Journal of Technology Law & Policy

Volume XIV – Spring 2014

ISSN 2164-800X (online)

DOI 10.5195/tlp.2014.139

http://tlp.law.pitt.edu

Break on Through: An Analysis of Computer Damage Cases

Ioana Vasiu and Lucian Vasiu, PhD, MBA

Break on Through: An Analysis of Computer Damage Cases

Ioana Vasiu[*] and Lucian Vasiu, PhD, MBA

INTRODUCTION

Computer crimes[1] represent an important percentage of all crimes[2] and have increased significantly over the last years in both sophistication and impact.[3] An important computer crime subclass is "computer damage."[4] According to a

[*] *Corresponding author*: Professor Ioana Vasiu, Faculty of Law, Babeş-Bolyai University; *E-mail*: ioanav3@yahoo.com. She was partner and lead researcher on several international projects, funded by the European Commission or other entities: the FP7 *Consent: Consumer Sentiment Regarding Privacy on User Generated Content Services in the Digital Economy* (2010–2013); *Rights of the Defense in Fraud Investigations* (2004–2005); *Grotius II (Criminal)*; and *Provision of Information by Courts and Court Administrations: A Comparative Inventory of Eight European Countries and the USA*. She worked as expert for the UNDP Romania, has spoken at numerous professional events and published widely on computer crimes. This article is part of a larger research project on computer crimes. We presented the research prototype at the 3rd INTERNET LAW WORKS-IN-PROGRESS CONFERENCE (Santa Clara Law School, 2013) and would like to thank Professor Eric Goldman and the other participants for their useful suggestions. We give special thanks to Ms. Chris Schlag, the Editors and the staff of the PITTSBURGH JOURNAL OF TECHNOLOGY LAW & POLICY for their very helpful comments and recommendations.

[1] "Computer crimes" involve criminal acts that have been committed using computers. Terms like "computer crime" and "cybercrime" are used interchangeably in various publications. Within this article, the two terms have the same meaning, as the offenses under examination involve computers used in interstate or foreign commerce or communication. *See* the discussion in Part I, section B, *infra*.

[2] *See* Office for Victims of Crime, *Statistical Overviews* (2013), *available at* http://ovc.ncjrs.gov/ncvrw2013/pdf/StatisticalOverviews.pdf (last visited Nov. 10, 2013); *The Economic Impact of Cybercrime and Cyber Espionage*, MCAFEE (July 6, 2013), http://www.mcafee.com/au/resources/reports/rp-economic-impact-cybercrime.pdf.

[3] *See* Verizon RISK Team, *2013 Data Breaches Investigations Report*, VERIZON (2013), http://www.verizonenterprise.com/DBIR/2013/ (last visited Oct. 23, 2013); *Security Threat Report*, SOPHOS (2013), http://www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf; ENISA, Flash Note, *Cyber-attacks—a new edge for old weapons* (2013), *available at* http://www.enisa.europa.eu/publications/flash-notes/cyber-attacks-2013-a-new-edge-for-old-weapons; ENISA, *Threat Landscape* (2012), *available at* http://www.enisa.europa.eu/media/press-releases/new-report-on-top-trends-in-the-first-cyber-threat-landscape-by-eu2019s-cyber-agency-enisa; Verizon RISK Team, *2012 Data breach investigations report*, VERIZON (2012), http://www.verizonenterprise.com/DBIR/2012/ (last visited Oct. 20, 2013).

[4] Numerous publications review the types or categories of computer crimes. *See, e.g.*, SUSAN W. BRENNER, CYBERCRIME AND THE LAW: CHALLENGES, ISSUES, AND OUTCOMES (2012); Marko Gercke, *Understanding Cybercrime: A Guide for Developing Countries* (2011), *available at* http://www.itu.int/

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

comprehensive study conducted by the United Nations Office on Drugs and Crime ("UNODC"),[5] organizations from the private sector consider computer damage to be a larger threat than any other type of computer crime.[6]

Computer damage attacks can target very important or prominent computer systems.[7] In extreme or widespread forms, these attacks are multi-target and multi-vector.[8] Such attacks can inflict direct and proximate harm on such a large scale that they reverberate over a significant amount of time and large geographical area.[9]

In certain circumstances, computer attacks can cause both electronic and physical damage. Physical damage or destruction can have a kinetic effect resulting in systemic harm. Such harm would be the result of successful attacks against computers controlling critical infrastructure or other important physical systems.[10]

ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pdf; Susan W. Brenner, *Is There Such a Thing as "Virtual Crime?,"* 4 CAL. CRIM. L. REV. 1 (2001).

