

# THE JOHN MARSHALL REVIEW OF INTELLECTUAL PROPERTY LAW



## THE COMPUTER FRAUD AND ABUSE ACT: A VEHICLE FOR LITIGATING TRADE SECRETS IN FEDERAL COURT

GRAHAM M. LICCARDI

### ABSTRACT

Federal jurisdictions are split on the reach of the Computer Fraud and Abuse Act (“CFAA”) in situations where computer-stored trade secrets are stolen by former employees who possessed authorization to access and use the trade secret information. This comment explores both the broad and narrow interpretations of the CFAA. It proposes that courts adopt the broad interpretation, which includes principles of agency law, in order to determine when an employee is “without authorization” under the CFAA. Courts should also adopt the broad interpretation in situations where trade secrets are stolen because an employee is only granted a “limited license” to use and access a trade secret, which defines the parameters of the employee’s authorization. This comment also identifies three different perspectives regarding the inclusion of trade secret misappropriation within the CFAA definition of “damage.” Ultimately, trade secret misappropriation should be included within the statutory definition of “damage” because the secrecy of trade secret information, and its “integrity,” is impaired with every disclosure.

Copyright © 2008 The John Marshall Law School



*Cite as* Graham M. Liccardi, *The Computer Fraud and Abuse Act: A Vehicle for Litigating Trade Secrets in Federal Court*, 8 J. MARSHALL REV. INTELL. PROP. L. 155 (2008).

# THE COMPUTER FRAUD AND ABUSE ACT: A VEHICLE FOR LITIGATING TRADE SECRETS IN FEDERAL COURT

GRAHAM M. LICCARDI\*

## INTRODUCTION

In September of 2003, Former FBI Director Robert Mueller stated that U.S. businesses are losing more than \$200 billion dollars annually from theft of intellectual property.<sup>1</sup> These losses can be attributed to economic espionage, internal employee theft, and outside hacking of computer networks.<sup>2</sup> This should be a concern for any business because it is estimated that 80% of assets in an information-based economy are intangible.<sup>3</sup> Indeed, most are also trade secrets.<sup>4</sup> With the simple click of a button, an electronic file can be deleted, copied, or sent to the other side of the world.<sup>5</sup> The methods for stealing electronic trade secrets through unauthorized access to computers, hacking of computers, and destruction of data on computers are evolving at a rapid rate.<sup>6</sup> Therefore, the methods for protecting trade secrets must develop at an equal pace.<sup>7</sup> American companies must have security measures in place to guard their trade secret information against thievery, thus

---

\* J.D. Candidate, May 2009, The John Marshall Law School. M.S. Higher Education and Student Affairs, Miami University, Oxford, Ohio, May 2006. B.A. Political Science and History, Miami University, Oxford, Ohio, May 2001. A special thanks to my editor Michael D. Karson for his invaluable editorial assistance. Thank you also to the staff of *The John Marshall Review of Intellectual Property Law* for their support during the research and writing process.

<sup>1</sup> Robert Mueller, Dir. Fed. Bureau of Investigations, Address to the National Press Club Luncheon (June 23, 2003) (“Economic espionage is costing our U.S. businesses now more than \$200 billion a year in theft of intellectual property.”); see also R. MARK HALLIGAN & RICHARD F. WEYAND, TRADE SECRET ASSET MANAGEMENT: AN EXECUTIVE’S GUIDE TO INFORMATION ASSET MANAGEMENT, INCLUDING SARBANES-OXLEY ACCOUNTING REQUIREMENTS FOR TRADE SECRETS 23 (2006) (discussing losses suffered by business across the country from stolen trade secrets).

<sup>2</sup> See ASIS INT’L, TRENDS IN PROPRIETARY INFORMATION LOSS 12 (2007), available at <http://www.asisonline.org/newsroom/surveys/spi2.pdf>.

<sup>3</sup> See MARGARET M. BLAIR & STEVEN M.H. WALLMAN, UNSEEN WEALTH: REPORT OF THE BROOKINGS TASK FORCE ON INTANGIBLES (2001) (evaluating the importance of intangible assets on economic growth within the U.S. economy).

<sup>4</sup> See *id.*

<sup>5</sup> See 2 JOHN J. FALVEY, JR. & AMY M. MCCALLEN, INTERNET LAW AND PRACTICE § 26:6 (2008) (“Growth in use of the Internet has also offered inviting opportunities for intellectual property crimes.”); R. Mark Halligan, *Protecting Trade Secrets Online*, in BUSINESS, LAW, AND THE INTERNET: ESSENTIAL GUIDANCE FOR YOU, YOUR CLIENTS, AND YOUR FIRM 14–9 (Michael S. Simon & André C. Frieden eds., 2002) (“The Internet has become an engine for the destruction of trade secret rights. Within seconds, a disgruntled employee can upload and transmit trade secret information to the Internet, from which it can be accessible to millions of people around the world.”).

<sup>6</sup> See 2 FALVEY & MCCALLEN, *supra* note 6, § 26:6. (“The widespread use of the Internet, coupled with specific technologies that have developed to facilitate copying, makes intellectual property theft easier than ever.”).

<sup>7</sup> Halligan, *supra* note 5, at 14–10 (“Deterrence of trade secret theft via the Internet is a daunting task. Hackers are always one step ahead of legitimate computer users. In designing trade secret protection programs, you should anticipate theft and set traps so that if a theft occurs you can identify and track down the offender.”).

maintaining the information's status as a protectable asset.<sup>8</sup> Once a corporation or small business, however, falls victim to trade secret misappropriation, civil litigation becomes the party's only means to recoup the loss from its damaged trade secret asset.<sup>9</sup>

Trade secret litigation will inevitably become more complex as a result of advances in technology, globalization, employee mobility, and increasing corporate ownership of intangible assets.<sup>10</sup> In order to meet the demands of complex trade secret litigation, parties desire the procedural benefits of the federal courts, primarily nationwide service of process.<sup>11</sup> At this time, however, there is no federal civil cause of action for trade secret misappropriation.<sup>12</sup> Indeed, trade secrets remain the only major area of intellectual property not protected by a federal statute.<sup>13</sup> A party seeking to litigate the misappropriation of its trade secrets in federal court must rely on the parties' diversity of citizenship in order for the court to have subject matter jurisdiction.<sup>14</sup> Unfortunately, diversity jurisdiction may not be present in situations where a current or former employee misappropriates the employer's trade secrets. Where diversity jurisdiction does not exist, the party's only means to gain subject matter jurisdiction in a federal venue would be through federal question jurisdiction.<sup>15</sup>

This comment advances a means to secure access to the federal courts in order to meet the needs of complex trade secret litigation. The Computer Fraud and Abuse Act ("CFAA")<sup>16</sup> can serve as a vehicle to allow aggrieved parties access to the federal

---

<sup>8</sup> See, e.g., UNIF. TRADE SECRETS ACT § 1(4)(ii) (amended 1985), 14 U.L.A. 538 (2005) (including a requirement that a trade secret be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy."); HALLIGAN & WEYAND, *supra* note 1, at 61 (asserting that, with the evolution of new threats to information security, corporations and small business must develop new software, hardware, and business methods for maintaining the secrecy of their trade secrets).

<sup>9</sup> HALLIGAN & WEYAND, *supra* note 1, at 27 ("The only way to validate a trade secret is through litigation.").

<sup>10</sup> See Albert P. Halluin & Lorelei P. Westin, *Nanotechnology: The Importance of Intellectual Property Rights in an Emerging Technology*, 86 J. PAT. & TRADEMARK OFF. SOC'Y 220, 225 (2004).

Although trade secrets can be a powerful arsenal in the protection of intellectual property rights, it is becoming more and more difficult to keep such knowledge confidential. Because of the increased mobility of employees and the accessibility of the internet, the ease of getting information makes trade secrets difficult to defend.

*Id.*

<sup>11</sup> See Roy E. Hofer & Susan F. Gullotti, *Presenting the Trade Secret Owner's Case, in* PROTECTING TRADE SECRETS 1985, at 145, 160–61 (PLI Patents, Copyrights, Trademarks, & Literary Prop., Course Handbook Series No. 196, 1985), available at WL, 196 PLI/Pat 145.

<sup>12</sup> See 1 JOHN GLADSTONE MILLS III, DONALD CRESS REILEY, III & ROBERT CLAIRE HIGHLEY, PATENT LAW FUNDAMENTALS § 4:5 (2008) ("Civil liability for misappropriation of a trade secret, whether predicated on a breach of contract, a breach of confidence, a tort, or on any other theory, is a state-law claim, not a federal claim.").

<sup>13</sup> Compare *id.* (noting that state law governs trade secrets), with 15 U.S.C. § 1114–17 (2006) (trademarks), 17 U.S.C. § 501–05 (copyrights), and 35 U.S.C. § 271–73 (patents).

<sup>14</sup> 28 U.S.C. § 1332.

<sup>15</sup> *Id.* § 1331 ("The district courts shall have original jurisdiction of all civil actions arising under the Constitution, laws, or treaties of the United States.").

<sup>16</sup> 18 U.S.C.A. § 1030 (West 2008). On September 26, 2008, the provisions of Identity Theft Enforcement and Restitution Act of 2008 became effective. Identity Theft Enforcement and Restitution Act of 2008, Pub. L. No. 110-326, §§ 201–09, 122 Stat. 3560, 3560–65 (2008) (to be

courts in order to litigate their trade secret rights. This comment supports the view that the causes of action within the CFAA defend all electronic trade secrets as well as trade secrets stored on a computer.<sup>17</sup> The protection provided by the CFAA does not stop with its causes of action; as long as a party's primary claim arises under the CFAA, that party can also file one or more state law claims for trade secret misappropriation through the federal courts' supplemental jurisdiction.<sup>18</sup>

The CFAA can serve as a "gap-filler" until Congress enacts legislation authorizing federal question jurisdiction specifically for trade secret misappropriation. That authorization could take the form of a federal trade secret statute or, in the alternative, an amendment to the Economic Espionage Act of 1996 adding a civil cause of action.<sup>19</sup> The CFAA has been challenged by some and championed by others, but it has a distinct advantage in that it protects *all* valuable computer data regardless of whether it is proven a trade secret under state law.<sup>20</sup>

Part I of this Comment discusses the traditional state law cause of action for trade secret misappropriation, provides the statutory background and history of the CFAA, and discusses cases demonstrating the split in authority regarding the meaning of terms within the CFAA. Part II analyzes the complexities surrounding the term "without authorization," and the definitions of, "exceeds authorized access," and "damage." Part III advocates for the use of the CFAA in trade secret litigation, and for the wider adoption of the broad view of the key terms and provisions within the CFAA in order to ensure access to the federal courts for complex trade secret litigation.

---

codified at 18 U.S.C. § 1030); Press Release, Office of the Press Sec'y, President Bush Signs H.R. 5938 Into Law (on file with author) *available at* <http://www.whitehouse.gov/news/releases/2008/09/20080926-12.html>. Because the Identity Theft Enforcement and Restitution Act of 2008 amended the sections of 18 U.S.C. § 1030, all references to this statute will refer to the unofficial U.S.C.A. reporter.

<sup>17</sup> Nick Akerman & Edward M. Stroz, *Trade Secrets: Computer Security*, NAT'L L.J., Sept. 16, 2002, at B8 ("The CFAA protects all valuable computer data, whether or not it would be considered a trade secret.").

<sup>18</sup> See 28 U.S.C. § 1367(a); see also *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930 (9th Cir. 2004) (affirming a jury's special verdict in favor of the plaintiff's assertion violations of both the CFAA and the Idaho Trade Secrets Act).

[I]n any civil action of which the district courts have original jurisdiction, the district courts shall have supplemental jurisdiction over all other claims that are so related to claims in the action within such original jurisdiction that they form part of the same case or controversy under Article III of the United States Constitution.

28 U.S.C. § 1367(a).

<sup>19</sup> See Victoria A. Cundiff, *Digital Defense: Protecting Trade Secrets Against New Threats*, in 14TH ANNUAL INSTITUTE ON INTELLECTUAL PROPERTY LAW, at 707, 720–21 (PLI Patents, Copyrights, Trademarks, & Literary Prop., Course Handbook Series No. 947, 2008), *available at* WL, 947 PLI/Pat 707.

<sup>20</sup> See Akerman & Stroz, *supra* note 17, at B8 ("The CFAA was enacted to 'ensure that the theft of intangible information by the unauthorized use of a computer is prohibited in the same way theft of physical items are protected.'" (quoting *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1128 (W.D. Wash. 2000)); see also S. REP. NO. 104-357, at 7 (1996).

## I. BACKGROUND

*A. Sources of State Trade Secret Law*

Every state in the United States has laws protecting trade secrets.<sup>21</sup> Forty-seven jurisdictions including the District of Columbia have adopted the Uniform Trade Secrets Act (“UTSA”),<sup>22</sup> or some variation thereof, as the basis for its trade secret misappropriation cause of action.<sup>23</sup> Further, many states derive their trade secret laws from the Restatement (First) of Torts as well as the Restatement (Third) of Unfair Competition.<sup>24</sup> The UTSA and the Restatements each provide a definition of trade secret, which is fundamentally the same.<sup>25</sup> The doctrinal principle is that a trade secret is information used in a party’s business that derives economic value from its secrecy.<sup>26</sup>

There are three essential elements to a state trade secret misappropriation claim.<sup>27</sup> First, the information must qualify as a trade secret.<sup>28</sup> Second, the plaintiff must have made reasonable efforts to prevent disclosure of its trade secret.<sup>29</sup> Third, the plaintiff must prove that the defendant acquired the trade secret through wrongful means.<sup>30</sup>

In order to demonstrate that information qualifies as a trade secret, a party must show that the information meets the state’s definition of a trade secret.<sup>31</sup> The UTSA defines a trade secret as information that “derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons”<sup>32</sup> and “is the subject of efforts that

<sup>21</sup> ROBERT P. MERGES, PETER S. MENELL, & MARK A. LEMLEY, *INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE* 35 (rev. 4th ed. 2007) (“Today, every one of the United States protects trade secrets in some form or another.”).

<sup>22</sup> UNIF. TRADE SECRETS ACT §§ 1–12 (amended 1985), 14 U.L.A. 537–659 (2005).

<sup>23</sup> 14 U.L.A. 18–19 (Supp. 2008) (listing the forty-seven jurisdictions that have adopted the UTSA, including the District of Columbia and the U.S. Virgin Islands).

