tex. 1999) ("It is unnecessary for someone to *lack* a computer in order to be a 'potential purchaser' of one. Similarly, it is not necessary for someone to actually *own* a defective computer in order to experience continuing, adverse effects from it.").

30. *See* Thurmond v. Compaq Computer Corp., 171 F. Supp. 2d 667, 679-81 (E.D. Tex. 2001).

minor act caused the requisite amount of damages. The results of a single act, however, can be added together for all plaintiffs and for the period of one year as described by the 1986 Senate Report:

> Certain types of malicious mischief may cause smaller amounts of damage to numerous individuals, and thereby collectively create a loss of more than $1,000. By using "one or more others," the Committee intends to make clear that losses caused by the same act may be aggregated for purposes of meeting the $1,000 threshold.[31]

There is further support for this view in the 2001 amendments. In those amendments, section (a)(5) was largely reorganized and combined with parts of subsection (g). The amendment also revised sub-paragraph (a)(5)(B)(i):

> [L]oss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value.[32]

Accordingly, it would seem that Congress intended to allow only prosecutors to include the damages of separate but related acts.

In at least two cases relating to computer "cookies," defendants succeeded in convincing the court to focus the analysis on damage done to the "micro" level:

> It is undisputed that each time a web page sends a message to a user's computer instructing the computer to communicate the contents of the cookie on the user's hard drive with Avenue A, it is an individual, singular act. . . . Plaintiffs have not shown any facts that prove an aggregate damage of over $5,000 for any single act of the Defendant, from either the initial placement of an Avenue A cookie or a subsequent accessing of this cookie.[33]

Or:

> One could reasonably argue . . . that DoubleClick commits a violation *each* time it accesses a cookie on a plaintiff's hard drive. However, one could also plausibly maintain that DoubleClick's systematic uploading of data from a cookie on a particular computer's hard drive constitutes a single act of "access," even though it occurs over multiple electronic transactions.[34]

---

31. S. REP. NO. 99-432, at 6 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2482-83, *quoted in In re* Am. Online, Inc. v. Version 5.0 Software Litig., 168 F. Supp. 2d 1359, 1373-74 (S.D. Fla. 2001).

32. *See* 18 U.S.C. § 1030(a)(5)(B)(i) (2000).

33. Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1159 (W.D. Wash. 2001).

34. *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 524 (S.D.N.Y. 2001).

This micro focus has not yet been applied to other types of claims under the CFAA and two other opinions reject the act-by-act perspective.[35] Consider how this one change in perspective could have produced a different conclusion from the United States Court of Appeals for the First Circuit in the *EF Cultural Travel BV v. Explorica, Inc.* opinion.[36] In that case, the defendant was found to have "scraped" more than 60,000 lines of code and data from a competitor's database, especially including detailed pricing information. The circuit court summarized the allegation as follows: "Appellees allege that the appellants knowingly and with intent to defraud accessed the server hosting EF's website more than 30,000 times to obtain proprietary . . . information about appellees' technical abilities."[37] If the scraper robot that invaded the plaintiff's system and transmitted the data back to a competitor had been shown to have transmitted just two lines of code and data per access, and therefore per act, is it likely that the plaintiff could have shown that the loss from any two lines of data would have exceeded $5000?

5. Damage or Loss

There are three types of loss or damage applicable to claims under the CFAA:

(A) The cost of restoring the hardware, programming files or data files to their original condition;
(B) Consequential commercial losses to the plaintiff from impaired access to the hardware or files; and
(C) The loss in market value of the hardware, programming files or data files from the exposure of the data to competitors or the public.[38]

Only the third category of damages is subject to serious debate or disagreement in different jurisdictions.

In 1996, Congress amended the statute to distinguish between damage and loss for the purposes of allowing civil claims.[39] Prior to that time, the statute required a plaintiff to show "damage and loss." In the

35. *In re* Toys R Us, Inc., Privacy Litig., No. 00-CV-2746, 2001 WL 34517252, at *11 (N.D. Cal. Oct. 9, 2001) ("In America Online, the single act recognized by the district court was the defendant's release for distribution of millions of copies of an Internet access product, which, once installed, allegedly caused damage to computers." (citing *In re Am. Online*, 168 F. Supp. 2d at 1373)).

36. 274 F.3d 577, 577 (1st Cir. 2001).

37. *Id.* at 581.

38. Computer Fraud and Abuse Act, 18 U.S.C. § 1030(e)(11) (2000).

39. National Information Infrastructure Protection Act of 1996, Pub. L. No. 104-294, 110 Stat. 3491 (1996).

1996 Amendment, however, Congress specifically recognized that losses or damages should apply for the statutory minimum, i.e., Congress recognized that certain losses to the victims might not be deemed to be "damage" but should still qualify towards the statutory minimum.[40] In its legislative history, Congress acknowledged that "loss" is not limited to the costs of actual repairs but should also include lost computer time, the costs of reprogramming, the costs of restoring data, and costs incurred as a result of relying on fraudulently manipulated data.[41] Furthermore, the 1996 Amendment defined "damage" to mean "any impairment to the integrity or availability of data, a program, a system, or information."[42]

In the USA Patriot Act of 2001, Congress added a definition of loss in subsection (e)(11):

> [T]he term "loss" means 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.[43]

The Department of Justice regards this amendment as signifying Congress's adoption of the definition of "loss" rendered by the Ninth Circuit in *United States v. Middleton*,[44] but the legislative history reflects no such specific intent.