[5] This study was conducted at the request of the General Assembly (Resolutions 65/230 and 67/189). Topics covered included cybercrime responses, by Member States, the international community and the private sector, prevention, criminal justice capabilities, international organizations, and technical assistance. *See* UNODC, *Comprehensive Study on Cybercrime* (Draft Feb. 2013), at IX and X, *available at* http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [hereinafter UNDOC].

[6] *Id.* at 27.

[7] *See* U.S. Attorney's Office, *Alleged Hacker Charged in Virginia with Breaching Multiple Government Agency Computers*, FBI (Oct. 28, 2013), http://www.fbi.gov/washingtondc/press-releases/2013/alleged-hacker-charged-in-virginia-with-breaching-multiple-government-agency-computers (discussing the attacks on systems owned by the U.S. Army, the U.S. Missile Defense Agency, the Environmental Protection Agency and the National Aeronautics and Space Administration). *See also Virtual Criminology Report 2009, Virtually Here: The Age of Cyber Warfare*, MCAFEE (2009), *available at* http://www.mcafee.com/us/resources/reports/rp-virtual-criminology-report-2009.pdf (discussing the attacks against the computer systems of the White House, the Department of Homeland Security, the U.S. Secret Service, the National Security Agency, the Federal Trade Commission, the Department of the Treasury, the Department of Defense and the Department of State).

[8] *See, e.g.*, *Defending Against the "Operation Ababil" Financial Services DDoS Attacks* (2013), *available at* http://www.arbornetworks.com/threats/ (last visited Feb. 21, 2014) (discussing Operation Ababil).

[9] *See* Nicole Perlroth & David E. Sanger, *Cyberattacks Seem Meant to Destroy, Not Just Disrupt* (Mar. 28, 2013, 12:00 AM), http://www.nytimes.com/2013/03/29/technology/corporate-cyberattackers-possibly-state-backed-now-seek-to-destroy-data.html?pagewanted=1&_r=0&partner=rss&emc=rss; Ronald J. Deibert, Rafal Rohozinski & Masashi Crete-Nishihata, *Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War*, 43 SECURITY DIALOGUE 3 (2012), *available at* http://sdi.sagepub.com/content/43/1/3.abstract; Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARV. INT'L L.J. 374 (2011); Marc Donner, *Cyberassault on Estonia*, 6 IEEE SECURITY & PRIVACY 4 (2007).

[10] *See* Alan Butler, *When Cyberweapons End up on Private Networks: Third Amendment Implications for Cybersecurity Policy*, 62 AM. U. L. REV. 1203 (2013); Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584 (2011); Maurizio Martellini, Stephanie Meulenbelt & Krzysztof Paturej, *Cyber Security for Chemical Plants*, *in* CYBER SECURITY 37 (Maurizio Martellini ed., 2013);

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

The scope of this article, however, is limited to cases involving electronic damage, brought to courts under the Computer Fraud and Abuse Act ("CFAA").[11] Successful claims under the CFAA allege improper acts that affect the integrity or availability of computer data or systems, or that are contrary to the intended use or operation of data or systems.

Integrity and availability are fundamental computer security attributes. Integrity generally refers to maintaining computer data in a protected state, unaltered by improper, unauthorized or subversive conduct or acts contrary to what the system owner or privilege grantor intended.[12] Integrity concerns computer data stored, processed, or in transit.[13] In the context of databases, integrity also regards metadata and the functions involved.

Availability refers to computer data and systems that are reliably and timely obtainable and usable or accessible for all legitimate users in accordance with their privileges.[14] Adverse actions in this context are acts that alter, encrypt, encipher, encode, transmit or delete data or exhaust system resources. These acts result in system malfunctions or temporarily or permanently delayed, hindered, disrupted, impeded, diminished or denied legitimate access to computer data or services. Protecting the integrity and availability of computer data and systems implies combating all adverse actions.