<sup>24</sup> MERGES, MENELL & LEMLEY, *supra* note 21, at 36; *see* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1993); RESTATEMENT (FIRST) OF TORTS §§ 757–58 (1939); *id.* § 757 cmt. b.

<sup>25</sup> *See* UNIF. TRADE SECRETS ACT § 1(4) (amended 1985), 14 U.L.A. 538 (2005); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1993); RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939).

<sup>26</sup> *See* UNIF. TRADE SECRETS ACT § 1(4)(i)–(ii) (amended 1985), 14 U.L.A. 538 (2005) (“Trade Secret’ means information . . . that derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons . . .”); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (“A trade secret is any information . . . that is sufficiently valuable and secret to afford an actual or potential economic advantage over others.”); RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (“A trade secret may consist of . . . information which is used in one’s business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it.”).

<sup>27</sup> MERGES, MENELL & LEMLEY, *supra* note 21, at 37.

<sup>28</sup> *Id.*

<sup>29</sup> *Id.*

<sup>30</sup> *Id.*

<sup>31</sup> *See* Sharon K. Sandeen, *A Contract by Any Other Name is Still a Contract: Examining the Effectiveness of Trade Secret Clauses to Protect Databases*, 45 IDEA 119, 128–29 (2005) (stating that under the UTSA there is a proper shift in trade secrets cases to a focus on proving the existence of a trade secret and not a focus on the relationship of the parties).

<sup>32</sup> UNIF. TRADE SECRETS ACT § 1(4)(i) (amended 1985), 14 U.L.A. 538 (2005).

are reasonable under the circumstances to maintain its secrecy.”<sup>33</sup> A party must show that its alleged trade secret satisfies *all* of the elements of the UTSA test.<sup>34</sup> The Restatement (First) of Torts, as opposed to the UTSA’s explicit test, lists several factors that courts may consider when determining whether information is protectable as a trade secret.<sup>35</sup> Those factors are:

- (1) the extent to which the information is known outside of [the plaintiff’s] business;
- (2) the extent to which it is known by employees and others involved in [the plaintiff’s] business;
- (3) the extent of measures taken by [the plaintiff] to guard the secrecy of the information;
- (4) the value of the information to [the plaintiff’s business] and to [the plaintiff’s] competitors;
- (5) the amount of effort or money expended by [the plaintiff] in developing the information;
- (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.<sup>36</sup>

None of these six factors are outcome determinative.<sup>37</sup> Furthermore, unlike the UTSA, plaintiffs need not demonstrate that all six factors weigh in their favor in order to prove the existence of a trade secret.<sup>38</sup>

The party alleging trade secret misappropriation must also have made reasonable efforts to maintain the secrecy of the information it purports to be a trade secret.<sup>39</sup> This showing is required under both the UTSA and the Restatement (First) of Torts.<sup>40</sup> What constitutes reasonable efforts to maintain secrecy varies depending on the circumstances, the size of the entity, and its economic resources.<sup>41</sup>

After making it over the first two hurdles, a plaintiff must prove that the defendant misappropriated the trade secret or, put another way, acquired the trade

---

<sup>33</sup> *Id.* § 1(4)(ii), 14 U.L.A. at 538.

<sup>34</sup> *See* Sandeen, *supra* note 31, at 131 (“Obviously, because information must meet the foregoing requirements to be deemed a trade secret, a trade secret cannot be established by the mere recitation of its existence in a contract.”).

<sup>35</sup> RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939).

<sup>36</sup> *Id.*

<sup>37</sup> *E.g.*, Learning Curve Toys, Inc. v. Playwood Toys, Inc., 342 F.3d 714, 722 (7th Cir. 2003).

Contrary to Learning Curve’s contention, we do not construe the foregoing factors as a six-part test in which the absence of evidence on any single factor necessarily precludes a finding of trade secret protection. Instead, we interpret the common law factors as instructive guidelines for ascertaining whether a trade secret exists under the [Illinois Trade Secrets] Act.

*Id.*

<sup>38</sup> *E.g.*, *id.* (“The language of the [Illinois Trade Secrets] Act itself makes no reference to these factors as independent requirements for trade secret status, and Illinois case law imposes no such requirement that each factor weigh in favor of the plaintiff.”).

<sup>39</sup> UNIF. TRADE SECRETS ACT § 1(4)(ii) (amended 1985), 14 U.L.A. 538 (2005).

<sup>40</sup> *Id.*; RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939) (including “the extent of measures taken by [the plaintiff] to guard the secrecy of the information” among the six factors used to determine whether information is a trade secret).

<sup>41</sup> *See, e.g.*, Rockwell Graphic Sys., Inc. v. DEV Indus., Inc. 925 F.2d 174 (7th Cir. 1991) (defining the meaning of reasonable efforts to maintain secrecy based on an economic analysis); Elmer Miller, Inc. v. Landis, 625 N.E.2d 338, 342 (Ill. App. Ct. 1993) (stating that reasonable efforts to maintain secrecy are different for a small business than they are for a larger company).

secret wrongfully.<sup>42</sup> Essentially, the UTSA defines “misappropriation” as a person, not the trade secret owner, acquiring the trade secret by improper means.<sup>43</sup> These three steps provide the basis for the trade secret misappropriation causes of action based on the UTSA.

### *B. The Computer Fraud and Abuse Act*

Congress enacted the CFAA in 1984 as an exclusively criminal statute in order to protect classified information stored on computers belonging to the government and financial institutions.<sup>44</sup> The CFAA is an anti-hacking law, but in 1994 Congress added a civil remedy to offset the monetary damage caused by the criminal violations.<sup>45</sup> Congress further amended the CFAA to broaden its scope in order to protect any computer used in interstate commerce and not just those computers used by the government or financial institutions.<sup>46</sup> Arguably any computer attached to the Internet can be used in interstate commerce.<sup>47</sup> The CFAA, therefore, protects all networked business computers and the information stored on them.<sup>48</sup>

---

<sup>42</sup> UNIF. TRADE SECRETS ACT § 1(2) (amended 1985), 14 U.L.A. 537 (2005); RESTATEMENT (FIRST) OF TORTS § 757 (1939).

One who discloses or uses another’s trade secret, without a privilege to do so, is liable to the other if

- (a) he discovered the secret by improper means, or
- (b) his disclosure or use constitutes a breach of confidence reposed in him by the other in disclosing the secret to him, or
- (c) he learned the secret from a third person with notice of the facts that it was a secret and that the third person discovered it by improper means or the third person’s disclosure of it was otherwise a breach of his duty to the other, or
- (d) he learned the secret with notice of the facts that it was a secret and that the its disclosure was made to him by mistake.

*Id.*

<sup>43</sup> See UNIF. TRADE SECRETS ACT § 1(2) (amended 1985), 14 U.L.A. 537 (2005).

<sup>44</sup> Nick Akerman & Patricia Finnegan, *Computer Law: Civil Relief Under CFAA*, NAT’L L.J., Dec. 24–31, 2001, at A19 (“Enacted in 1984, the CFAA began as an exclusively criminal statute, designed to protect classified information on government computers and financial records or credit information on financial institution computers.”).

<sup>45</sup> *Id.*

<sup>46</sup> S. REP. NO. 104-357, at 10 (1996) (“[T]he 1994 amendment to subsection 1030(a)(5) . . . was intended to broaden the reach of the provision by replacing the term ‘federal interest computer’ with the term ‘computer used in interstate commerce or communication.’”); Akerman & Finnegan, *supra* note 44, at A19.

<sup>47</sup> *Am. Libraries Ass’n v. Pataki*, 969 F. Supp. 160, 170–71 (S.D.N.Y. 1997).

The Internet is wholly insensitive to geographic distinctions. In almost every case, users of the Internet neither know nor care about the physical location of the Internet resources they access. Internet protocols were designed to ignore rather than document geographic location; while computers on the network do have “addresses,” they are logical addresses on the network rather than geographic addresses in real space.

*Id.*

<sup>48</sup> Michael R. Levinson & Christopher E. Paetsch, *The Computer Fraud and Abuse Act: A Powerful New Way to Protect Information*, INTELL. PROP. NEWSL. (Am. Bar Ass’n, Chicago, Ill.),

The CFAA provides six civil causes of action that can be used in trade secret litigation.<sup>49</sup> A person or entity may be civilly liable when it:

1. “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution . . . ;”<sup>50</sup>
2. “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer;”<sup>51</sup>
3. “knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period;”<sup>52</sup>
4. “knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;”<sup>53</sup>
5. “intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage;”<sup>54</sup> or
6. “intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.”<sup>55</sup>

The CFAA provides civil relief in the form of compensatory damages or injunctive relief to any person who suffers damages or loss from a violation of the Act.<sup>56</sup> The trade secret violation must involve at least one aggravating factor, which includes (I) loss to one or more person during a one-year period aggregating at least

---

Spring 2002, at 24 (“Any information, whether or not it is secret, can be protected under the CFAA. All that most sections of the statute require is that the information be stored on a computer.”).

<sup>49</sup> 18 U.S.C.A. § 1030(a)(2)(A), (a)(2)(C), (a)(4), (a)(5)(A)–(C) (West 2008).

<sup>50</sup> *Id.* § 1030(a)(2)(A).

<sup>51</sup> *Id.* § 1030(a)(2)(C).

<sup>52</sup> *Id.* § 1030(a)(4).

<sup>53</sup> *Id.* § 1030(a)(5)(A).

<sup>54</sup> *Id.* § 1030(a)(5)(B).

<sup>55</sup> *Id.* § 1030(a)(5)(C).

<sup>56</sup> *Id.* § 1030(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 subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(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.

*Id.*

\$5,000,<sup>57</sup> (II) the modification or impairment of a medical examination of one or more individuals,<sup>58</sup> (III) “physical injury to any person,”<sup>59</sup> (IV) “a threat to public health or safety,”<sup>60</sup> or (V) damage affecting a government computer used for national security, defense, or justice.<sup>61</sup> There is a two-year statute of limitations for civil relief and the CFAA does not provide civil relief for the negligent design of computer hardware or software.<sup>62</sup>

In order to gain civil relief, a party must satisfy a two-part inquiry: (1) there must be a violation of the CFAA giving rise to one of the six causes of action enumerated in the statute resulting in damage or loss, and (2) the violation must involve conduct described in one of the five aggravating factors.<sup>63</sup> Notwithstanding the convoluted nature of the CFAA’s text, a claim for civil relief may be brought under any of the six causes of action as long as any of the five aggravating factors is demonstrated.<sup>64</sup> If the aggravating factor is loss to one or more persons during any one-year period then relief is limited to economic damages.<sup>65</sup> The CFAA also provides several definitions of key terms that have become the focus of trade secret litigation including: “exceeds authorized access,”<sup>66</sup> “damage,”<sup>67</sup> and “loss.”<sup>68</sup> The

<sup>57</sup> *Id.* § 1030(c)(4)(A)(i)(I).

<sup>58</sup> *Id.* § 1030(c)(4)(A)(i)(II).

<sup>59</sup> *Id.* § 1030(c)(4)(A)(i)(III).

<sup>60</sup> *Id.* § 1030(c)(4)(A)(i)(IV).

<sup>61</sup> *Id.* § 1030(c)(4)(A)(i)(V).

<sup>62</sup> *Id.* § 1030 (g).

<sup>63</sup> *Lockheed Martin Corp., v. Speed*, 81 U.S.P.Q.2d (BNA) 1669, 1671 (M.D. Fla. 2006) (“Thus, before reaching the merits of the alleged violations, the CFAA’s private cause of action sets forth a two-part injury requirement, where a plaintiff must: (1) suffer a root injury of damage or loss; and (2) suffer one of five operatively-substantial effects in subsection (a)(5)(B)(i)–(v).”).

<sup>64</sup> *See Fiber Sys. Int’l Inc. v. Roehrs*, 470 F.3d 1150, 1157 (5th Cir. 2006); *P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC.*, 428 F.3d 504, 512 (3rd Cir. 2005); *Theofel v. Farey-Jones*, 359 F.3d 1066, 1078 n.5 (9th Cir. 2004);

We do not read section 1030(g)’s language that the claim must *involve* one or more of the numbered subsections of subsection (a)(5)(B) as limiting relief to claims that are *entirely based only on* subsection (a)(5), but, rather, as requiring that claims brought under other sections must meet, in addition, one of the five numbered (a)(5)(B) “tests.”

*P.C. Yonkers*, 428 F.3d at 512. Under the statute effective September 26, 2008, the “(a)(5)(B) ‘tests’” are presently located at 18 U.S.C.A. § 1030(c)(4)(A)(i)(I)–(V). *Compare* 18 U.S.C. § 1030(a)(5)(B)(i)–(v) (2006) (listing the “(a)(5)(B) ‘tests’”), *with* 18 U.S.C.A. § 1030(c)(4)(A)(i)(I)–(V) (using identical language to the old “(a)(5)(B) ‘tests’”). This change does not appear to be a substantive change to the meaning of the statute. Likewise, under the statute effective September 26, 2008, the “subsection (a)(5)” claims are presently located at 18 U.S.C.A. § 1030(a)(5)(A)–(C). *Compare* 18 U.S.C. § 1030(a)(5)(A)(i)–(iii) (listing the “subsection (a)(5)” claims), *with* 18 U.S.C.A. § 1030(a)(5)(A)–(C) (using substantially identical language to the old “subsection (a)(5)” claims). Thus, although the CFAA has been amended, the substantive effect of the statute appears to remain unchanged.

<sup>65</sup> 18 U.S.C.A. § 1030 (g).

<sup>66</sup> *Id.* § 1030(e)(6) (“[T]he term ‘exceeds authorized access’ means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.”).

<sup>67</sup> *Id.* § 1030(e)(8) (“[T]he term ‘damage’ means any impairment to the integrity or availability of data, a program, a system, or information.”).

<sup>68</sup> *Id.* § 1030(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.”).

CFAA is a complex statute that could be a powerful tool for the protection of electronic trade secret assets and trade secrets stored on computers, but courts are split on the applicability of the statute to employee computer abuse.<sup>69</sup> Since 2000, courts have grappled with whether to interpret the CFAA provisions and key terms broadly or narrowly, and the following section illuminates the courts' varying points of view.