While it must be acknowledged that no specific Conference Report specifically discussed the exact issue, it seems inescapable that Congress intended that the term "loss" should include the loss in value of the data due to the unauthorized access. Congress has firmly stated that the statute aims to treat computer data as property and prevent even the observation of computer data. The seriousness of the violation varies with the value of the data and damages should be construed with a view

---

40. Arguably, in such a situation, neither the computer nor its information is damaged. Nonetheless, this conduct allows the intruder to accumulate valid user passwords to the system, requires all system users to change their passwords, and requires the system administrator to devote resources to resecuring the system. Thus, although there is arguably no "damage," the victim does suffer "loss." If the loss to the victim meets the required monetary threshold, the conduct should be criminal, and the victim should be entitled to relief. S. REP. NO. 104-357, at 9 (1996).

41. "[U]sers of computer services might incur substantial costs as a result of relying on information contained in a database that has been tampered with." S. REP. NO. 99-432, at 11-12 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2488-89.

42. *See* S. REP. NO. 104-357 (1996), *as reprinted in* 1996 U.S.C.C.A.N. 3491, 3493.

43. 18 U.S.C. § 1030(e)(11).

44. 231 F.3d. 1207, 1213 (9th Cir. 2000); *see* Computer Crime & Intellectual Prop. Section, U.S. Dep't of Justice Criminal Div., *Field Guidance on New Authorities that Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001*, http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm (last visited Apr. 8, 2006).

to the harms that the statute attempts to prevent.[45] Clearly, "loss" must include the loss in value of the data due to the access and use of the data.[46]

In *Carpenter v. United States*, the Supreme Court suggested that there may be a useful distinction between monetary loss and economic loss:

> Petitioners' arguments that they did not interfere with the Journal's use of the information or did not publicize it and deprive the Journal of the first public use of it, see Reply Brief for Petitioners 6, miss the point. The confidential information was generated from the business, and the business had a right to decide how to use it prior to disclosing it to the public. Petitioners cannot successfully contend based on *Associated Press* that a scheme to defraud requires a monetary loss, such as giving the information to a competitor; it is sufficient that the Journal has been deprived of its right to exclusive use of the information, for exclusivity is an important aspect of confidential business information and most private property for that matter.[47]

If the concept is transferable, it could be established that the loss in value of the data files is not a monetary loss, but should still be considered an economic loss for the same reasons cited in *Carpenter*.

C. Minimum Damage Amounts Separate Pranksters from Criminals

Even in its earliest form, the CFAA was always about more than protecting national security.[48] Protected computer information always included customer records of large financial institutions.[49] The Senate Report for the 1986 amendments makes it clear that subsection (a)(2) of the statute was drafted for the purpose of protecting privacy:

> The premise of 18 U.S.C. § 1030(a)(2) will remain the protection, for privacy reasons, of computerized credit records and computerized information relating to customers' relationships with financial institutions. . . . Because the premise of this subsection is privacy

---

45. Rather than providing a list of prohibited actions and risk being under inclusive, the statute focuses instead on "the harm that the law seeks to prevent." S. REP. NO. 104-357, at 9 (1996).

46. The seriousness of a breach in confidentiality depends, in considerable part, on the value of the information taken, or on what is planned for the information after it is obtained. Thus, the statutory penalties are structured to provide that obtaining information is only a misdemeanor, but obtaining valuable information, or misusing information in other more serious ways, is a felony. *Id.* at 6.

47. 484 U.S. 19, 26-27 (1987).

48. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213, 1213 (codified as amended at 18 U.S.C. § 1030 (2000)).

49. *Id.*

> protection, the Committee wishes to make clear that "obtaining information" in this context includes mere observation of the data.[50]

The coverage of the statute and the definition of protected computers changed as it became common for individuals to own their own computers at home. The National Information Infrastructure Protection Act of 1996 (NII) indicates that Congress's commitment to privacy has, if anything, increased.[51] As noted in the commentary to the Draft Principles, "the NII will only achieve its full potential if individual privacy is properly protected."[52]

The statute's goal of protecting privacy can be outweighed by a competing congressional concern that the application of the statute must not ignore the essential difference between prank and crime or trespass and sabotage. Thus, a statutory minimum was established for criminal or civil claims which was raised from $1000 to $5000. More importantly, the relevant measure for civil claims is restricted to economic losses.[53] As long as the statute is intended to assess the seriousness of a breach of confidentiality on the basis of the commercial or "economic" value of the information obtained,[54] most civil claims under this statute for invasion of personal privacy will be dismissed. Thus, the plaintiff survived the defendant's motion to dismiss or for summary judgment in only one of the eight civil cases relating to invasion of privacy.