Effectively combating the computer damage phenomenon requires a holistic understanding of the aspects involved and associated interrelationships. In large part due to the evolution of the perpetration means,[15] there is a periodic need to

---

Ralph Langner, *Stuxnet: Dissecting a Cyberwarfare Weapon*, 9 IEEE SECURITY & PRIVACY 49 (2011); Susan W. Brenner, *"At Light Speed"—Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 J. CRIM. L. & CRIMINOLOGY 379 (2007). *See also* Eric Chabrow, *Anonymous Set to Do Real Damage*, GOV INFO SECURITY, *available at* http://www.govinfosecurity.com/blogs/anonymous-set-to-do-real-damage-p-1203 (last visited Feb. 20, 2014).

[11] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012) [hereinafter CFAA].

[12] This term has been defined in several ways. *See, e.g.*, Ravi S. Sandhu, *On Five Definitions of Data Integrity*, Proc. of the IFIP WG11.3 Workshop on Database Security (1993), *available at* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.29.5877&rep=rep1&type=pdf. *See also* 44 U.S.C. § 3542(b)(A) (defining integrity).

[13] *Id.*

[14] *See* 44 U.S.C. § 3542(b)(C); CJIS Advisory Policy, *Criminal Justice Information Services (CJIS) Security Policy* (Version 5.2, 8/9/2013), *available at* http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/at_download/file; Algirdas Avižienis et al., *Basic Concepts and Taxonomy of Dependable and Secure Computing*, 1 IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING 11 (2004).

[15] While the perpetration of these offenses does not always require highly developed skills, tools or techniques, sophisticated attacks are committed using advanced techniques or software tools. Some of these tools are available on the Internet free of charge, while others available on the black market. *See*

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

review the nature of these offenses and the effectiveness of the legal framework. While there is a significant body of academic research that explores issues pertaining to computer damage,[16] existing studies do not present comprehensive examinations, involving a large number of real cases, in order to reveal and discuss the essential characteristics of these offenses.

This article is based on a extensive inquiry, involving the study of over three hundred computer damage cases. This near exhaustive approach permitted an empirical categorization of the essential aspects. Based on the cases' merits, this article reports and analyzes the most relevant issues, interpretations, and arguments available under each category. These categories include fundamental facets, such as legal elements; motive and intent; results; profile of perpetrators; and means of perpetration, including, if applicable, the software involved.

This article makes two important contributions: a comprehensive analysis and a conceptual approach for this area. Part I concerns theoretical aspects and discusses the legal elements of computer damage offenses under the CFAA. Part II considers the practical aspects and discusses the essential features involved in the perpetration of these offenses and the profile of attackers. Finally, Part III provides a summary of findings and the implications of this study for stakeholders.

Thomas J. Holt, *Examining the Forces Shaping Cybercrime Markets Online*, 31 SOC. SCI. COMPUTER REV. 165 (2013); Indictment, United States v. Ancheta, No. 05-1060 (C.D. Cal. 2005), *available at* http://www.justice.gov/usao/cac/Pressroom/pr2005/Botnet_Indictment.pdf; Luca Allodi, Woohyun Shim & Fabio Massacci, *Quantitative Assessment of Risk Reduction with Cybercrime Black Market Monitoring* (2013), *available at* http://disi.unitn.it/~allodi/allodi-13-iwcc.pdf.