### *C. CFAA Lines of Thinking: Unauthorized Access*

#### *1. Broad Interpretation*

The meaning of the terms “without authorization” and “exceeds authorized access” have been the focal point of many CFAA decisions.<sup>70</sup> And courts are currently split in determining whether to apply a broad or narrow meaning to the terms.<sup>71</sup> The broad interpretation rests on principles of agency law.<sup>72</sup> It asserts that an employee with authorization to access a protected computer,<sup>73</sup> and the trade secrets on it, loses authorization with the advent of a disloyal mindset toward the employer.<sup>74</sup> One of the first reported CFAA district court decisions applied this approach<sup>75</sup> and the Seventh Circuit has expressly adopted it.<sup>76</sup>

*Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*<sup>77</sup> is the seminal case championing the broad interpretation of the term “without authorization.”<sup>78</sup> In

<sup>69</sup> See Linda K. Stevens & Jesi J. Carlson, *The CFAA: New Remedies for Employee Computer Abuse*, 96 ILL. B.J. 144 (2008) (“A split of authority has developed, however, regarding the CFAA’s applicability to employee computer abuse, and even among the jurisdictions applying the CFAA to employees, construction and application of the statute vary greatly.”).

<sup>70</sup> See generally Nick Akerman, *Computer Access: ‘Unauthorized Access’*, NAT’L L.J., Dec. 12, 2005, at 15 (“Unauthorized access to a computer is a critical element to proving most violations of the federal Computer Fraud and Abuse Act (CFAA).”).

<sup>71</sup> Compare, e.g., *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000) (broad interpretation), with *Lockheed Martin Corp., v. Speed*, 81 U.S.P.Q.2d (BNA) 1669 (M.D. Fla. 2006) (narrow interpretation).

<sup>72</sup> See *Shurgard*, 119 F. Supp. 2d at 1124–25.

<sup>73</sup> 18 U.S.C.A. § 1030(e)(2) (defining the term “protected computer” as any computer “used in or affecting interstate or foreign commerce or communication”).

<sup>74</sup> See *Int’l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420–21 (7th Cir. 2006).

Citrin’s breach of his duty of loyalty terminated his agency relationship (more precisely, terminated any rights he might have claimed as [plaintiff’s] agent—he could not by unilaterally terminating any duties he owed his principal gain an advantage!) and with it his authority to access the laptop, because the only basis of his authority had been that relationship. “Violating the duty of loyalty, or failing to disclose adverse interests, voids the agency relationship.”

*Id.*

<sup>75</sup> *Shurgard*, 119 F. Supp. 2d at 1121.

<sup>76</sup> *Citrin*, 440 F.3d at 418.

<sup>77</sup> 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

<sup>78</sup> See, e.g., *Citrin*, 440 F.3d at 421 (citing *Shurgard*); *P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC.*, 428 F.3d 504, 510 (3rd Cir. 2005) (same); *Register.com, Inc., v. Verio, Inc.*, 356 F.3d 393, 440 (2d Cir. 2004) (same); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 584 (1st Cir. 2001) (same); *Charles Schwab & Co. v. Carter*, No. 04 C 7071, 2005 WL 2369815, at \*7 (N.D. Ill. Sept. 27, 2005) (same).

*Shurgard*, the plaintiff, an industry leader in self-service storage facilities, developed sophisticated marketing and business development plans, which were the electronic trade secrets at issue.<sup>79</sup> As a part of his employment, the former employee was allowed full access to the confidential plans.<sup>80</sup> The defendant, a direct competitor, offered the former employee a position with its company.<sup>81</sup> While remaining in the plaintiff's employ, the former employee sent emails containing the electronic trade secrets and proprietary information to the defendant.<sup>82</sup> The former employee continued to provide the defendant with the plaintiff's confidential information even after beginning his employment with the defendant.<sup>83</sup>

The plaintiff filed a claim for civil relief under the CFAA alleging that: (1) the former employee intentionally accessed a protected computer without authorization or by exceeding his authorized access and obtained information from a protected computer,<sup>84</sup> (2) that he knowingly and with the intent to defraud accessed a protected computer without authorization or by exceeding his authorized access to further the fraud,<sup>85</sup> and (3) that he intentionally accessed a protected computer without authorization and as result of the conduct caused damage.<sup>86</sup> The court denied the defendant's motion to dismiss, stating that the plaintiff asserted violations under all three provisions of the CFAA.<sup>87</sup>

Safeguard attempted to defend against the plaintiff's claim by arguing that the former employees were not "without authorization" to access the computers and information at issue.<sup>88</sup> The court was not persuaded and took the opportunity to broadly define the phrase "without authorization."<sup>89</sup> The court determined that the employee became the defendant's agent when he emailed trade secret information to the defendant.<sup>90</sup> The court held that the employee's authorized access ceased to exist the moment he acted against his employer for the defendant's benefit.<sup>91</sup>

In *International Airport Centers, L.L.C. v. Citrin*,<sup>92</sup> the Seventh Circuit took the opportunity to adopt the broad interpretation of "without authorization" and "exceeds authorized access" and to define the meaning of the word "transmission" as applied in the CFAA.<sup>93</sup> The defendant, Citrin, violated his employment contract when he left his real estate prospecting job at International Airport Centers ("IAC") to go into

---

<sup>79</sup> *Shurgard*, 119 F. Supp. 2d at 1122–23.

<sup>80</sup> *Id.* at 1123.

<sup>81</sup> *Id.*

<sup>82</sup> *Id.*

<sup>83</sup> *Id.*

<sup>84</sup> *Id.* at 1124 (discussing the claim arising under 18 U.S.C.A. § 1030(a)(2)(C) (West 2008)).

<sup>85</sup> *Id.* at 1125 (discussing the claim arising under 18 U.S.C.A. § 1030(a)(4)).

<sup>86</sup> *Id.* at 1126 (discussing the claim arising under 18 U.S.C.A. § 1030(a)(5)(C)).

<sup>87</sup> *Id.* at 1129.

<sup>88</sup> *Id.* at 1124.

<sup>89</sup> *Id.* at 1124–25.

<sup>90</sup> *Id.* at 1125 ("Therefore, for the purposes of this 12(b)(6) motion, [the plaintiff's former employees] lost their authorization and were 'without authorization' when they allegedly obtained and sent the proprietary information to the defendant via e-mail.")

<sup>91</sup> See *id.* (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.")

<sup>92</sup> 440 F.3d 418 (7th Cir. 2006).

<sup>93</sup> See *id.* at 418–21.

work for himself.<sup>94</sup> Prior to returning his company-issued laptop computer, Citrin used a secure-erasure program to delete all the data pertaining to IAC real estate ventures.<sup>95</sup> Importantly, IAC did not have duplicates of the files Citrin deleted.<sup>96</sup> Citrin also deleted all the data pertaining to his improper conduct while he was in IAC's employ.<sup>97</sup> IAC sued Citrin for destroying data through the transmission of the erasure program<sup>98</sup> and also for recklessly causing damage to the computer data without authorized access.<sup>99</sup>

The court reversed the district court's dismissal of the case and interpreted the word transmission within the CFAA to include both a signal sent via a program running on a disk or a long distance attack via a virus on the Internet.<sup>100</sup> The court also expressly affirmed the ruling in *Shurgard* by reading principles of agency law into the CFAA, stating that unauthorized access occurs when an employee acts in an adverse manner to his employment.<sup>101</sup>

## 2. Narrow Interpretation

*Shurgard*, *Citrin*, and their progeny provide a broad application of the CFAA in trade secret litigation. In other cases, however, courts have applied a narrow interpretation of "without authorization" and "exceeds authorized access."<sup>102</sup> The

---

<sup>94</sup> *Id.* at 419.

<sup>95</sup> *Id.*

<sup>96</sup> *Id.* at 421.

<sup>97</sup> *Id.* at 419.

<sup>98</sup> *Id.*; see 18 U.S.C.A. § 1030 (a)(5)(A) (West 2008)

<sup>99</sup> *Citrin*, 440 F.3d at 420; see 18 U.S.C.A. § 1030 (a)(5)(B).

<sup>100</sup> *Citrin*, 440 F.3d at 420. The court interpreted the word "transmission" to mean not only a long distance malicious attack from an outsider sent via an Internet connection, but also an attack by an insider via a downloaded program such as the one used by Citrin. *Id.* The court analyzed the technology and found that it was irrelevant whether the program was downloaded from the Internet, or copied from a CD inserted in the computer, or attached via a wire because the only difference is in the mechanics of the transmission. Nick Ackerman, *Business Information: CFAA and Data Destruction*, NAT'L L.J., Apr. 10, 2006, at 16. The court also distinguished erasing data through a secure-erasure program, which completely deletes the indexed file from the computer, from erasing data via the delete key, which only removes the data to free up space but does not completely remove the data from the computer. *Id.*

<sup>101</sup> See *Citrin*, 440 F.3d at 421 ("Unless otherwise agreed, the authority of the 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." (citing *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000); RESTATEMENT (SECOND) OF AGENCY § 112 (1958))).

<sup>102</sup> See, e.g., *Brett Senior & Assocs. v. Fitzgerald*, No. 06-1412, 2007 WL 2043377, at \*4 (E.D. Pa. July 13, 2007) (comparing the broad and narrow interpretations of the CFAA and applying the narrow interpretation); *Lockheed Martin Corp. v. Speed*, 81 U.S.P.Q.2d (BNA) 1669, 1674-76 (M.D. Fla. 2006) (applying narrow interpretation of "without authorization"); *Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479, 499 (D. Md. 2005).

Recognizing that *Shurgard* provides Plaintiff some support for a broader interpretation of these statutes, the court, nevertheless, concludes that in light of the more persuasive statutory interpretations discussed above, the legislative history, and the fact that the [Stored Wire and Electronic Communication and Transactional Records Access Act] and the CFAA are primarily criminal statutes, and, thus, should be construed narrowly . . . .

narrow interpretation purports that agency law principles cannot be read into the statute.<sup>103</sup> This line of cases asserts that based on its plain meaning, the CFAA only applies when (1) a party accessed a computer or information without ever having had authorization to access the computer or information at all, or (2) a party who had authorization to *some* computers or to *some* information nonetheless accessed a computer or information that surpassed its authorization.<sup>104</sup> Thus, the narrow interpretation does not allow courts to consider the accesser's mindset.<sup>105</sup>

In *Lockheed Martin Corp. v. Speed*<sup>106</sup> the court narrowly applied the CFAA and expressly rejected *Shurgard*.<sup>107</sup> Lockheed Martin filed suit against three former employees each of whom had access to trade secret information regarding a major defense contract.<sup>108</sup> The employees copied confidential and proprietary information before resigning from their positions and accepting employment with L-3, a major Lockheed competitor.<sup>109</sup> Lockheed responded by alleging three violations of the CFAA.<sup>110</sup> Lockheed argued that: (1) the former employees knowingly and with the intent to defraud accessed a protected computer without authorization or by exceeding their authorization and obtained anything of value worth more than \$5,000,<sup>111</sup> (2) they knowingly caused the transmission of a program or information, which intentionally caused damage to a protected computer,<sup>112</sup> and (3) they intentionally accessed a protected computer without authorization and a result of such conduct recklessly caused damage.<sup>113</sup> Lockheed also asserted that as a result of

---

*Id.*

<sup>103</sup> See *Lockheed Martin*, 81 U.S.P.Q.2d (BNA) at 1674 (“To the extent *Citrin* holds that an employee access “without authorization” at the moment the employee acquires a subjectively adverse interest to the employer, the Court respectfully disagrees.”).

<sup>104</sup> See *id.* at 1673.

Thus, it is plain from the outset that Congress singled out two groups of accessers, those “without authorization” (or those *below* authorization, meaning those having no permission to access whatsoever—typically outsiders, as well as insiders that are not permitted any computer access) and those exceeding authorization (or those *above* authorization, meaning those that go beyond the permitted access granted to them—typically insiders exceeding whatever access is permitted to them).

*Id.*

<sup>105</sup> See *id.* at 1674 (“Congress singled out those accessing ‘without authorization’ (or below authorization) and those ‘exceeding authorization’ (or above authorization) while purposefully leaving those in the middle untouched (those accessing with authorization), regardless of their subjective intent.”).

<sup>106</sup> 81 U.S.P.Q.2d (BNA) 1669 (M.D. Fla. 2006).

<sup>107</sup> *Id.* at 1673–76.

<sup>108</sup> *Id.* at 1670.

<sup>109</sup> *Id.* One of the defendants copied 200 documents onto a compact disc (“CD”) from his Lockheed computer before resigning from Lockheed and going to work for a competitor. *Id.* The second defendant burned 262 files onto a CD, sent nine files to his personal Personal Data Assistant (“PDA”), and on his last day at Lockheed copied another sixty-three detailed files regarding the defense project onto two CDs. *Id.* The final defendant, the third employee, synchronized his PDA with his Lockheed computer and removed strategic defense project files. *Id.*

<sup>110</sup> *Id.* at 1672–76.

<sup>111</sup> *Id.* at 1672; see 18 U.S.C.A. § 1030(a)(4) (West 2008).

<sup>112</sup> *Lockheed Martin*, 81 U.S.P.Q.2d (BNA) at 1676; see 18 U.S.C.A. § 1030(a)(5)(A).

<sup>113</sup> *Lockheed Martin*, 81 U.S.P.Q.2d (BNA) at 1676; see 18 U.S.C.A. § 1030(a)(5)(B).

the violations, there was a loss to one or more person in a one-year period aggregating \$5,000.<sup>114</sup>

Even though Lockheed alleged injury sufficient to warrant civil relief, the court granted the defendants' motion to dismiss because Lockheed did not sufficiently plead the CFAA violations.<sup>115</sup> The court determined that when the defendants accessed Lockheed's protected computers, they had authorization.<sup>116</sup> According to the court, applying a narrow interpretation, the CFAA only protects against wrongful access of information without authorization or access which exceeds authorization.<sup>117</sup> The court stated that Congress singled out two groups of accessers: parties with no permission to access, which are typically outsiders, and insiders who go above the parameters of their permissible access.<sup>118</sup> The court refused to adopt the agency law principles asserted in *Shurgard* and *Citrin* that an employee's breach of loyalty eliminates any authorization to access the information.<sup>119</sup> According to the court, the plain meaning of the statute was unambiguous and there was no need to resort to extrinsic materials to construe the CFAA.<sup>120</sup>

In *International Association of Machinists and Aerospace Workers v. Werner-Masuda*,<sup>121</sup> a federal district court in Maryland came to a similar decision as the court in *Lockheed Martin* by applying the narrow view of the CFAA.<sup>122</sup> In this case, Werner-Masuda, the Secretary-Treasurer of a Local Chapter of the plaintiff Union, signed a registration agreement giving her secure access to the Union's online membership database.<sup>123</sup> She subsequently used her access approximately 10,000 times in a three month period to give confidential membership data from her union to a rival union.<sup>124</sup> The plaintiff alleged violations of the Stored Wire and Electronic Communications and Transactional Records Access Act ("SECA")<sup>125</sup> and the CFAA.<sup>126</sup>

Regarding the CFAA, the Union alleged that Werner-Masuda violated the CFAA when she intentionally accessed the Union's membership database in a manner that exceeded her authorization under her signed computer registration agreement.<sup>127</sup> The court held that under the plain meaning of the statute, Werner-Masuda did not

---

<sup>114</sup> *Lockheed Martin*, 81 U.S.P.Q.2d (BNA) at 1672; see 18 U.S.C.A. § 1030(c)(4)(A)(i)(I).