1. CFAA Case Law Table 1 and Table 2

Table 1 lists the principal case opinions relating to the CFAA. For some cases, two opinions are reported separately to distinguish the issues. In the hope that one chart can save a long detailed recounting of specific issues, various quotes and comments are provided in Table 1,

---

50. S. REP. NO. 99-432, at 6 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2484.

51. National Information Infrastructure Protection Act of 1996, Pub. L. No. 104-294, 110 Stat. 3941 (1996).

52. Draft Principles for Providing and Using Personal Information, 56 Fed. Reg. 27,206-207 (May 25, 1994).

53. National Information Infrastructure Protection Act, 110 Stat. at 3491. In passing it may be interesting to note that the tort claim of trespass to chattel depends on the plaintiff showing damage to the chattel. "Intel's claim fails not because e-mail transmitted through the Internet enjoys unique immunity, but because the trespass to chattels tort—unlike the causes of action just mentioned—may not, in California, be proved without evidence of an injury to the plaintiff's personal property or legal interest therein." Intel Corp. v. Hamidi, 71 P.3d 296, 299 (Cal. 2003).

54. Those who improperly use computers to obtain other types of information—such as financial records, nonclassified government information, and information of nominal value from private individuals or companies—face only misdemeanor penalties, unless the information is used for commercial advantage, private financial gain or to commit any criminal or tortuous act. National Information Infrastructure Protection Act, 110 Stat. at 3492.

Part B in regard to specific subsections of the statute. Furthermore, the statute has been frequently amended and the court's opinion as to an act committed prior to the effectiveness of the amendment may already be out of date. Table 2 lists eight criminal cases and two cases related to trespass to chattel, which may be used as an alternative route instead of the CFAA. The criminal cases are added to provide special holdings and are not intended to be representative of the entire group of criminal cases.[55] (Please note that damage calculations in criminal trials are influenced more by the Sentencing Guidelines, which may differ from the definitions of the statute.)

Cases are categorized between the following substantive categories: cookies, hacking—invasion of privacy, hacking—sabotage, product liability, scraping and sending unsolicited bulk e-mails (UBE or spam). For information regarding the relative frequency or the financial impact of "cyber-crime," see the annual survey conducted by the FBI and the Computer Security Institute.[56]

Table 1, below, summarizes Exhibit 1 and shows that on a statistical basis, the prevailing party to the opinion greatly varies by the primary reason for the opinion and the nature of the complaint. It shows that the defendant prevailed in the opinion about two thirds of the time when damages was the primary issue, but that the plaintiff prevailed two thirds of the time when an issue other than damages was the primary reason for the opinion. The defendant generally prevails on complaints like cookies, hacking or product liability. The plaintiff generally prevails on complaints like scraping and spam.

Table 1
Summary of CFAA Case Law: Prevailing Party By Complaint

Count of Opinions		Prevailing Party		
Primary Reason	Complaint	D	P	Grand Total
Damages	Cookies	4	1	5
	Hacking—Invasion Privacy	4	1	5
	Hacking—Sabotage	3	1	4
	Product Liability	3	0	3
	Scraping	5	4	9
	UBE	2	3	5

55. An extensive list of criminal cases (whose representativeness of the entire case population at large is unknown) is available online. *See* Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice Home Page, http://www.cybercrime.gov (last visited Apr. 8, 2006).

56. *See id.*

Count of Opinions		Prevailing Party		
Primary Reason	Complaint	D	P	Grand Total
Damages Total		21	10	31
Other	Hacking—Invasion Privacy	3	0	3
	Hacking—Sabotage	0	2	2
	Product Liability	0	1	1
	Scraping	1	7	8
	UBE	2	3	5
Other Total		6	13	19
Grand Total		27	23	50

Table 2, below, summarizes the case law by the effective outcome of the opinion. About thirty-three of these opinions relate to motions to dismiss or for summary judgment. The plaintiff only prevailed in nine of these opinions and it seems likely that the plaintiff won a jury verdict in even fewer cases. In thirteen of the cases, injunctions sought by the plaintiff were obtained in all but two.