[16] *See* Lauren Eisenberg, Tiffany Ho & Rob Boyd, *Computer Crimes*, 50 AM. CRIM. L. REV. 681 (2013); David Gray, Danielle Keats Citron & Liz Clark Rinehart, *Fighting Cybercrime After* United States v. Jones, 103 J. CRIM. L. & CRIMINOLOGY 745 (2013); David Thaw, *Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement*, 103 J. CRIM. L. & CRIMINOLOGY 907 (2013); Alden Anderson, Comment, *The Computer Fraud and Abuse Act: Hacking into the Authorization Debate*, 53 JURIMETRICS J. 447 (2013); Natch Greyes, *A New Proposal for the Department of Justice's Interpretation of the Computer Fraud & Abuse Act*, 17 VA. J.L. & TECH. 293 (2013); Lee Goldman, *Interpreting the Computer Fraud and Abuse Act*, 13 PGH. J. TECH. L. & POL'Y 1 (2012); Shawn E. Tuma, *"What Does CFAA Mean and Why Should I Care?"—A Primer on the Computer Fraud and Abuse Act for Civil Litigators*, 63 S.C. L. REV. 141 (2011); Obie Okuh, Comment, *When Circuit Breakers Trip: Resetting the CFAA to Combat Rogue Employee Access*, 21 ALB. L.J. SCI. & TECH. 637 (2011); Cyrus Y. Chung, Note, *The Computer Fraud and Abuse Act: How Computer Science Can Help With the Problem of Overbreadth*, 24 HARV. J.L. & TECH. 233 (2010); Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561 (2010); Sarah Boyer, *Computer Fraud and Abuse Act: Abusing Federal Jurisdiction?*, 6 RUTGERS J.L. & PUB. POL'Y 661 (2009); Matthew Andris, Comment, *The Computer Fraud and Abuse Act: Reassessing the Damage Requirement*, 27 J. MARSHALL J. COMPUTER & INFO. L. 279 (2009); Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164 (2004); Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 MD. L. REV. 320 (2004).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

I. LEGAL ELEMENTS

Computer attacks can cause damage or interference that cannot be addressed satisfactorily by traditional laws. This includes attacks that cause malfunctions or temporarily interrupt or deny access to certain services. Consequently, there is a clear need for specific legal provisions to enhance the ability to prosecute such offenses.

As underlined in the UNODC study, the criminalization of computer damage across the globe reveals divergent approaches, with respect to both the object of the offense and the proscribed conduct.[17] For instance, there are varying arguments as to what constitutes unauthorized access to computer systems; and only a small percentage of jurisdictions include harm or loss as a necessary element of a data interference offense.[18]

The Convention on Cybercrime, an important multilateral instrument used in the development of computer crime legislation, contains the criminalization of computer damage in two separate provisions.[19] The first provision defines "data interference" as the "damaging, deletion, deterioration, alteration or suppression of computer data without right."[20] The second provision defines "system interference" as "serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data."[21]

The CFAA contains the United States' federal computer damage legal provisions. The CFAA intends to provide an adequate "balance between the Federal Government's interest in computer crime and the interests and abilities of the States to proscribe and punish such offenses."[22] The CFAA was enacted in

[17] *See* UNODC, *supra* note 5, at 81. *See also* Lorenzo Picotti & Ivan Salvadori, *National Legislation Implementing the Convention on Cybercrime—Comparative Analysis and Good Practices* (Version 28 August 2008), at 20–24, *available at* http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20study2-d-version8%20_28%20august%2008.pdf (last visited Feb. 20, 2014).

[18] *Id.* at 90.

[19] The Convention on Cybercrime was signed by the U.S. on November 23, 2001, ratified on September 29, 2006, and has been in force since 2007. *See Convention on Cybercrime*, COUNCIL OF EUROPE (Jan. 18, 2014), http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

[20] *Id.* at art. 4(1).

[21] *Id.* at art. 5.

[22] S. REP. NO. 99-432, at 4 (1986).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

1986 and has been amended several times since.[23] The CFAA criminalizes the following conduct: (1) unauthorized obtaining of national security information; (2) unauthorized obtaining of information from a financial institution, United States department or agency, or from any protected computer; (3) unauthorized access to government computers; (4) computer fraud; (5) computer damage; (6) passwords trafficking; and (7) computer extortion.[24]

According to CFAA § 1030(a)(5), computer damage can take three specific forms: (A) 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; (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.[25]

Based on the CFAA provisions, and as explained by the court in *United States v. Stratman*, insiders or those individuals who are authorized to access a computer system will face criminal liability only when damage was caused intentionally, whereas intruders or those individuals not authorized to access a computer system will face criminal charges for causing intentional, reckless, or accidental damage.[26] Apart from criminal sanctions, perpetrators that inflict damage or loss can also incur civil liability if the misconduct inflicted any of the § 1030(c)(4)(A)(i) subclauses: (1) loss to one or more persons aggregating to at least $5,000 loss during any one-year period; (2) modification or impairment, or potential modification or impairment, of medical documents; (3) physical injury to any person; (4) a threat to public health or safety; (5) damage to a computer used by or for an entity of the U.S. Government in furtherance of justice administration or national security or defense; (6) damage affecting 10 or more protected computers during any one-year period.[27]