<sup>115</sup> *Lockheed Martin*, 81 U.S.P.Q.2d (BNA) at 1676.

<sup>116</sup> *Id.* at 1673.

<sup>117</sup> *Id.*

<sup>118</sup> *Id.*

<sup>119</sup> *Id.* at 1674–76.

<sup>120</sup> *Id.* at 1672–73.

<sup>121</sup> 390 F. Supp. 2d 479 (D. Md. 2005).

<sup>122</sup> *Id.* at 499.

<sup>123</sup> *Id.* at 483. The defendant was authorized to access the Union's secure proprietary website, housed on the Union's own server, which required entry of a user ID and password. *Id.*

<sup>124</sup> *Id.* The defendant allegedly gave confidential membership information to the Union of Independent Flight Attendants ("UIFA"), which was formed to challenge the International Association of Machinists and Aerospace Workers ("IAM"). *Id.* The plaintiff alleged that the defendant's user ID was used to access the Union internal database approximately 10,000 times in a three month period in order to search names and addresses of members from four local IAM lodges. *Id.* "According to Plaintiff, the members of these four locals comprise the exact same members that Defendant UIFFA is attempting to organize into a rival union." *Id.*

<sup>125</sup> *Id.* at 484; 18 U.S.C. § 2701 (2006).

<sup>126</sup> *Werner-Masuda*, 390 F. Supp. 2d at 484; 18 U.S.C. § 1030.

<sup>127</sup> *Werner-Masuda*, 390 F. Supp. 2d at 495.

exceed her authorized access because, as a part of her official duties as Secretary-treasurer, she was authorized to access the membership information and the Union did not revoke her authorization.<sup>128</sup> The court rejected the plaintiff's argument that Werner-Masuda exceeded her authorized access to the database because, according to the court, Werner-Masuda was authorized to *access* the database under her registration agreement; she was not, however, authorized to *use* the information for a competing union's benefit.<sup>129</sup> Werner-Masuda argued, and the court accepted, that the CFAA applied mainly to outside computer hackers and "high-tech" criminals.<sup>130</sup> It concluded by saying that Congress did not intend for the term "exceeds authorized access" to have a sweeping meaning and offer broad protection.<sup>131</sup>

#### *D. CFAA Lines of Thinking: Loss and Damage*

Although courts are split on the meaning of "without authorization" and the application of the term "exceeds authorized access," those are not the only terms within the CFAA that have vexed litigants and the courts. The civil remedy provision begins by stating "[a]ny 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 . . ."<sup>132</sup> As a result, the meanings of the terms "damage" and "loss" have been a focal point of trade secret litigation under the CFAA.<sup>133</sup> A court's interpretation of these terms determines whether a proper CFAA claim has been

---

<sup>128</sup> *Id.* at 499. The court recognized that the broader interpretation of the CFAA supported the plaintiffs, but nevertheless rejected that approach and application of the RESTATEMENT (SECOND) OF AGENCY § 112 because it concluded that the statutory provisions, legislative history, and the fact that the CFAA was primarily a criminal statute supported a narrow interpretation. *Id.*

<sup>129</sup> *Id.* at 498.

Contrary to Plaintiff's assertion regarding the effect of the Registration Agreement on [Defendant's] authority to access [the database], the Agreement states clearly that "by signing this agreement, [she] agreed not to use the information provided through [the database] for any purpose that would be contrary to the policies and procedures established by the Constitution of the Grand Lodge of the International Association of Machinists and Aerospace Workers." Thus, to the extent that [Defendant] may have breached the Registration Agreement by using the information obtained for purposes contrary to the policies established by the IAM Constitution, it does not follow, as a matter of law, that she was not authorized to access the information, or that she did so in excess of her authorization in violation of the SECA or the CFAA.

*Id.*

<sup>130</sup> *Id.* at 496.

<sup>131</sup> *Id.* at 499. The court determined that the legislative history discussing the addition of the definition of "exceeds authorized access" demonstrates that Congress did not intend to penalize authorized federal employees whose access might be legitimate in some circumstances and criminal in others. *Id.*

<sup>132</sup> 18 U.S.C.A. § 1030(g) (West 2008).

<sup>133</sup> *See, e.g.,* Black & Decker (US), Inc. v. Smith, 568 F. Supp. 2d. 929 (W.D. Tenn. 2008) (discussing the meaning of "damage" within the CFAA); Garelli Wong & Assocs., Inc. v. Nichols, 551 F. Supp. 2d. 704 (N.D. Ill. 2008) (discussing the meaning of "damage" and "loss" within the CFAA); Resdev, LLC v. Lot Builders Ass'n, No. 6:04-CV-1374ORL31DAB, 2005 WL 1924743 (M.D. Fla. Aug. 10, 2005) (discussing the meaning of "damage" and "loss" within the CFAA).

raised and, more importantly, whether a party can receive compensation under the CFAA for its purloined trade secret.<sup>134</sup>

### 1. The “Loss” Requirement

The loss requirement acts as a jurisdictional bar in trade secret cases.<sup>135</sup> The CFAA definition of “loss” is:

[A]ny 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.”<sup>136</sup>

In order to properly state a claim under the CFAA, the plaintiff must allege two things: (1) a violation giving rise to one of the statute’s six causes of action, and (2) conduct involving one of the statute’s five aggravating factors.<sup>137</sup> The aggravating factor most frequently cited in civil trade secrets cases is that the conduct caused loss to one or more persons during any one year period aggregating at least \$5,000.<sup>138</sup> This dollar figure is the minimum that must be alleged and it constitutes losses connected with the physical harm to a computer, the costs incurred responding to the violation, and any destruction to the computer data.<sup>139</sup> It also includes the costs associated with a loss of business caused by the interruption of service to the computers or data network.<sup>140</sup> It is well settled from early CFAA decisions that the statute contains no “single act” requirement, which means that the \$5,000 threshold

---

<sup>134</sup> Daniel J. Winters & John F. Costello, Jr., *The Computer Fraud and Abuse Act: A New Weapon in the Trade Secrets Litigation Arena*, INTELL. PROP., April 2005, at 3.

<sup>135</sup> *Id.* (“In the majority of cases, the jurisdictional threshold has been met by establishing loss of at least \$5,000 attributable to the alleged violation of the CFAA.”).

<sup>136</sup> 18 U.S.C.A. § 1030(e)(11).

<sup>137</sup> *Lockheed Martin Corp., v. Speed*, 81 U.S.P.Q.2d (BNA) 1669, 1671 (M.D. Fla. 2006) (“Thus, before reaching the merits of the alleged violations, the CFAA’s private cause of action sets forth a two-part injury requirement, where a plaintiff must: (1) suffer a root injury of damage or loss; and (2) suffer one of five operatively-substantial effects in subsection (a)(5)(B)(i)-(v).”).

<sup>138</sup> 18 U.S.C.A. § 1030(c)(4)(A)(i)(I); *see, e.g.*, *Fiber Sys. Int’l, Inc. v. Roehrs*, 470 F.3d 1150, 1159 (5th Cir. 2006) (citing 18 U.S.C. § 1030(a)(5)(B)(i), now codified at 18 U.S.C.A. § 1030(c)(4)(A)(i)(I) (West 2008)); *P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC.*, 428 F.3d 504, 512 (3rd Cir. 2005) (same); *Charles Schwab & Co. v. Carter*, No. 04 C 7071, 2005 WL 2369815, at \*6 n.9 (N.D. Ill. Sept. 27, 2005) (same); *Four Seasons Hotels & Resorts B.V. v. Consorcio Barr, S.A.*, 267 F. Supp. 2d 1268, 1321–22 (S.D. Fla 2003) (same), *aff’d in part, rev’d in part without opinion*, 138 F. App’x 297 (11th Cir. 2005).

<sup>139</sup> *See Resdev, LLC v. Lot Builders Ass’n*, No. 6:04-CV-1374ORL31DAB, 2005 WL 1924743, at \*4 (M.D. Fla. Aug. 10, 2005) (focusing on the word “cost” within the CFAA definition of “loss,” the word “cost” limiting losses to those directly associated with or addressing the unauthorized computer access).

<sup>140</sup> *See Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 935 (9th Cir. 2004) (discerning that lost profits and loss of goodwill constitutes economic damages); *see also EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 584 (1st Cir. 2001) (“[A] general understanding of the word ‘loss’ would fairly encompass a loss of business, goodwill, and the cost of diagnostic measures . . .”).

can be met by aggregating multiple violations in a one year period.<sup>141</sup> It is not difficult to meet the \$5,000 loss threshold; rather, the issue in litigation is determining what damages constitute cognizable losses under the CFAA. This determination directly impacts whether a court will provide relief for the lost value of a trade secret.

## 2. The “Damage” Requirement

In many instances where computer-stored trade secrets are misappropriated, there will be no physical harm to the computers, no costs associated with responding to the violation, and no costs resulting from the interruption to the computer network.<sup>142</sup> This is the main reason why trade secret litigation under the CFAA often deals with the “loss” and “damage” requirements.<sup>143</sup> The CFAA definition of “damage” is “any impairment to the integrity or availability of data, a program, a system, or information.”<sup>144</sup> The other reason why trade secret litigation surrounds the “damage” requirement is that courts have not consistently construed the definition of “damage.”<sup>145</sup> Some courts have held that the CFAA definition of “damage” includes damage to the trade secret information.<sup>146</sup> Others have held that trade secret misappropriation alone is not actionable under the CFAA.<sup>147</sup> The following cases highlight the different interpretations of the loss and damage requirement.

In *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*,<sup>148</sup> the court also had to determine, on a motion to dismiss, whether the conduct of a former employee constituted “damage” under the CFAA.<sup>149</sup> As a part of his employment with the plaintiff, the former employee had full access to the plaintiff’s electronic and

---

<sup>141</sup> *Creative Computing*, 386 F.3d at 935. (“[T]he Computer Fraud and Abuse Act contains no ‘single act’ requirement.”).

<sup>142</sup> See *Winters & Costello*, *supra* note 134, at 4.

In some situations, no response costs and loss of business costs may be incurred as a result of the unauthorized access. In such situations, the unauthorized access causes no impairment to the protected computer or interruption of service, and, as such, no assessment by a computer consultant or employee is required. An unauthorized accessor may simply copy data containing trade secrets, without damaging the protected computer in any manner.

*Id.*

<sup>143</sup> See *id.*

<sup>144</sup> 18 U.S.C.A § 1030(e)(8) (West 2008).

<sup>145</sup> Compare, e.g., *Creative Computing*, 386 F.3d at 935 (broad construction of “damage”), with *Resdev, LLC v. Lot Builders Ass’n*, No. 6:04–CV–1374ORL31DAB, 2005 WL 1924743, at \*4 (M.D. Fla. Aug. 10, 2005) (narrow construction of “damage”).

<sup>146</sup> See *Four Seasons Hotels & Resorts B.V. v. Consorcio Barr, S.A.*, 267 F. Supp. 2d 1268, 1324 (S.D. Fla 2003) (awarding \$2,118,000 in compensatory damages to the plaintiff under the CFAA for damage to the plaintiff’s trade secrets), *aff’d in part, rev’d in part without opinion*, 138 F. App’x 297 (11th Cir. 2005).

<sup>147</sup> See, e.g., *Garelli Wong & Assocs., Inc. v. Nichols*, 551 F. Supp. 2d. 704, 710 (N.D. Ill. 2008) (asserting that the taking of a trade secret alone does not impair the integrity of the information and, therefore, does not constitute damage under the CFAA).

<sup>148</sup> 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

<sup>149</sup> *Id.* at 1126–28.

computer-stored trade secrets.<sup>150</sup> The former employee, while still working for the plaintiff but acting as an agent for the defendant, emailed trade secrets and other confidential information owned by the plaintiff to the defendant.<sup>151</sup> As there was no tangible harm to the information, the court had to determine whether this act constituted “damage” under the CFAA.<sup>152</sup>

The court looked at the definition of “damage” and determined that “any impairment to the integrity . . . of data . . . or information” had to include the damage to the trade secrets caused by the former employee.<sup>153</sup> The court reasoned that the word “any” within the definition of “damage” was unambiguous; “any” means “any.”<sup>154</sup> The court also determined that the word “integrity,” which was ambiguous in the computer context, meant “unimpaired or unmarred condition” and the maintaining of information in a protected state.<sup>155</sup> The court held that the CFAA protects intangible information that cannot suffer physical damage the same way that the statute protects tangible information.<sup>156</sup> The court denied the defendant’s motion to dismiss.<sup>157</sup>

Not all courts have taken the same view as the court in *Shurgard*. In *Resdev, LLC v. Lot Builders Ass’n*,<sup>158</sup> the United States District Court for the Middle District of Florida focused on the “loss” and “damage” definitions within the CFAA and applied a more limited view of those terms to the trade secret claims.<sup>159</sup> Two former employees of the plaintiff joined the defendant company and improperly accessed the plaintiff’s website, taking information from one of its databases.<sup>160</sup> Plaintiff argued that the defendants unlawfully obtained the plaintiff’s trade secrets through unauthorized web-access.<sup>161</sup> The Plaintiff sought to recover damages based on the trade secret’s lost value.<sup>162</sup> The court proceeded with a detailed statutory construction of the CFAA’s “loss” and “damage” definitions.<sup>163</sup> The court held that the lost value of a trade secret was not a cognizable loss under the CFAA because the alleged lost revenue was neither a “but-for” result nor a “proximate consequence” of the damage associated with the unauthorized access and, therefore, it could not warrant compensatory damages.<sup>164</sup> Further, the court defined “integrity,” a word used in the CFAA definition of “damage,” as “wholeness” or “soundness” and stated that “integrity” does not contemplate the loss of a trade secret.<sup>165</sup>

---

<sup>150</sup> *Id.* at 1123.