Table 2
Summary of CFAA Case Law: Prevailing Party by Outcome

Count of Opinions		Prevailing Party		
Primary Reason	Outcome	D	P	Grand Total
Damages	Injunction	0	4	4
	No injunction	2	0	2
	Judgment	1	3	4
	No trial	13	0	13
	Trial	5	3	8
Damages Total		21	10	31
Other	Injunction	0	6	6
	Judgment	0	1	1
	No trial	5	0	5
	Trial	1	6	7
Other Total		6	13	19
Grand Total		27	23	50

Cookies. While there is more than one way to technically accomplish the result, cookies are attached to the host computer of a visitor to a Web site and enable the owner of the Web site to both track subsequent activities of the visitor on the Internet and to gather certain information from the visitor's computer. The key issue in this subset of the case law is that most plaintiffs fail to satisfy the damages requirement of 1030(g) when defendants persuade the court to require that damages be distinguished per wrongful act of the defendant. For the purposes of civil claims, damages are allowed to be summed over one year of time

and over multiple plaintiffs but only based on each act of the defendant.[57] Only prosecutors are now allowed to also sum all damages from all of the defendant's related acts for 1030(a)(5)(B)(I). So far, the defendant has prevailed in four of five cases. As security software simplifies one's ability to exclude some or all cookies, plaintiffs will also probably encounter increasing difficulty in establishing that the "cookies" made unauthorized access.

Hacking—Invasion of Privacy. These cases generally include actions of the defendant to access a computer system without authorization or in excess of prescribed authority. Frequently, courts find defendants have satisfied all elements of a claim under the CFAA, except that either the plaintiff fails to state a case for damages or the court finds that the basis for the plaintiff's damages (loss of personal information, loss of privacy) must be excluded and the claim must be dismissed. This trend appears likely to continue because it is difficult for a private individual (unrelated to a business activity) to show economic damages of at least $5000 unless the number of plaintiffs is very large. Various theories of loss of privacy or the opportunity cost of lost fees for the information have not succeeded.[58] The defendant has prevailed in seven of eight cases.

Hacking—Sabotage. This group of cases includes intentional acts to access a computer without authorization and cause damage to the computer or its files. Note that for some of the causes of action, the mens rea requirement does not necessarily apply to the damage element but rather only to the intent to access the system without authorization element. However, within this group of cases, the sabotage is generally substantial and usually the intentional act of a disgruntled employee. The defendant has prevailed in three of six cases.

Product Liability. These are claims against manufacturers for knowingly distributing defective hardware (generally a floppy drive

---

57. There are two versions of this perspective: that the plaintiff must show damages of $5000 for each wrongful act of the defendant or that the plaintiff must show damages of $5000 for at least one wrongful act of the defendant.

58. One possibility exists of trying restitution or unjust enrichment. Consider this dicta from the *Carpenter* opinion:

> As the New York courts have recognized: "It is well established, as a general proposition, that a person who acquires special knowledge or information by virtue of a confidential or fiduciary relationship with another is not free to exploit that knowledge or information for his own personal benefit but must account to his principal for any profits derived therefrom." *Diamond v. Oreamuno*, 24 N.Y. 2d 494, 497, 248 N.E.2d 910, 912 (1969); *see also* RESTATEMENT (SECOND) OF AGENCY § 388, cmt. c (1958).

Carpenter v. United States, 484 U.S. 19, 27-28 (1987).

controller) that can transmit harmful signals to the host computer. These cases established that the transmission element in subsection (a)(5)(A) can be liberally interpreted to include almost any kind of transmission, including transmission by the distribution of disks to update a computer. The amendment in 2001 has practically eliminated any further claims for product liability under the CFAA by prohibiting such claims in subsection (g): "No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware."[59] Defendants have succeeded in three of four cases.[60]

Scraping. This group ranges from the simple act of accessing a keyboard and downloading data on a disk to more elaborate schemes of competitors to infiltrate the computer system of their rivals with a "robot scraper" that transmits commercial data to an employee (present or former) and/or an existing competitor. Of significant note is the United States Court of Appeals for the First Circuit's opinion in a second case relating to EF Cultural Travel. Even though the district court's injunction was affirmed, the First Circuit was unwilling to affirm the district court's conclusion that any visitor to a Web site lacks the authorization to scrape the Web site for data absent specific notice on the Web site.[61] Plaintiffs have prevailed in eleven of seventeen cases.

Unsolicited Bulk E-mail (UBE).[62] These cases relate to the practice of sending large numbers of unsolicited e-mails (or spam), generally for commercial gain. Fundamentally, such a practice is little different from advertising circulars that are generically distributed through the U.S. postal system or even solicitation phone calls. (For cases in which the defendant accesses a system to obtain a file of e-mail addresses and then sends them spam, the claim is classified as scraping.) As to commercial e-mail, the California Supreme Court has provided dicta to indicate that there is no First Amendment right for an individual to send large amounts of e-mail to all of the employees in a company on that company's server.[63] In relation to the plaintiff's claim for trespass to chattel, the court in that

---

59. 18 U.S.C. § 1030(e)(8) (2000).

60. *Id.* § 1030(g).

61. EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62 (1st Cir. 2003).

62. For a thorough discussion of venue issues in spam cases, see *Verizon Online Services, Inc. v. Ralsky*, 203 F. Supp. 2d 601 (E.D. Va. 2002).