---

[23] *See* Pamela Taylor, Comment, *To Steal or Not to Steal: An Analysis of the Computer Fraud and Abuse Act and Its Effect on Employers*, 49 HOUS. L. REV. 201, 207 (2012); David J. Rosen, Note, *Limiting Employee Liability Under the CFAA: A Code-Based Approach to "Exceeds Authorized Access,"* 27 BERKELEY TECH. L.J. 737, 738 (2012).

[24] 18 U.S.C. § 1030(a) (2012).

[25] *Id.* at (a)(5).

[26] United States v. Stratman, No. 4:13-CR-3075, 2013 WL 5676874, at *2 (D. Neb. Oct. 18, 2013).

[27] 18 U.S.C. § 1030(g) (2012). Damage claims brought under 18 U.S.C. § 1030(g) (2012) are limited to economic damages.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

The CFAA also applies to misconduct affecting protected computers situated outside the United States.[28] Under certain circumstances, computer damage cases can be classified as federal crimes of terrorism.[29] If two or more persons conspire to intentionally cause computer damage against the United States, in violation of 18 U.S.C. § 1030(a)(5), each perpetrator can be held guilty of conspiracy, in violation of 18 U.S.C. § 371.[30]

A. Protected Computer

CFAA § 1030(A)(5) regarding computer damage only applies to protected computers.[31] According to § 1030(e)(2), a "protected computer" means a computer used exclusively by a financial institution or by the United States' Government, used by or for such an entity that is affected by the offensive conduct, or used in or affecting interstate or foreign commerce or communication, including situations where it is located outside the United States.[32] Courts generally hold that because the Internet and interstate commerce are inexorably intertwined, any computer connected to the Internet should be considered a computer affecting interstate commerce and therefore protected.[33]

In *United States v. Trotter*, the court rejected the defendant's contention that if computers used by non-profit organizations were considered protected, the CFAA

---

[28] *See* Energy Power Co. Ltd. v. Wang, No. 13-11348-DJC, 2013 WL 6234625, at *6-7 (D. Mass. Dec. 3, 2013); Four Seasons Hotels & Resorts BV v. Consorcio Barr, SA, 267 F. Supp. 2d 1268, 1322 (S.D. Fla. 2003).

[29] *See* Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817 (2012); CHARLES DOYLE, CONG. RESEARCH SERV., 97-1025, CYBERCRIME: AN OVERVIEW OF THE FEDERAL COMPUTER FRAUD AND ABUSE STATUTE AND RELATED FEDERAL CRIMINAL LAWS 38 (2010).

[30] *See* Indictment, United States v. Collins, No. l:13-cr-383 (E.D. Va. 2013), *available at* http://msnbcmedia.msn.com/i/MSNBC/Sections/NEWS/A_U.S.%20news/US-news-PDFs/anonymous-indictment.pdf; Pleading, United States v. Keys, No. 2:13-CR-082 KJM, 2013 WL 987573 (E.D. Cal. 2013); Indictment, United States v. Ancheta, No. 05-1060 (C.D. Cal. 2005), *available at* http://www.justice.gov/usao/cac/Pressroom/pr2005/Botnet_Indictment.pdf.

[31] According to 18 U.S.C. § 1030(e)(1) (2012), "computer" is defined as an:

> [E]lectronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.

[32] *Id.* at (e)(2)(A)–(B).