<sup>151</sup> *Id.*

<sup>152</sup> *Id.* at 1126.

<sup>153</sup> *Id.* at 1126–27; 18 U.S.C.A. § 1030(e)(8) (West 2008).

<sup>154</sup> *Id.* at 1126.

<sup>155</sup> *Id.*

<sup>156</sup> *Id.*

<sup>157</sup> *Id.* at 1129.

<sup>158</sup> No. 6:04–CV–1374ORL31DAB, 2005 WL 1924743 (M.D. Fla. Aug. 10, 2005).

<sup>159</sup> *See id.* at \*2–6.

<sup>160</sup> *Id.* at \*1.

<sup>161</sup> *Id.*

<sup>162</sup> *See id.* at \*4.

<sup>163</sup> *Id.* at \*2.

<sup>164</sup> *Id.* at \*4.

<sup>165</sup> *Id.* at \*5 n.3 (“Integrity,’ however, ordinarily means ‘wholeness’ or ‘soundness,’ and contemplates, in this context, some diminution in the completeness or useability of data or information on a computer system.” (citation omitted)).

## II. ANALYSIS

The CFAA protects all data stored on any computer used in the course of business.<sup>166</sup> This makes the CFAA a powerful weapon in the fight against the theft of proprietary information assets.<sup>167</sup> Violations of the CFAA often involve corporate insiders or outsiders.<sup>168</sup> Insiders are employees and third parties, such as consultants, who have a fiduciary duty under agency, contract, and employment law to hold a company's trade secrets in confidence and not to use them for the benefit of others.<sup>169</sup> Outsiders are basically everyone else.<sup>170</sup> For the purpose of litigation under the CFAA, however, outsiders include computer hackers, competitors, and competitive intelligence professionals.<sup>171</sup>

It is undisputed that the CFAA applies to: (1) outsiders who never have authorization to access a business's computers, network, or trade secrets, (2) employee insiders who never possessed authorization to access the proprietary information, and (3) employee insiders who go beyond the parameters of their authorized access.<sup>172</sup> CFAA disputes arise when an employee insider, amongst other things, inflicts damage to a computer, places a virus on a corporate network, spoofs network IP addresses, misuses computer passwords, copies confidential files, or misappropriates trade secrets while the employee possesses authorization to access

---

<sup>166</sup> Akerman & Stroz, *supra* note 17, at B8 (“The CFAA protects all valuable computer data, whether or not it would be considered a trade secret.”); Levinson & Paetsch, *supra* note 48, at 24 (“Any information, whether or not it is secret, can be protected under the CFAA. All that most sections of the statute require is that the information be stored on a computer.”).

<sup>167</sup> See Levinson & Paetsch, *supra* note 48, at 24 (“The CFAA has the potential to be a powerful weapon in the arsenal of statutes designed to prevent and remedy the theft or misuse of information. . . . The significance of this should not be underestimated.”).

<sup>168</sup> S. REP. NO. 104–357, at 9 (1996).

<sup>169</sup> HALLIGAN & WEYAND, *supra* note 1, at 63. It is both easier and more common for insiders to steal proprietary information than for a theft by outsiders because insiders are authorized to be on the computers and access the trade secret. *Id.* at 81–82. Companies face a catch–22 because they must disclose trade secrets to employees, consultants, and contractors when necessary in order to perform their functions, but every disclosure to an insider runs the risk of damage to the proprietary trade secret information. *Id.* at 82.

<sup>170</sup> *Id.* at 63.

<sup>171</sup> See *id.* Outside access by improper means includes access by fraud, trespass, theft, hacking, and inducing an insider to breach a duty owed to its employer. *Id.* at 72–79. Access by hacking is the most common form of outsider access and it is defined as “unauthorized access to information on the company's computers through their electronic connections to the outside world.” *Id.* at 77.

<sup>172</sup> See *Lockheed Martin Corp. v. Speed*, 81 U.S.P.Q.2d (BNA) 1669, 1674–75 (M.D. Fla. 2006); Stevens & Carlson, *supra* note 69, at 4 (“According to the *Lockheed* court's analysis, the plain language of the CFAA reveals clearly that the CFAA was meant to apply to two distinct groups: those without authorization (for example, outsiders or hackers) and those who have authorized access but exceed it.”). Although *Lockheed* explicitly referred to only two groups, outsiders (those without authorization) and insiders who go beyond their authorized access (those who exceed authorized access), *Lockheed Martin*, 81 U.S.P.Q. (BNA) at 1675, the CFAA must also apply to those insiders who never possessed authorization at all. There is no principled reason to distinguish between outsiders who clearly never possessed authorization and insiders who also never possessed authorization.

the computer or the trade secret information.<sup>173</sup> It is this last fact scenario that most often leads to trade secret theft, but it is not evident that courts will afford aggrieved parties the benefits of the CFAA in this situation. This analysis focuses on the two essential issues that must be resolved in order to determine if the CFAA will protect a business that suffers a trade secret loss at the hands of an employee or former employee who had authorization to access the computer and the trade secrets, but subsequently misappropriated the information. The issues surround the meaning of unauthorized access, including both “without authorization” and “exceeds authorized access,” and the losses and damages covered by the CFAA.

*A. What Is the Meaning of “Without Authorization” and “Exceeds Authorized Access”?*

Central to the CFAA analysis in trade secrets litigation is an exploration of the terms “without authorization” and “exceeds authorized access.” This is so because any CFAA cause of action requires the violation to be caused by a party without authorization to access the computer or the trade secret information.<sup>174</sup> Further, three of the causes of action also support a violation of the CFAA by a party that exceeds its authorized access to a computer or the trade secret information.<sup>175</sup>

*1. Broad Interpretation of “Without Authorization”*

The broad interpretation of the term “without authorization” can be characterized as a subjective approach.<sup>176</sup> It looks to the mindset of the employee and the surrounding circumstances at the time of the misappropriation in order to determine when the employee’s authorization to access the computer and the computer–stored trade secret ceased to exist. The broad interpretation of “without authorization” in the CFAA advanced by *Shurgard* and *Citrin* finds legal justification in the fundamental precepts of agency law.<sup>177</sup> The tenets of agency law run through

---

<sup>173</sup> See Stevens & Carlson, *supra* note 69, at 2 (“The line blurs when an employee is planning to leave his job and, while still employed and still authorized to use his employer’s computer system, uses that system for purposes adverse to the employer’s interest.”).

<sup>174</sup> See 18 U.S.C.A. § 1030(a)(2)(A), (a)(2)(C), (a)(4), (a)(5)(A)–(C) (West 2008).

<sup>175</sup> See *id.* § 1030(a)(2)(A), (a)(2)(C), (a)(4).

<sup>176</sup> Cf. *Lockheed Martin*, 81 U.S.P.Q.2d (BNA) at 1675 (“Congress singled out those accessing ‘without authorization’ . . . and those ‘exceeding authorization’ . . . while purposefully leaving those in the middle untouched (those accessing *with* authorization), regardless of their *subjective* intent.” (second emphasis added)). Although the *Lockheed Martin* court ultimately embraced the narrow interpretation of unauthorized access, it distinguished *Int’l Airport Ctrs. v. Citrin*, 440 F.3d 418 (7th Cir. 2006) and *Shurgard Storage Ctrs. Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp 2d 1121 (W.D. Wash. 2000), which both embraced the broad interpretation of unauthorized access. *Lockheed Martin*, 81 U.S.P.Q.2d (BNA) at 1674–75. While distinguishing *Citrin* and *Shurgard*, the *Lockheed Martin* court made explicit what those decisions left implicit; the broad interpretation of unauthorized access is a subjective inquiry. *Id.* at 1675.

<sup>177</sup> See *Citrin*, 440 F.3d at 420–21; *Shurgard*, 119 F. Supp 2d. at 1124–25.

the employer-employee relationship and provide legal meaning to the relationship.<sup>178</sup> Therefore, agency law should determine whether an employee possesses authorization to act on behalf of the employer, or possesses authorization to access information.<sup>179</sup> An agent is subject to a duty to act in the best interests of the principal in all aspects of the agency relationship.<sup>180</sup> When an agent intentionally acts contrary to the best interests of the principal, the agent's interests become adverse to the principal's.<sup>181</sup> The agent's adverse interests, if unknown to the principal, immediately terminate the relationship.<sup>182</sup> A serious breach of loyalty by the agent also terminates the relationship.<sup>183</sup> Thus, when the agency relationship terminates, any authority the agent possessed to access the principal's computers immediately ceases to exist.<sup>184</sup>

In the context of the CFAA, the United States Court of Appeals for the Seventh Circuit expressly included agency principles within the meaning of "without authorization."<sup>185</sup> It found that when an employee destroys his employer's proprietary electronic or computer-stored trade secret assets, he breaches the duty of loyalty imposed on him by agency law.<sup>186</sup> The only basis for authority to access the trade secret information is the employment relationship, and breaching the duty of loyalty ends that agency relationship.<sup>187</sup> With the termination of the agency relationship, therefore, the employee loses all authorization to access its employer's confidential information.<sup>188</sup> This approach does not look at the CFAA in a vacuum; rather, it considers the alleged misappropriator's mindset, the context, and the

---

<sup>178</sup> See HAROLD GILL REUSCHLEIN & WILLIAM A. GREGORY, *THE LAW OF AGENCY AND PARTNERSHIP* 3 (2nd ed. 1990) ("We usually characterize the employees of enterprises which mine, manufacture, buy, sell or transport, as servants, but they also fall within the general category of agents, inasmuch as their work is performed subject to the direction of and for the benefit of their employers.").

<sup>179</sup> See *Shurgard*, 119 F. Supp. 2d at 1124–25.

<sup>180</sup> RESTATEMENT (SECOND) OF AGENCY § 387 (1958) ("Unless otherwise agreed, an agent is subject to a duty to his principal to act solely for the benefit of the principal in all matters connected with his agency.").

<sup>181</sup> See *Citrin*, 440 F.3d at 421 ("Violating the duty of loyalty, or failing to disclose adverse interests, voids the agency relationship.").

<sup>182</sup> 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 . . .").

<sup>183</sup> *Id.* ("Unless otherwise agreed, the authority of an agent terminates if, without knowledge of the principal, . . . he is otherwise guilty of a serious breach of loyalty to the principal.").

<sup>184</sup> *Citrin*, 440 F.3d at 420–21.

[Defendant's] breach of his duty of loyalty terminated his agency relationship (more precisely, terminated any rights he might have claimed as [Plaintiff's] agent—he could not by unilaterally terminating any duties he owed his principal gain an advantage!) and with it his authority to access the laptop, because the only basis of his authority had been that relationship.

*Id.*

<sup>185</sup> *Id.* at 419–21.

<sup>186</sup> *Id.* at 421; see also 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").

<sup>187</sup> *Citrin*, 440 F.3d at 420–21.

<sup>188</sup> *Id.* (terminating the agency relationship terminates any authority that stems from that relationship).

circumstances surrounding the misuse when determining whether the alleged misappropriator actually had authorization.

## 2. *Narrow Interpretation of “Without Authorization”*

In contrast to the subjective approach associated with the broad interpretation, the narrow interpretation of unauthorized access can be characterized as an objective approach focusing only on whether the employee possessed permission to access the computer and the computer-stored trade secrets.<sup>189</sup> Under this approach, if the employer granted the employee authorization to the data or computer at any time, the employee’s access cannot be unauthorized, making the employee’s mindset irrelevant. The narrow interpretation to the CFAA relies solely on the text of the statute and declines to read in the principles of agency law or other extrinsic materials in the interpretation of “without authorization.”<sup>190</sup> Proponents of the narrow interpretation utilize rules of statutory construction to derive the meaning of the undefined statutory term “without authorization.”<sup>191</sup> “The first rule in statutory construction is to determine whether the language at issue has a plain and unambiguous meaning with regard to the particular dispute.”<sup>192</sup> If Congress used clear statutory language, so the argument goes, a court should not rely on extrinsic materials such as legislative history or restatements of the law to derive the meanings of terms.<sup>193</sup> Where Congress used ambiguous statutory language, courts should focus on the larger statutory context and resort to extrinsic materials only if the plain meaning of the statute’s words produces an absurd result.<sup>194</sup>

The court in *Lockheed Martin* applied the rules of statutory construction and concluded that the plain language of the CFAA singles out only two groups of people who could be “without authorization” as used in the statute.<sup>195</sup> According to the court, only outsiders, such as hackers or employees with no authorization to access computers, and insiders who go beyond their permitted access and exceed their authorized access are without authorization.<sup>196</sup> Under the narrow interpretation of the CFAA, the statute does not apply to employees who are authorized to access

---

<sup>189</sup> See *Lockheed Martin*, 81 U.S.P.Q.2d (BNA) at 1675 (“Congress singled out those accessing ‘without authorization’ . . . and those ‘exceeding authorization’ . . . while purposefully leaving those in the middle untouched (those accessing *with* authorization), regardless of their subjective intent.”).

<sup>190</sup> *Id.* at 1672–73.

<sup>191</sup> See *Resdev, LLC v. Lot Builders Ass’n*, No. 6:04–CV–1374ORL31DAB, 2005 WL 1924743, at \*2 (M.D. Fla. Aug. 10, 2005) (“This case turns primarily on statutory construction.”).

<sup>192</sup> *Lockheed Martin*, 81 U.S.P.Q.2d (BNA) at 1673 (quoting *Shotz v. City of Plantation*, 344 F.3d 1161, 1167 (11th Cir. 2003)).

<sup>193</sup> *Resdev*, 2005 WL 1924743, at \*2 (citing *Shotz*, 344 F.3d at 1167).

<sup>194</sup> *Lockheed Martin*, 81 U.S.P.Q.2d (BNA) at 1673. (“There is one instance where extrinsic materials are permitted to define a term: when the statutory language either produces a clearly absurd result or presents a substantial ambiguity.” (citing *Shotz*, 344 F.3d at 1167.)).

<sup>195</sup> *Id.* at 1675 (“Congress singled out those accessing ‘without authorization’ (or below authorization) and those ‘exceeding authorization’ (or above authorization) while purposefully leaving those in the middle untouched (those accessing *with* authorization), regardless of their subjective intent.”).