63. Intel Corp. v. Hamidi, 71 P.3d 296, 311-12 (Cal. 2003); *see also* Cyber Promotions, Inc. v. Am. Online, Inc., 948 F. Supp. 436, 456 (E.D. Pa. 1996) ("Put another way, the First Amendment does not prevent AOL from using its Preferred Mail System to protect its private property rights by blocking Cyber's mass e-mail advertisements from clogging AOL's system and damaging AOL's reputation while at the same time not receiving any compensation whatsoever from Cyber.").

case held that the plaintiff could not claim damages for the cost or value of the employees' time that the employer lost from the distraction. Defendants have prevailed in six of ten cases.[64]

2. Review of Damage Case Law by Statutory Subsection

The statute did not provide for civil claims until the amendments of 1990 and that may account for the slow development of "damages" and "loss" in the early years. The initial Conference Report for the 1984 statute states that the minimum loss or damage could be met by loss to the plaintiff or benefit to the defendant.[65] This appears to be an isolated remark as there are not other references to such an equivalency.[66]

Some of the statute's subsections overlap and a given set of facts could be (and have been) claimed under multiple sub-sections. For commercial cases in particular, subsections (a)(2)(C), (a)(4), and (a)(5)(A)(iii) may sometimes appear interchangeable for certain groups of case facts. There are some distinctions between the three: (a)(2)(C) requires the use of an interstate or foreign communication; (a)(4) requires intent to defraud; and (a)(5)(A)(iii) is sometimes misinterpreted to require damage to the protected computer.

Cases relating to subsection (a)(2) are divided on two specific issues. Two of three cases have held that the value of the plaintiffs' personal information cannot be attributed as a damage or loss.[67] Five different courts have held that diminution in commercial value of the plaintiff's database or losses of goodwill can be included as damage or loss.[68]

In cases related to subsection (a)(4), two opinions have allowed the inclusion of damage or loss from the damages to goodwill or loss of reputation,[69] and two opinions have accepted the inclusion of damage or

---

64. *Intel Corp.*, 71 P.3d at 311-12.

65. H.R. REP. NO. 98-894, at 22 (1984), *as reprinted in* 1984 U.S.C.C.A.N. 1213, 1214.

66. *Id.*

67. *See In re* Double Click Inc. Privacy Litig., 154 F. Supp. 2d 497, 525 (S.D.N.Y. 2001); Fischer v. Mt. Olive Lutheran Church, 207 F. Supp. 2d 914, 926 (W.D. Wis. 2002). *But see In re* Toys R Us, Inc., Privacy Litig., No. 00-CV-2746, 2001 WL 34517252, at *11-12 (N.D. Cal. 2001).

68. Physicians Interactive v. Lathian Sys. Inc., No. CA-03-1193-A, 2003 U.S. Dist. LEXIS 22868, at *19 (E.D. Va. Dec. 5, 2003); Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1273 (N.D. Iowa 2000); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1127 (W.D. Wash. 2000); Register.com v. Verio, Inc., 126 F. Supp. 2d 238, 252 (S.D.N.Y. 2000); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 451 (E.D. Va. 1998).

69. See the holding in *In re America Online*, 168 F. Supp. 2d 1359, 1380 (S.D. Fla. 2001), and the dicta in *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 584 (1st Cir. 2001).

loss from a decline in the value of the plaintiff's data or information.[70] However, one opinion rejected the notion that damages or loss could result from an errant IRS agent viewing the tax returns of various individuals for his own personal entertainment.[71]

It is useful to remember Congress's original intent for this subsection:

> The acts of fraud we are addressing in proposed section 1030(a)(4) are essentially thefts in which someone uses a federal interest computer to wrongly obtain something of value from another. . . . Proposed section 1030(a)(4) is intended to reflect the distinction between the theft of information, a felony, and mere unauthorized access, a misdemeanor.[72]

For the purposes of criminal prosecution, the value of the information wrongfully obtained is used to distinguish between a felony and a misdemeanor. Accordingly, the loss in economic value of the information that results from the wrongful "obtaining" must be relevant for civil purposes.

In the legislative history section of the National Information Infrastructure Protection Act of 1996, Senator Hatch makes it clear that subsection (a)(4) is intended to include computer abuses as simple as a significant use of the host computer:

> This provision contains a "computer use" exception that exempts fraudulent conduct to obtain only the use of the computer. While every trespass in a computer should not be converted into a felony scheme to defraud, a blanket exception for "computer use" is too broad. Hackers, for example, have broken into Cray supercomputers for the purpose of running password cracking programs, sometimes amassing computer time worth far more than $5,000. In light of the large expense to the victim caused by some of these trespassing incidents, the amendment would limit the "computer use" exception to cases where the stolen computer use involved less than $5,000 during any one-year period.[73]

Inexplicably, a federal district court in Minnesota opined that a civil claim cannot be made under this subsection.[74] There is abundant case law and legislative history to the contrary, and the Minnesota court appears to have fallen into the common misunderstanding that all civil

---

70. *See Physicians Interactive*, 2003 U.S. Dist. LEXIS 22868, at *19; Credentials Plus, LLC v. Calderone, 230 F. Supp. 2d 890, 906 (N.D. Ind. 2002).

71. United States v. Czubinski, 106 F.3d 1069, 1078 (1st Cir. 1997).

72. *Id.* at 1078-79 (quoting 132 Cong. Rec. S4072, S4074 (daily ed. Apr. 10, 1986) (statement of Sen. Laxalt)).

73. S. REP. NO. 104-357, at 6 (1996).

74. McLean v. Mortgage One & Fin. Corp., No. 04-1158 (PAM/JSM), 2004 U.S. Dist. LEXIS 7279, at *5 (D. Minn. Apr. 9, 2004).

claims under the statute must be under subsection (a)(5)(B). A review of the amendments introduced by the USA Patriot Act in 2001 would reveal the fallacy of this conception, one that was recently pointed out by the Northern District of Texas: "A careful reading of the statute shows that a civil plaintiff is not required to state a cause of action pursuant to subsection (a)(5), but merely to allege one of the factors enunciated in subsection (a)(5)(B)."[75]

The major issue for subsection (a)(5)(A) is whether only physical damage and the costs to remediate that damage should be admitted for damages or loss, or whether claims under the subsection should allow a broader group of losses or damage. Only one opinion has allowed the inclusion of lost personalty for the purpose of damages under sub-clause (i).[76] As discussed above, two opinions have indicated that physical damage should only be considered for at least one sub-clause,[77] one opinion holds that physical damage is not required in sub clause (a)(5)(A)(ii),[78] two opinions hold that physical damage is not required in sub-clause (a)(5)(A)(iii),[79] and three opinions hold that physical damage is not required for any of the sub-clauses in (a)(5)(A).[80]

The First Circuit's opinion in *Explorica* held that the definition of damages for subsection (a)(5) needed to include more than just physical damage to the protected computer in order for the statute to remain relevant in the twenty-first century:

> As we move into an increasingly electronic world, the instances of physical damage will likely be fewer while the value to the victim of what has been stolen and the victim's costs in shoring up its security features undoubtedly will loom ever-larger. If we were to restrict the statute as appellants urge, we would flout Congress's intent by effectively permitting the CFAA to

---

75. Sw. Airlines Co. v. Farechase, Inc., 318 F. Supp. 2d 435, 439 (N.D. Tex. 2004).

76. *In re* Toys R Us, Inc., Privacy Litig., No. 00-CV-2746, 2001 WL 34517252, at *11-12 (N.D. Cal. 2001).

77. Am. Online, Inc. v. Nat'l Health Care Disc, Inc., 121 F. Supp. 2d 1255, 1276 (N.D. Iowa 2000) (noting that the legislative history makes clear that under (a)(2)(C), intangible property may be obtained not only by physical theft, but also by "mere observation of the data"); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 251 (S.D.N.Y. 2000) (asserting that damages claimed by plaintiff under (a)(2)(C) are best analyzed under (a)(5)(C), which specifically addresses damages to the computer system).

78. Four Seasons Hotels & Resorts B.V. v. Consorcio Barr, S.A., 267 F. Supp. 2d 1268, 1322-23 (S.D. Fla. 2003).

79. Shurgard Storage Ctrs., Inc., v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1126-27 (W.D. Wash. 2000); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 451 (E.D. Va. 1998).

80. Theofel v. Farey Jones, 341 F.3d 978, 986 (9th Cir. 2003); United States v. Middleton, 231 F.3d 1207, 1211-13 (9th Cir. 2000); *In re Toys R Us*, 2001 WL 34517252, at *10.

> languish in the twentieth century, as violators of the Act move into the twenty-first century and beyond.[81]

Much of this discussion appears to ignore that it was never within the legislative intent for this subsection to be limited to physical damage:

> The computer abuse amendments make it a felony intentionally to cause harm to a computer or the information stored in it by transmitting a computer program or code—including destructive computer viruses—without the knowledge and authorization of the person responsible for the computer attacked. This is broader than existing law, which prohibits intentionally access[ing] a Federal interest computer without authorization, if that causes damage.[82]

Some of the damage decisions have hinged on the plaintiff's methodology in calculating damages. In two cases, the court rejected or encouraged the plaintiff to limit his claimed expenses for the cost of investigating the unauthorized access.[83] Since the plaintiff could not prove any damage from the unauthorized access, the court in *Moulton* rejected the plaintiff's claim for investigative expenses.[84] Similarly, the court in *Tyco* did not dismiss the plaintiff's claim for $136,026.94 of investigative expenses, but it clearly thought the amount disproportionately high and required the plaintiff to review its calculations.[85] The court's opinion in *Thurmond* disallowed any investigative expenses that were incurred for the plaintiff's litigation.[86] Finally, opinions in three criminal cases disagree on what accounting data or methodology is appropriate to calculate remedial costs. The courts in *Middleton*[87] and *Sablan*[88] rejected the defendant's claim that only

---

81. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 585 (1st Cir. 2001); *see also In re* Pharmatrak, Inc., Privacy Litig., 220 F. Supp. 2d 4, 15 (D. Mass. 2002) ("[T]he First Circuit . . . allow[s] recovery for more than purely physical damage.").