<sup>196</sup> *Id.* at 1673.

computers and computer-stored trade secrets, but whose use of the computer or trade secret information is improper.<sup>197</sup>

### 3. “Exceeds Authorized Access”

Determining the meaning of unauthorized access does not stop at defining “without authorization” because the statute provides a civil cause of action for violations caused by those who exceed their authorized access as well.<sup>198</sup> The United States Court of Appeals for the Seventh Circuit stated that the difference between the meaning of “without authorization” and “exceeds authorized access” is “paper thin.”<sup>199</sup> The CFAA definition of “exceeds authorized access” is “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.”<sup>200</sup> In *Lockheed Martin*, the court stated that the plain meaning of “exceeds authorized access” is “to go beyond the access permitted.”<sup>201</sup> Thus, in the context of accessing a computer or computer-stored trade secrets, the meaning of “exceeds authorized access” should be clear.<sup>202</sup>

Indeed, Congress expounded on the definition of “exceeds authorized access” in the legislative history of the CFAA. In 1986, Congress added the term “exceeds authorized access” into the CFAA causes of action<sup>203</sup> in order to make the language of those causes of action less “cumbersome.”<sup>204</sup> Congress intended the “change to simplify the language in” the CFAA.<sup>205</sup> The old statutory language read “knowingly accesses a computer without authorization, *or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such*

---

<sup>197</sup> See, e.g., *id.*

Because Lockheed permitted the Employees to access the company computer, they were not without authorization. Further, because Lockheed permitted the Employees to access the precise information at issue, the Employees did not exceed authorized access. The Employees fit within the very group that Congress chose not to reach, *i.e.*, those with access authorization.

*Id.*

<sup>198</sup> 18 U.S.C.A. § 1030(a)(2)(A), (a)(2)(C), (a)(4) (West 2008); see *Int’l Airport Ctrs. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006).

<sup>199</sup> *Citrin*, 440 F.3d at 420 (“The difference between without authorization and exceeding authorized access is paper thin.”).

<sup>200</sup> See 18 U.S.C.A. § 1030(e)(6). See generally *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001) (asserting that an employee with authorized access exceeds his authorization by disclosing confidential and proprietary information in violation of his employee confidentiality agreement).

<sup>201</sup> *Lockheed Martin*, 81 U.S.P.Q.2d (BNA) at 1674 (“Without authorization’ means no access authorization and ‘exceeds authorized access’ means to go beyond the access permitted.”).

<sup>202</sup> See S. REP. NO. 99-432, at 13 (1986) (“Section (2)(g) establishes [a] definition[] for . . . the term ‘exceeds authorized access,’ . . . which [is] self-explanatory.”).

<sup>203</sup> Computer Fraud and Abuse Act of 1986, Pub. L. 99-474, § 2(c), 100 Stat. 1213, 1215.

<sup>204</sup> S. REP. NO. 99-432, at 9. (“Section 2(c) substitutes the phrase ‘exceeds authorized access’ for the more cumbersome phrase [it replaces].”).

<sup>205</sup> *Id.* (“The Committee intends this change to simplify the language in 18 U.S.C. 1030(a)(1) and (2), and the phrase ‘exceeds authorized access’ is defined separately in Section (2)(g) of the bill.”).

*authorization does not extend . . .*<sup>206</sup> Congress eliminated this language and added the definition of “exceeds authorized access”<sup>207</sup> to clarify the effect of the statute on Federal employees.<sup>208</sup> Importantly, at this time, the CFAA was an exclusively criminal statute and did not provide a *civil* remedy.<sup>209</sup>

Prior to the 1986 amendment, federal employees were arguably subject to criminal liability under the CFAA if they were authorized to access information but did so for “purposes to which such authorization [did] not extend.”<sup>210</sup>

[The amendment] removes from the sweep of the statute one of the murkier grounds of liability, under which a Federal employee’s access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization. As the committee report points out, administrative sanctions should ordinarily be adequate to deal with real abuses of authorized access to Federal computers (assuming, of course, that no other provision of section 1030 is violated). Like the heightened scienter requirement, this change serves to minimize the likelihood that a Federal employee, uncertain about the scope of his authority, would face a Hobson’s choice between the disclosure mandates of FOIA [Freedom of Information Act] and the criminal sanctions of title 18.<sup>211</sup>

Congress wanted to make the CFAA less murky in situations where access might be legitimate in some circumstances, but criminal in other, “not clearly distinguishable,” circumstances.<sup>212</sup>

In *Werner–Masuda*, the United States District Court for the District of Maryland followed Congress’s mandate and found that an employee did not exceed her authorized access, as defined by the CFAA, when she allegedly misused information because she did not go beyond her permitted *access*.<sup>213</sup> It is possible, however, to draft employment or confidentiality agreements such that an employee’s access may be deemed excessive if the employee violates the agreement through improper use.<sup>214</sup> The agreement’s language must be drafted such that it not only

---

<sup>206</sup> Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. 98-473, ch. 21, sec. 2102, § 1030(a)(1)–(2), 98 Stat. 2190, 2190–91 (emphasis added); S. REP. NO. 99-432, at 9.

<sup>207</sup> § 2(g)(4), 100 Stat. at 1215.

<sup>208</sup> S. REP. NO. 99-432, at 21.

<sup>209</sup> Computer Abuse Amendments Act of 1994, Pub. L. 103-322, § 29001(d), 108 Stat. 2097, 2098 (adding a civil action to the CFAA in 1994).

<sup>210</sup> S. REP. NO. 99-432, at 21.

<sup>211</sup> *Id.*

<sup>212</sup> *Id.*

<sup>213</sup> *Int’l Ass’n of Machinists & Aerospace Workers v. Werner–Masuda*, 390 F. Supp. 2d 479, 499 (D. Md. 2005) (“[Defendant] was authorized to access the information contained in [the database], and that at the time she was allegedly accessing it on behalf of [the competitor], her access had not been revoked.”).

<sup>214</sup> *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582 (1st Cir. 2001) (“[Plaintiff] is likely to prove such excessive access based on the confidentiality agreement between [Defendant] and [Plaintiff].”); *see also* *Hewlett–Packard Co. v. Byd:Sign, Inc.*, No. 6:05-CV-456, 2007 WL 275476, at \*13 (E.D. Tex. Jan. 25, 2007).

[Plaintiff] has actually alleged that the Defendants had agreed [in a signed confidentiality agreement] not only to refrain from disclosing information, but

prohibits certain *uses*, but also delineates the point where an employee's authorized *access* ends, and liability under the CFAA begins.<sup>215</sup>

*B. Does the Misappropriation of a Trade Secret Constitute "Damage" Under the CFAA?*

In addition to the analysis of what constitutes unauthorized access under the CFAA, it is also necessary to analyze the "damage" requirement within the statute.<sup>216</sup> The CFAA provides a civil remedy in the form of compensatory damages or injunctive relief to "any person who suffers *damage* or *loss* by reason of a violation of this section."<sup>217</sup> A problem surfaces in trade secret misappropriation cases where the computer system, data, or information is not damaged, in the traditional physical sense of the word, because the files are merely improperly accessed, copied, transferred, or moved to a non-secure device.<sup>218</sup> The issue is whether the misappropriation of a computer-stored trade secret, or the use of a protected computer to misappropriate a trade secret, will constitute "damage" under the CFAA. There are three perspectives to consider in this regard. The first is that misappropriation of a trade secret does not constitute "damage."<sup>219</sup> The second is that misappropriation of a trade secret, coupled with other harm, constitutes

---

also to refrain from sending or accessing messages on [Plaintiff's] computer systems for personal gain. By doing so, [Plaintiff] has alleged more than misappropriation of trade secrets, but has alleged actual access without or in excess of authorization. This is enough to defeat the Moving Defendants' motion to dismiss as to [Plaintiff's] claims under §§ 1030(a)(2) and 1030(a)(4).

*Id.*

<sup>215</sup> See *Werner-Masuda*, 390 F. Supp. 2d at 498 (reasoning that by signing the employer's registration agreement, the employee agreed "*not to use the information*" contrary to the policies of the employer, but her conduct did not exceed her authorized *access*).

<sup>216</sup> 18 U.S.C.A. § 1030(g) (West 2008).

<sup>217</sup> *Id.* Section 1030(g)'s requirement of "damage or loss" is phrased in the disjunctive. *Id.* Certain CFAA causes of action, however, specifically require a showing of "damage," *id.* § 1030(a)(5)(A), or *both* "damage *and* loss," *id.* § 1030(a)(5)(C). Thus, a showing of "damage," without more, gives a plaintiff more swords under the CFAA than a showing of "loss," without more. Further, trade secret misappropriation arguably fits better within the CFAA's definition of "damage," than it does "loss."

<sup>218</sup> See *Winters & Costello*, *supra* note 134, at 4.

In some situations, no response costs and loss of business costs may be incurred as a result of the unauthorized access. In such situations, the unauthorized access causes no impairment to the protected computer or interruption of service, and, as such, no assessment by a computer consultant or employee is required. An unauthorized accessor may simply copy data containing trade secrets, without damaging the protected computer in any manner. However, it is in these situation where the most harm is done to trade secrets.

*Id.*

<sup>219</sup> See *Lockheed Martin Corp. v. Speed*, 81 U.S.P.Q.2d (BNA) 1669, 1676 (M.D. Fla. 2006) (copying of confidential data does not constitute "damage" under the CFAA); *Resdev, LLC v. Lot Builder Ass'n, Inc.*, No. 6:04-CV-1374ORL31DAB, 2005 WL 1924743, at \*5 n.3 (M.D. Fla. Aug. 10, 2005) (noting that "damage" contemplates "some diminution in the completeness or useability of data or information on a computer system").

“damage.”<sup>220</sup> And the third is that the very misappropriation of a trade secret, without more, constitutes “damage” under the CFAA.<sup>221</sup>

*1. First Perspective: Misappropriation Does Not Constitute “Damage”*

Courts adopting this view derive its foundation from rules of statutory construction and a limited view of the plain meaning of the CFAA.<sup>222</sup> This perspective asserts that the meaning of the word “integrity,” found in the definition of “damage,” is clear and that courts should not rely on extrinsic materials to derive meaning for the term “damage.”<sup>223</sup> The CFAA defines “damage” as “any impairment to the integrity or availability of data, a program, a system, or information.”<sup>224</sup> According to this view, the unauthorized copying or emailing of confidential or proprietary information, without deletion or removal of the information, would not constitute “damage” within the plain meaning of the CFAA because there is no impairment to the data, information, or a system.<sup>225</sup> The limited perspective focuses on the word “integrity” in the definition of damage.<sup>226</sup> One meaning of “integrity” is “wholeness” or “soundness.”<sup>227</sup> Therefore, to have “damage” under the CFAA, there must be “some diminution in the completeness or useability of the data or information on a computer system.”<sup>228</sup> The first perspective hinges on a physical change in the data, program, system, or information.<sup>229</sup>

---

<sup>220</sup> See *Black & Decker (US), Inc. v. Smith*, 568 F. Supp. 2d. 929, 937 (W.D. Tenn. 2008) (misappropriating a trade secret coupled with other harm to the data constituted “damage” under the CFAA); cf. *Garelli Wong & Assocs., Inc. v. Nichols*, 551 F. Supp. 2d. 704, 710 (N.D. Ill. 2008) (misappropriating a trade secret alone does not constitute “damage” under the CFAA).

<sup>221</sup> See *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1126 (W.D. Wash. 2000) (“The word ‘integrity’ in the context of data necessarily contemplates maintaining the data in a protected state. . . . [T]hus ‘damage’ could include the alleged access and disclosure of trade secrets in this case.”).

<sup>222</sup> See *Lockheed Martin*, 81 U.S.P.Q.2d (BNA) at 1673 (“Because the plain language is sufficient to interpret the disputed terms, this Court need not resort to extrinsic materials.”); *Resdev*, 2005 WL 1924743, at \*2 (“This case turns primarily on statutory construction.”).

<sup>223</sup> *Resdev*, 2005 WL 1924743, at \*5 n.3.

<sup>224</sup> 18 U.S.C.A. § 1030(e)(8) (West 2008).

<sup>225</sup> *Lockheed Martin*, 81 U.S.P.Q.2d (BNA) at 1676 (“The copying of information from a computer onto a CD or PDA is a relatively common function that typically does not, by itself, cause permanent deletion of the original computer files. In the absence of an allegation of permanent deletion or removal, the Court will not create one.”); cf. *Worldspan, L.P. v. Orbitz, LLC*, No. 05-C-5386, 2006 WL 1069128, at \*5 (N.D. Ill. 2006) (parroting the “damage” text of the CFAA without alleging facts of impairment to the completeness, useability, or availability of the data was not enough to meet the CFAA damage requirement).

<sup>226</sup> *Resdev*, 2005 WL 1924743, at \*5 n.3; see also *Garelli Wong & Assocs., Inc. v. Nichols*, 551 F. Supp. 2d. 704, 709 (N.D. Ill. 2008) (following *Resdev*); *Orbitz*, 2006 WL 1069128 at \*5 (following *Resdev*).

<sup>227</sup> See *Resdev*, 2005 WL 1924743, at \*5 n.3 (citing the OXFORD ENGLISH REFERENCE DICTIONARY 731 (Judy Pearsall & Bill Trumble eds., rev. 2d ed. 2002)).

<sup>228</sup> *Id.*

<sup>229</sup> *Id.* at \*4–5.

### 2. *Second Perspective: Misappropriation Plus Other Harm Constitutes “Damage”*

The second perspective builds on the first, holding that trade secret misappropriation, alone, does not constitute damage under the CFAA.<sup>230</sup> Rather, the “damage” requirement can be met when the misappropriation is coupled with other harm.<sup>231</sup> Intentional conduct that renders a computer system less secure, even though there was no damage or destruction to the actual data, program, system, or information, constitutes “damage” under the CFAA.<sup>232</sup> Other harm that qualifies can include, among other things, transferring data from a secure server to a non-secure device or external drive,<sup>233</sup> spoofing IP addresses,<sup>234</sup> or misusing and improperly accumulating valid network passwords.<sup>235</sup>

### 3. *Third Perspective: Misappropriation Alone Constitutes “Damage”*

The third perspective of “damage” holds that trade secret misappropriation alone should meet the “damage” requirement of the CFAA.<sup>236</sup> The third perspective relies on both the plain language of the statute as well and the legislative history because the word “any” within the definition of “damage” is unambiguous while the word “integrity” within the definition of “damage” is ambiguous.<sup>237</sup> The word “any” is not ambiguous and, in the context of “damage” under the CFAA, it applies to any damage to the integrity of the data.<sup>238</sup> The word “integrity,” however, is ambiguous.<sup>239</sup> Another definition of “integrity” is “unimpaired” or “unmarred.”<sup>240</sup> In the context of electronic trade secrets or computer-stored trade secrets, “integrity” means maintaining the data in a protected state.<sup>241</sup> Thus, making a trade secret less

---

<sup>230</sup> *Garelli Wong & Assocs., Inc. v. Nichols*, 551 F. Supp. 2d. 704, 710 (N.D. Ill. 2008).

<sup>231</sup> *Black & Decker (US), Inc. v. Smith*, 568 F. Supp. 2d. 929, 937 (W.D. Tenn. 2008) (misappropriating a trade secret coupled with other harm to the data constituted “damage” under the CFAA).

<sup>232</sup> *Id.* (“The legislative history of the [CFAA] supports the conclusion that intentionally rendering a computer system less secure should be consider ‘damage’ under § 1030(a)(5)(A), even when no data, program, or system, is damaged or destroyed.”).

<sup>233</sup> *Id.* (“This case is distinguishable from *Nichols*, and *Lockheed Martin* however, because the Complaint alleges that, in addition to copying certain information, [Defendant] transferred certain confidential documents from a secure server to a non-secure shared company drive.”).

<sup>234</sup> *Four Seasons Hotels & Resorts B.V. v. Consorcio Barr, S.A.*, 267 F. Supp. 2d 1268, 1322 (S.D. Fla 2003), *aff’d in part, rev’d in part without opinion*, 138 F. App’x 297 (11th Cir. 2005).

<sup>235</sup> *See* S. REP. NO. 104-357, at 11 (1996) (copying or altering existing network passwords constitutes “damage” within the CFAA).

<sup>236</sup> *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1126–28 (W.D. Wash. 2000).

<sup>237</sup> *Id.* at 1126 (“The unambiguous meaning of ‘any’ clearly demonstrates that the statute is meant to apply to ‘any’ impairment to the integrity of data. However, the word ‘integrity’ is ambiguous in this context.”).

<sup>238</sup> *Id.*

<sup>239</sup> *Id.*

<sup>240</sup> *See id.* (“[A]n unimpaired or unmarred condition: entire correspondence with an original condition.” (quoting WEBSTER’S THIRD NEW INTERNATIONAL DICTIONARY 1174 (Philip Babcock Gove ed. 1993))).

<sup>241</sup> *See id.* (“The word ‘integrity’ in the context of data necessarily contemplates maintaining the data in a protected state.”).

secure by exposing it to additional parties inevitably damages the information's "integrity."<sup>242</sup> Seeing that there are many ordinary meanings for the word "integrity," courts may rely on the legislative history of the CFAA to determine the meaning of the word "damage".<sup>243</sup>

The legislative history states, "the definition of 'damage' is amended to be sufficiently broad to encompass the types of harm against which people should be protected."<sup>244</sup> The CFAA does not require physical change, erasure, or destruction of the data in order for there to be "damage" under the statute.<sup>245</sup> Damage to intangible information, such as a network login password or a trade secret, is within the purview of the CFAA.<sup>246</sup>

### III. PROPOSAL

Trade secret litigation is becoming even more complex<sup>247</sup> and many factors can be attributed to this fact. First, a vast majority of trade secrets are intangible,

---

<sup>242</sup> See *Black & Decker (US), Inc. v. Smith*, 568 F. Supp. 2d 929, 937 (W.D. Tenn. 2008) ("[Defendant] transferred certain confidential documents from a secure server to a non-secure shared company drive. The legislative history of the [CFAA] supports the conclusion that intentionally rendering a computer system less secure should be considered 'damage' under § 1030(a)(5)(A), even when no data, program, or system, is damaged or destroyed." (citation omitted)).

<sup>243</sup> *Am. Bankers Ins. Group v. United States*, 408 F.3d 1328, 1332 (11th Cir. 2005) ("[W]ords are given their ordinary, plain meaning unless defined otherwise.").

<sup>244</sup> S. REP. NO. 104-357, at 11 (1996).

<sup>245</sup> See *id.*

The 1994 amendment required both "damage" and "loss," but it is not always clear what constitutes "damage." For example, intruders often alter existing log-on programs so that user passwords are copied to a file which the hackers can retrieve later. After retrieving the newly created password file, the intruder restores the altered log-on file to its original condition. 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.

*Id.*

<sup>246</sup> See *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1126-27 (W.D. Wash. 2000).

This example given in [Senate Report 357] is analogous to the case before the Court. The "damage" and thus violation to the "integrity" that was caused in the example is the accumulation of passwords and subsequent corrective measures the rightful computer owner must take to prevent the infiltration and gathering of confidential information. Similarly, in this case, the defendant allegedly infiltrated the plaintiff's computer network, albeit through different means than in the example, and collected and disseminated confidential information. In both cases no data was physically changed or erased, but in both cases an impairment of its integrity occurred.

*Id.*

<sup>247</sup> See *Hofer & Gullotti*, *supra* note 11, at 151-52 ("[T]rade secret litigation is not for the faint of heart.").

digital, and stored on computers.<sup>248</sup> Second, the proliferation of new technologies such as PDAs, digital cameras, camera enabled cell phones, instant messengers, and Universal Serial Bus (“USB”) flash drives make copying and transferring confidential data simple for anyone with access.<sup>249</sup> Third, technology has made the world a much smaller place. Employees may live in one state, but work across the country in another, and the workforce is highly mobile.<sup>250</sup> The Internet and ease of travel allows business to be conducted anywhere.<sup>251</sup> And because of technology, the marketplace is no longer only national, but global.<sup>252</sup> Technology provides legitimate avenues for conducting business internationally, but technology also opens the door to foreign economic espionage.<sup>253</sup> Lastly, trade secret litigation is time sensitive, requiring quicker adjudication and more liberal discovery.<sup>254</sup> All of these factors point to the conclusion that litigators will require access to the federal courts in order to provide the most effective means for protecting trade secret assets. As there is no federal trade secret statute, the CFAA can fill the gap in the law, and afford plaintiffs federal subject matter jurisdiction. But more importantly, the CFAA also has the ability to provide modern protection for electronic and computer-stored trade secrets.<sup>255</sup>

In order to ensure access to the federal courts and provide the widest amount of protection for trade secrets owners, this comment proposes that federal courts apply

---

<sup>248</sup> See Cundiff, *supra* note 19, at 714 (“Many valuable trade secrets, however, are created, developed, updated or maintained in a collaborative digital environment. Thus most trade secrets owners will need to focus on computer security as they assess how to protect their trade secrets.”).

<sup>249</sup> *Id.* at 715.

Digital technology is capable of not only protecting trade secrets, of course; it can also place them at substantial risk. Because so many individuals regularly carry their own personal devices for generating and recording (such as cameras in cell phones), storing (such as USB drives and iPods), and transmitting (such as PDAs and instant messaging devices) digital data (and often these functions are combined in one device, such as the iPhone® device), the trade secrets owner will want to consider whether it is feasible to restrict those given access to trade secrets from bringing such devices into highly sensitive areas of the company where the secrets are stored or may be viewed.

*Id.*

<sup>250</sup> Halluin & Westin, *supra* note 10, at 225 (“Because of the increased mobility of employees and the accessibility of the internet, the ease of getting information makes trade secrets difficult to defend.”).

<sup>251</sup> *See id.*

<sup>252</sup> See THOMAS L. FRIEDMAN, *THE WORLD IS FLAT: A BRIEF HISTORY OF THE TWENTY-FIRST CENTURY* (2005) (describing the effects of globalization on American culture and business).

<sup>253</sup> See Cundiff, *supra* note 19, at 714; *see also* ASIS INT’L, *supra* note 2, at 24 (documenting the increasing instances of economic espionage on U.S. companies from foreign countries, mainly China, India, and Russia).

<sup>254</sup> See Hofer & Gullotti, *supra* note 11, at 160–61.

[W]here there is a choice between state and federal court, many litigators express a preference for a federal forum. . . . Often, federal dockets are less crowded than those in the state court. More resources are available to federal judges, including law clerks. In addition, the federal discovery rules tend to be more liberal than their state counterpart.

*Id.*

<sup>255</sup> See Levinson & Paetsch, *supra* note 48, at 24 (“The CFAA has the potential to dramatically enlarge the scope of litigation and liability for misuse of electronically stored information, particularly in connection with trade secrets claims.”).

the broad application of “without authorization.” Further, this comment proposes that courts include trade secret misappropriation within the CFAA definition of “damage.” There is foundation for the broad interpretation of these terms in the principles of agency law, the legislative history of the CFAA, and within the existing body of trade secrets law. The CFAA provides major benefits for litigators and, in turn, the trade secrets owners that suffer from trade secret misappropriation.

*A. Adoption of the Broad Interpretation of “Without Authorization”*

Today, “[e]mployers . . . are increasingly taking advantage of the CFAA’s civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer’s computer system.”<sup>256</sup> In order to ensure that the CFAA civil remedies are available to a company whose former employee misappropriates its trade secrets while the employee possesses authorization to access the computer or trade secret information, courts should adopt the broad interpretation of “without authorization.”<sup>257</sup> Principles of agency law and the fundamental precept that employees are granted authorization to access and use a trade secret only for a limited purpose provide two sound and common-sense avenues for understanding the CFAA term “without authorization.”

*1. Agency Law and “Without Authorization”*

When a violation of the CFAA involves an employee or former employee, courts should adopt the broad interpretation of the statutory phrase “without authorization” and include principles of agency law in its analysis of the violation. The broad interpretation asserts that an employee is “without authorization” when the employee acts with adverse interests to the employer’s or is responsible for a serious breach of the duty of loyalty owed to its employer and acts for the benefit of a competitor.<sup>258</sup> Once the employee develops an adverse mindset regarding the use of its employer’s confidential information, the employee’s authorization immediately ceases to exist.<sup>259</sup> The CFAA focuses on unauthorized access<sup>260</sup> and an employee’s authority to act derives from agency law, therefore the concept of an employee’s

---

<sup>256</sup> Pac. Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1196 (E.D. Wash. 2003).

<sup>257</sup> See Int’l Airport Centers, L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000).

<sup>258</sup> Citrin, 440 F.3d at 421 (noting that the authority of an agent terminates when the agent’s interests become adverse to the principal’s, even if the principal does not have knowledge of it, or when the employee seriously breaches his duty of loyalty to the principal); Shurgard, 119 F. Supp. 2d at 1125 (stating that the authority of a plaintiff’s former employees’ authorization ended when the employees became disloyal to the plaintiff and acted as agents for the defendant); see 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.”).

<sup>259</sup> See Citrin, 440 F.3d at 421.

<sup>260</sup> See, e.g., 18 U.S.C.A. § 1030(a)(2)(A), (a)(2)(C), (a)(4), (a)(5)(A)–(C) (West 2008); EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 63 (1st Cir. 2003) (“[L]ack of authorization may be implicit, rather than explicit.”).

authorization terminating due to a serious breach of loyalty should be read into the CFAA.<sup>261</sup> This interpretation makes sense when the CFAA violation deals with an employee because the principles of agency law provide the bedrock for the employee–employer relationship and agency law can be applied to all business organizations.<sup>262</sup> Further, agency law principles are also read into many commercial state and federal laws.<sup>263</sup> The application of agency principles within different laws is not novel; rather it is fundamental and should not be overlooked when evaluating a CFAA claim.

## 2. *The “Limited License” and “Without Authorization”*

In addition to applying agency principles, when a violation of the CFAA involves stolen trade secret information, courts should adopt a broad interpretation of the statutory phrase “without authorization” because any authorization to use or access a trade secret is given with a “limited license.” This concept asserts that an employee only possesses a “limited license” to use and access a trade secret for a particular purpose, which limits any authorization to that specific use or purpose.<sup>264</sup> Under the law of trade secrets, information would not constitute a trade secret if the party with access to the information, or the computers storing it, were authorized to use the information in *any* way and for *any* purpose.<sup>265</sup> If access and use were not limited, the information would not be subject to reasonable measures to maintain its secrecy and, thus, never obtain the protections of a trade secret.<sup>266</sup> Because of the

---

<sup>261</sup> See RESTATEMENT (SECOND) AGENCY § 7 cmt. a (1958) (“‘Authority’ . . . is the power of the agent to do an act or to conduct a transaction on account of the principal which, with respect to the principal, he is privileged to do because of the principal’s manifestations to him.”).

<sup>262</sup> See REUSCHLEIN & GREGORY, *supra* note 178, at 3–4 (stating that most of the world’s business is conducted by agents and the principles of agency law apply to every business organization).

<sup>263</sup> See, e.g., Truth-in-Lending Act, 15 U.S.C. § 1602(o) (2006) (“The term ‘unauthorized use,’ . . . means a use of a credit card by a person other than the cardholder who does not have actual, implied, or apparent authority for such use and from which the cardholder receives no benefit.”); U.C.C. § 3-402 cmts. 1–2 (2005).

<sup>264</sup> See E-mail from R. Mark Halligan, Partner, Lovells LLP, to author (Oct. 25, 2007, 23:14:00 CDT)(on file with author) (explaining that when an employee has authorized access to a trade secret, that access is granted only for a limited purpose to perform a specific function or task and when that function or task is complete, the employee’s authorized access ceases to exist); R. Mark Halligan, *Safeguarding Secrets: Twelve Predictions for Trade Secret Law in the New Economy*, CORP. COUNS., Jan. 2000, at 44, 46 (predicting that the principle of limited use will be applied in trade secret law).

<sup>265</sup> See *Xantrex Tech. Inc. v. Advanced Energy Indus., Inc.*, No. 07-CV-02324-WYD-MEH, 2008 WL 2185882, at \*17 (D. Col. May 23, 2008) (“To be a ‘trade secret’ the owner thereof must have taken measures to prevent the secret from becoming available to persons other than those selected by the owner to have access thereto for limited purposes.” (quoting COLO. REV. STAT. § 7-74-102 (2008))).

<sup>266</sup> See *Harvey Barnett, Inc. v. Shidler*, 338 F.3d 1125, 1129 (10th Cir. 2003).