82. 139 CONG. REC. S16421, S16422 (daily ed. Nov. 19, 1993) (statement of Sen. Leahy).

83. *Middleton*, 231 F.3d at 1214; Physicians Interactive v. Lathian Sys. Inc., No. CA-03-1193-A, 2003 U.S. Dist. LEXIS 22868, at *19 (E.D. Va. Dec. 5, 2003) (allowing remedial and investigative expenses of $18,750).

84. Moulton v. VC3, No. 1:00CV434-TWT, 2000 WL 33310901, at *6 (N.D. Ga. Nov. 7, 2000).

85. Tyco Int'l (U.S.) Inc. v. John Does, 1-3, No. 01-CV-3856, 2003 WL 23374767, at *3-4 (S.D.N.Y. Aug. 29, 2003).

86. Thurmond v. Compaq Computer Corp., 171 F. Supp. 2d 667, 682-83 (E.D. Tex. 2001).

87. *Middleton*, 231 F.3d at 1213-14 (rejecting defendant's claim that damages must be marginal costs or out of pocket costs).

88. United States v. Sablan, 92 F.3d 865, 869-70 (9th Cir. 1996) (affirming the district court's damage calculation based on "the cost of repairs based upon the bank's standard hourly rate for its employees' time, computer time, and administrative overhead—the same rate that the bank uses in charging paying customers").

marginal or out-of-pocket expenses may be included in the calculation. In another case, however, the judge states in a footnote that he would not have accepted the calculation of lost profits based on daily averages.[89]

A fourth criminal case, relating to the defendant's defrauding the state out of sales proceeds for more than 525,000 lottery tickets, rejected the defendant's claim that damages be calculated on the basis of the state's lost profits.[90] The court ruled that the measure of damages for such fraud was the market value of the lottery tickets on the date of the fraud or one dollar per lottery ticket.[91] Effectively, the victim would have been entitled to not just his lost profits, but his total lost revenue, similar to a remedy of unjust enrichment.[92]

3. Damage Approaches Waiting To Be Explored

In the process of reviewing the statute's legislative history and the relevant case law, it is apparent that plaintiffs or prosecutors may want to consider including some of the following items in their damages pleadings. The legislative history, as noted previously, has made it clear that Congress has expected damages or loss to include the value of lost computer time and reliance damages. For example, courts have established a range of $.00078 to $.001 as the damage or loss from processing an unauthorized e-mail.[93] Lost computer time is based on total allocated costs or the price for which computer time is sold outside the company.

The statute provides for civil claims against the defendant for compensatory damages and equitable relief. While the statute does not detail potential equitable relief, it states no opposition to any type of equitable relief. Based on Supreme Court case law, the absence of a specific restriction authorizes a district court to exercise full jurisdiction over traditional equitable remedies.[94]

---

89. United States v. Pierre-Louis, No. 00-434-CR-GOLD/SIMON, 2002 WL 1268396, at *1 (S.D. Fla. Mar. 22, 2002).

90. United States v. Bae, 250 F.3d 774, 777-78 (D.C. Cir. 2001).

91. *Id.*

92. *Id.*

93. *See* Earthlink, Inc. v. Carmack, No. 1:02-CV-3041-TWT, 2003 U.S. Dist. LEXIS 9963, at *15 (N.D. Ga. May 7, 2003); Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1262 (N.D. Iowa 2000).

94. For jurisdiction, see *Mitchell v. Robert DeMario Jewelry, Inc.*, 361 U.S. 288, 290-91 (1960), and *Porter v. Warner Holding Co.*, 328 U.S. 395, 398 (1946). For traditional equitable remedies, see *Grupo Mexicano de Desarrollo, S.A. v. Alliance Bond Fund, Inc.*, 527 U.S. 308, 318 (1999). For a discussion of equitable remedies, see *Great-West Life & Annuity Ins. Co. v. Knudson*, 534 U.S. 204, 216-17 (2002).

Compared to suing for damages, suing for unjust enrichment can offer certain advantages. Even in cases where the plaintiff's damages are approximately equal to the defendant's unjust enrichment, the equitable monetary remedy can offer procedural advantages. These advantages require that the defendant carry the burden of proof for his expenses, and an award of a constructive trust can offer senior priority to the plaintiff as a creditor against the defendant. In cases where the defendant's unjust enrichment exceeds the plaintiff's losses, the plaintiff is entitled to the defendant's gain. Perhaps the biggest disadvantage is that equitable remedies are not well understood by attorneys or the judiciary.