Colorado has adopted the Uniform Trade Secrets Act, which defines a trade secret as “any scientific or technical information, design, process, procedure, formula, [or] improvement . . . which is secret and of value.” In order “[t]o be a ‘trade secret’ the owner thereof must have taken measures to prevent the secret from

requirement that trade secret information be the subject of reasonable measures to maintain its secrecy, it would be counterintuitive for an employer not to limit the information's use. Further, an employer would not authorize an employee to access a computer or to obtain the trade secrets stored on the computer for a purpose adverse to the employer, nor would it authorize an employee to alter or use the trade secret information for the employee's personal benefit or for the benefit of a competitor.<sup>267</sup> The circumstances surrounding the acquisition of a trade secret, such as a confidential relationship, lead to an understanding that the trade secret's use is limited and that it must remain confidential.<sup>268</sup>

Trade secret owners can also make a "limited license" express by advising employees in confidentiality agreements, and on the documents containing trade secrets, that their access to the trade secret is for a limited purpose and exceeding that purpose terminates the employee's authorization.<sup>269</sup> Further, in a digital age, reasonable measures to maintain secrecy, as required by trade secret law, should require that access to trade secrets be for limited purposes.<sup>270</sup> Through application of the broad interpretation, the employee who has authorized access to information, but uses it in a way not within the purpose of the authorization, should be treated as "without authorization" in CFAA civil causes of action. The broad interpretation of "without authorization" ensures that employee insiders who might be authorized to access a computer, network, or its trade secrets, if acting within their limited license, cannot avoid liability under the CFAA when they exceed their license.

---

becoming available to persons other than those selected by the owner to have access thereto for limited purposes."

*Id.* (alterations in original) (citation omitted) (quoting § 7-74-102).

<sup>267</sup> See *Victor G. Reiling Assocs. v. Fisher-Price, Inc.*, 450 F. Supp. 2d 175, 184 n.9 (D. Conn. 2006) (quoting *Heyman v. AR. Winarick, Inc.*, 325 F.2d 584, 587 (2d Cir. 1963).

As the prospective buyer is given the information for the limited purpose of aiding him in deciding whether to buy, he is bound to receive the information for use within the ambit of this limitation. He may not in good conscience accept the information; terminate negotiations for the sale; and then, using vital data secured from the would-be seller, set out on a venture of his own.

*Id.*

<sup>268</sup> See Ga. Code Ann. § 10-1-761(2)(B)(ii)(II)-(III) (2008) (defining misappropriation, in pertinent part, as disclosure of a trade secret by, or derived from, a party who was under a duty to limit its use); *Harvey Barnett*, 338 F.3d at 1129 (adopting a version of the UTSA, Colorado recognizes that in order to gain trade secret status, the owner of confidential information must only grant access to that information with the understanding that the authorized access is for a limited purpose).

<sup>269</sup> Cundiff, *supra* note 19, at 717.

Prudent trade secrets owners should explicitly legend highly confidential documents with precautionary language advising those who are given or obtain access to the materials that their access is conditioned on their agreement not to disclose the materials to those not under confidentiality contracts with the trade secrets owner and that any license to view or possess the documents is automatically revoked if the viewer exceeds the stated use.

*Id.*

<sup>270</sup> See *id.* at 718.

### B. Adoption of the Broad Interpretation of Damage

The nature of what constitutes a trade secret and the fundamental principles of trade secret law support the broad interpretation of the statutory term “damage.” Courts should adopt the third perspective of “damage,” discussed *supra*, and include trade secret misappropriation within the meaning of the CFAA term “damage.” This perspective is most appropriate because trade secret misappropriation constitutes “any impairment to the integrity or availability of data . . . or information.”<sup>271</sup> By considering the nature of a trade secret in conjunction with the purpose of the CFAA and its definition of “damage,” the misappropriation of a trade secret falls squarely within the meaning of “damage.”<sup>272</sup> The third and broadest perspective of “damage” holds that the term “any” within the definition of “damage” means just that, “any,” and is unambiguous.<sup>273</sup> Additionally, the ambiguous word “integrity,” in the computer context, means “unimpaired” and maintaining data in a protected state.<sup>274</sup> Further, making a trade secret less secure also constitutes damage.<sup>275</sup>

The United States Supreme Court explicitly held that a trade secret is property.<sup>276</sup> The essence of that property is its secrecy.<sup>277</sup> “[T]he extent of the property right therein is defined by the extent to which the owner of the secret protects his interest from disclosure to others.”<sup>278</sup> Therefore, the integrity of a trade secret, which is an information asset, is only maintained when a limited number of people know its contents. Thus, “damage” to the trade secret’s integrity occurs when more people gain access to the information. A trade secret is not “whole,” it is not “complete,” it is not “unimpaired,” and it is not “unmarred,” all different definitions of integrity applied by federal courts in CFAA cases, when it loses its secrecy.<sup>279</sup> The

---

<sup>271</sup> Compare 18 U.S.C.A. § 1030(e)(8) (West 2008) (defining “damage”), with *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1126 (W.D. Wash. 2000) (holding that trade secret misappropriation may constitute “damage” under the CFAA).

<sup>272</sup> *Shurgard*, 119 F. Supp. 2d at 1126.

<sup>273</sup> *Id.*

<sup>274</sup> *Id.*

The unambiguous meaning of “any” clearly demonstrates that the statute is meant to apply to “any” impairment to the integrity of data. However, the word “integrity” is ambiguous in this context. *Webster’s New International Dictionary* (3d ed. 1993), defines “integrity” as, “an unimpaired or unmarred condition: entire correspondence with an original condition.” The word “integrity” in the context of data necessarily contemplates maintaining the data in a protected state.

*Id.*

<sup>275</sup> *Black & Decker (US), Inc. v. Smith*, 568 F. Supp. 2d 929, 937 (W.D. Tenn. 2008) (transferring confidential documents from a secure server to a non-secure external hard drive renders the computer, and data, less secure, constituting damage under the CFAA even though the data or system was not damaged physically).

<sup>276</sup> *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1002 (1984) (“Trade secrets have many of the characteristics of more tangible forms of property.”).

<sup>277</sup> *Id.*; see also *Levinson & Paetsch*, *supra* note 48, at 24 (“[Trade secret] laws require proof that the information at issue qualifies as a trade secret or at least is confidential – meaning that it is not generally known, it is valuable because of its *secrecy*, and it is subject to reasonable efforts to protect its *secrecy*.” (emphasis added)).

<sup>278</sup> *Ruckelshaus*, 467 U.S. at 1002.

<sup>279</sup> See *Resdev, LLC v. Lot Builders Ass’n, Inc.*, No. 6:04-CV-1374ORL31DAB, 2005 WL 1924743, at \*5 n.3 (M.D. Fla. Aug. 10, 2005) (“wholeness” & “completeness”); *Shurgard Storage*

CFAA defines “damage” as “*any* impairment to the integrity . . . of . . . *information*.”<sup>280</sup> And under the CFAA, Congress intended to protect intangible assets stored on a computer in the same way that the law protects tangible assets.<sup>281</sup> Based on this analysis, trade secret misappropriation must constitute “damage” under the CFAA. The broad interpretation of the term “damage” provides the necessary protection to businesses against theft of their electronic and computer-stored trade secrets. It also allows trade secret litigators to avoid motions to dismiss for failure to claim appropriate “damage.” This allows the CFAA claims and the other state law claims brought within the court’s supplemental jurisdiction to remain in federal court, and it also allows for discovery to continue in the case.

### *C. Benefits of the CFAA*

There is no federal trade secrets statute, but a broad interpretation of the CFAA can act as a gap-filler until Congress explicitly provides for federal protection of trade secrets. There are three main benefits provided by the broad interpretation for national trade secret disputes that cannot be provided by state-based trade secret misappropriation causes of action: (1) the federal courts provide for nationwide service of process, (2) the plaintiff does not have to prove the existence of a trade secret or that reasonable security measures were taken, and (3) there would be more uniformity in the law.

First, the CFAA provides trade secret litigators with federal question subject matter jurisdiction.<sup>282</sup> This provides the benefit of bringing state law causes of action that arise from the same case or controversy as the CFAA claim under the district courts’ supplemental jurisdiction,<sup>283</sup> but more importantly, it provides nationwide service of process.<sup>284</sup> This benefit cannot be downplayed because often in complex trade secret litigation the plaintiff resides in one state, the defendant resides in a different state, and both the evidence of trade secret theft and key witnesses are in different states around the country.<sup>285</sup> Litigating this type of case in state court might require filing motions and proceedings in multiple jurisdictions throughout the country in order to depose key witnesses and obtain necessary evidence.<sup>286</sup> Nationwide service of process avoids this entire situation and saves substantial amounts of time.

---

Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1126 (W.D. Wash 2000) (“unimpaired” & “unmarred”).

<sup>280</sup> 18 U.S.C.A. § 1030(e)(8) (West 2008) (emphasis added).

<sup>281</sup> See *Shurgard*, 119 F. Supp. 2d at 1128 (“[§ 1030(a)(2)(C)] would ensure that the theft of intangible information by the unauthorized use of a computer is prohibited in the same way theft of physical items are protected.” (quoting S. REP. NO. 104-357, at 7 (1996))).

<sup>282</sup> See 28 U.S.C. § 1331 (2006) (“The district courts shall have original jurisdiction of all civil actions arising under the Constitution, laws, or treaties of the United States.”).

<sup>283</sup> See *id.* § 1367(a).

<sup>284</sup> See *id.* § 1391.

<sup>285</sup> See, e.g., *Pepsico, Inc. v. Redmond*, 54 F.3d 1262, 1264–65 (7th Cir. 1995).

<sup>286</sup> Rhonda Wasserman, *The Subpoena Power: Pennoyer’s Last Vestige*, 74 MINN. L. REV. 37, 123–25 (1989) (discussing the reach of subpoenas and the need to rely on the cooperation of other states in order to ensure the ability to reach out-of-state witnesses).

Second, the CFAA does not require the plaintiff to prove that a trade secret exists or that the plaintiff took reasonable efforts to prevent disclosure, both of which are required in all state-based causes of action relying on the UTSA.<sup>287</sup> Many trade secrets lawsuits fail because the plaintiff cannot prove that the information meets the UTSA definition of a trade secret.<sup>288</sup> Parties in trade secret litigation under the UTSA spend substantial amounts of time and resources litigating issues surrounding secrecy.<sup>289</sup> These issues include: (1) the timing and methods for identifying the trade secret, (2) a determination of whether the secret was known by others or publicly available, (3) whether reasonable efforts were taken to maintain the information's secrecy, and (4) the economic value of the secret information.<sup>290</sup> Unlike the state causes of action, however, the CFAA causes of action do not require that the information be secret.<sup>291</sup>

There are, however, certain measures businesses should take to enhance their CFAA claims. Although little or no case law exists on the subject, these measures may include: recording evidence of illegal entries and attempts into a proprietary network, reviewing computers, monitoring public entries into the public website, displaying terms of use on the website, changing passwords regularly, and having employees sign confidentiality agreements.<sup>292</sup> All of these protective measures are proactive steps an employer can take in not only preventing against trade secret theft, but also to increase the likelihood of proving the intent, unauthorized access, and damage or loss necessary in a CFAA claim.

Third, every state has different variations of laws protecting trade secrets, which lends itself to less uniformity in the law.<sup>293</sup> With the proliferation of the Internet, interstate communication, and global networks comes a need for uniformity necessary to enhance trade secret protection.<sup>294</sup> If courts adopt a single, broad interpretation of the CFAA, there will be more uniformity in litigating the misappropriation of electronic and computer-stored trade secrets.

In the absence of a federal trade secret law, the CFAA is a necessary tool for the litigation of trade secrets in federal court. The CFAA does not require a plaintiff to prove that a trade secret exists or that reasonable security measures have been taken. Further, because of the many variations in state trade secret causes of action, the CFAA enhances uniformity in the approach to trade secret litigation. Therefore,

---

<sup>287</sup> See MERGES, MENELL & LEMLEY, *supra* note 21, at 37; see also UNIF. TRADE SECRETS ACT §§ 1–12 (amended 1985), 14 U.L.A. 537–659 (2005). A trade secret must derive independent economic value from not being generally known, and not be readily ascertainable by proper means, and must be subject to reasonable measures to maintain its secrecy. *Id.* § 1(4), 14 U.L.A. at 538.

<sup>288</sup> See UNIF. TRADE SECRETS ACT §§ 1(4) (amended 1985), 14 U.L.A. at 538.

<sup>289</sup> Levinson & Paetsch, *supra* note 48, at 25.

<sup>290</sup> *Id.*

<sup>291</sup> See 18 U.S.C.A. § 1030(a)(2)(A), (a)(2)(C), (a)(4), (a)(5)(A)–(C) (West 2008).

<sup>292</sup> See Akerman & Finnegan, *supra* note 44, at A19 (listing measures employers can take in order to enhance their CFAA claims); Cundiff, *supra* note 19, at 712–19 (discussing in great detail measures employers can take to protect against employee theft of digital trade secrets).

<sup>293</sup> Christopher Rebel J. Pace, *The Case for a Federal Trade Secrets Act*, 8 HARV. J.L. & TECH. 427, 442 (1995) (“The best reason for enacting federal legislation to displace state law on trade secret misappropriation is the need for national uniformity in this area of the law.”).

<sup>294</sup> *Id.* at 448 (“A uniform system is also more appropriate for a nation constructing information superhighways, nationwide cellular networks, and portable technology systems, all of which simplify or accelerate the exchange of information.”).

a broader interpretation of the CFAA is advantageous in that it ensures that complex trade secrets lawsuits can be litigated in federal court.

#### CONCLUSION

The rise of the digital age has made trade secret theft easier than ever, necessitating the inclusion of trade secret misappropriation within the purview of the CFAA. The broad interpretation of the CFAA provides federal jurisdiction for complex trade secret litigation. The CFAA term “without authorization” should be understood in conjunction with agency law principles and also the fundamental meaning of a trade secret. Further, a trade secret is property, which is defined by its secrecy. Courts should consider this when determining “damage” under the CFAA, as a trade secret’s integrity is lessened with every disclosure. A broad interpretation of the CFAA can fill the gap in existing trade secret law by providing federal question jurisdiction for plaintiffs who have been victims of trade secret theft. This will ensure that litigators are able to utilize the procedural benefits of a federal venue when litigating complex trade secret suits.