At times, electing an equitable remedy or equitable cause of action permits a tactical plaintiff to avoid disadvantageous provisions regarding such procedural issues as statutes of limitations or jurisdiction. In the case of the CFAA, there appears to be no opportunity to take advantage of the distinction between damages and equitable relief that is sometimes very significant. Subsection (g) of section 1030 distinguishes claims as "civil actions" that include either claims for damages or equitable relief. Therefore the choice of remedy will not relieve the plaintiff of the minimum requirement for damages.[95]

> (g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.[96]

II. VICARIOUS LIABILITY

Plaintiffs are increasingly making claims under the CFAA against former employees and/or competitors for accessing commercial data to compete with the plaintiff. A number of opinions have considered the claims directly and find such applications of the CFAA within the

95. *See supra* note 58 and accompanying text.
96. 18 U.S.C. § 1030(g) (2000).

legislative intent of Congress.[97] In cases when the plaintiff makes a claim against both the ex-employee and a competitor, key questions of vicarious liability arise regarding the competitor's liability.

To date, few opinions have addressed vicarious liability as a matter of law. In two cases, plaintiffs have alleged vicarious liability based on strained case facts which the courts easily rejected on the factual basis alone and in which dicta indicates that the courts appear receptive in theory to such claims.[98] In addition, plaintiffs have prevailed in cases that included claims of vicarious liability that were not addressed as matters of law. Dicta again supports the feasibility of such a claim based on the courts' impression that claims under the CFAA should be regarded as normal business torts.[99] Thus far, only the opinion in *Physicians Interactive* has considered a claim of vicarious liability as a matter of law where the court refused to dismiss the claim, stating that liability was possible based upon respondeat superior.[100]

The Southern District of New York rejected a defendant's attempt to argue that the CFAA was not intended to apply to claims of vicarious liability and offered the opinion in *Doe v. Dartmouth-Hitchcock Medical Center* as support for this view. The court eventually granted the defendant's motion for summary judgment, but on grounds of damages as a matter of law after it quickly dismissed the defendant's argument.[101]

The factual basis of two cases draws an important distinction for vicarious liability, one being the role of the defendant's employer or principal in the defendant's activities. In situations where it appeared that the unauthorized access was facilitated by or in the interest of the defendant's employer, vicarious liability has been found to exist or to be possible.[102] However, in situations where the defendant's employer was

---

97. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 577 (1st Cir. 2001); *see* YourNetDating, LLC v. Mitchell, 88 F. Supp. 2d 870, 872 (N.D. I11. 2000); Pac. Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1196 (E.D. Wash. 2003) (citing Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1126 (W.D. Wash. 2000)).

98. *See* Role Models Am., Inc. v. Jones, Inc., 305 F. Supp. 2d 564, 567 (D. Md. 2004); Doe v. Dartmouth-Hitchcock Med. Ctr., No. 00-100-M, 2001 U.S. Dist. LEXIS 10704, at *11-16 (D.N.H. July 19, 2001) (unpublished opinion).

99. *Role Models Am.*, 305 F. Supp. 2d at 567.

100. Physicians Interactive v. Lathian Sys. Inc., No. CA-03-1193-A, 2003 U.S. Dist. LEXIS 22868, at *27-29 (E.D. Va. Dec. 5, 2003).

101. Nexans Wires S.A. v. Sark-USA, Inc., 319 F. Supp. 2d 468, 472 (S.D.N.Y. 2004).

102. In addition, federal common law should normally be assumed to apply as the statute says nothing to preclude federal common law or vicarious liability normally found under federal common law. *See* Meyer v. Holley, 537 U.S. 280, 285 (2003) ("And the Court has assumed that, when Congress creates a tort action, it legislates against a legal background of ordinary tort-related vicarious liability rules and consequently intends its legislation to incorporate those

harmed by the unauthorized access, the defendant's employer has been excluded as a defendant.

III. CONCLUSIONS: CONSIDER DAMAGES EARLY

Given the variety of possible claims, the frequent amendments made by Congress, and the differentiation between some of the claims, this statute is not easily generalized. Any precedent needs to be understood in relation to the applicable language of the statute at that date, the particular subsection of the statute, and the nature of the defendant's actions.

Given that understanding, claims can be successfully made under the CFAA relating to the access or misappropriation of data files. Cases involving claims of "faithless" employees or unfair competitors are now commonplace. On the other hand, prospects for claims of invasion of personal privacy are unlikely to reach a jury, absent some legislative changes. To date, defendants' most successful response has been to challenge plaintiffs' damages claims as a matter of law.

Finally, claimants under the CFAA which ignore or postpone consideration of damage issues early in a case risk the peril of dismissal or summary judgment. Damages strategy needs to be determined early in the case and only after a close review of the statute and its case law.

Until Congress significantly revises the definition of admissible damage beyond commercial measures, perhaps at the risk of including pranksters, plaintiffs for claims of invasion of privacy or relating to "cookies" are well-advised to reconsider a suit based solely on that claim.

---

rules."); United States v. Texas, 507 U.S. 529, 534 (1993) ("In order to abrogate a common-law principle, the statute must 'speak directly' to the question addressed by the common law.").