[33] *See, e.g.*, United States v. Roque, No. 12-540 (KM) (D.N.Y. June 6, 2013); Freedom Banc Mortgage Services, Inc. v. O'Harra, No. 2:11-cv-01073 (S.D. Ohio Sept. 5, 2012); Quantlab Technologies Ltd. (BVI) v. Godlevsky, 719 F. Supp. 2d 766 (S.D. Tex. 2010).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

would be too broad and unconstitutional.[34] In *Mobile Mark, Inc. v. Pakosz*, the court emphasized that the plaintiff need not prove that the computer files in discussion, deleted by the defendant, were used in interstate commerce, but only that the computer on which those files were stored was used in interstate commerce.[35] Laptop computers, even when used as virtual terminals to connect to desktop computers, are also considered protected, unless evidence is presented to disqualify the desktops as protected computers.[36]

B. Transmission

Subsection 1030(a)(5)(A) imposes liability on whoever "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[.]"[37] "Transmission" does not distinguish between remote and direct modes, and encompasses numerous subcategories or techniques.[38] The most basic form of transmission in this context is the pressing of the *Delete* key. Nevertheless, before a transmission will fall within this subsection, plaintiffs must demonstrate possessory interest in the deleted data and dual intent consisting of (1) knowing transmission and (2) damage. The intent to cause damage is not easy to prove, especially when defendants claim their intentions were to delete only their personal data or data presumed to have been backed up by the employer.[39]

If the deleted computer data or files can be recovered (i.e., made available again to the victim), the claim can be rejected. In *Dana Limited v. American Axle and Manufacturing Holdings, Inc.*, for instance, the plaintiff alleged unauthorized deletion of computer files by the defendants, who at that time were employed by the plaintiff.[40] The court determined that the plaintiff had not presented evidence that the files in discussion were original files or that the files contained information

---

[34] United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007).

[35] Mobile Mark, Inc. v. Pakosz, No. 11 C 2983, 2011 WL 3898032, at *2 (N.D. Ill. 2011).

[36] *See* Keen v. Bovie Medical Corp., No. 8:12-cv-305-T-24-EAJ, 2013 WL 1899791, at *13 (M.D. Fla. May 7, 2013).

[37] 18 U.S.C. § 1030(a)(5)(A) (2012).

[38] *See* Lloyd v. United States, No. Civ. 03-813 (WHW), 2005 WL 2009890, at *7 (D.N.J. Aug. 16, 2005).

[39] *See* Devon Energy Corp. v. Westacott, No. H-09-1689, 2011 WL 1157334, at *11 (S.D. Tex. Mar. 24, 2011).

[40] Dana Limited v. American Axle and Manufacturing Holdings, Inc., No. 1:10-CV-450, 2012 WL 2524008, at *5 (W.D. Mich. June 29, 2012).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

not otherwise available.[41] Regarding the latter, the court noted that the plaintiff did not request its computer expert to attempt to recover the deleted files.[42]

In *International Airport Centers, LLC v. Citrin*, the defendant used a special program to delete all data on a laptop belonging to his employer.[43] The specialized erasure program that the defendant used prevented any possible subsequent recovery of the deleted data, of which the company had no copies.[44] Regardless of whether the software used was downloaded from the Internet as a remote attack, or copied from a portable data storage device as an inside attack, it represents conduct actionable under the CFAA.[45]

In *United States v. Stratman*, the defendant alleged that since he was authorized to access the computer, he could not have perpetrated the alleged offense as a matter of law.[46] The court, however, construed § 1030(a)(5)(A)'s language to hold that "without authorization" modifies the phrase "intentionally causes damage," not the access to the protected computer.[47] The court reasoned that, although the defendant was authorized to access the computer, the intentional damage was done without authorization.[48]

A similar reasoning can be found in *B&B Microscopes v. Armogida*.[49] In that case, the plaintiff, a company engaged in the imaging software business, hired the defendant to sell and provide custom image solutions to the plaintiff's customers.[50] The defendant deleted and overwrote important files pertaining to the plaintiff's business for the purpose of depriving the plaintiff of important information, which

---

[41] *Id.*

[42] *Id.*

[43] Int'l Airport Centers, LLC v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006).

[44] *Id.*

[45] *Id.* at 420.

[46] United States v. Stratman, No. 4:13-CR-3075, 2013 U.S. Dist. LEXIS 150224, at *2 (D. Neb. Aug. 5, 2013).

[47] *Id.* at *4-5. *See also* 18 U.S.C. § 1030(a)(5)(A) (2012) (stating that to intentionally cause damage means to "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").

[48] United States v. Stratman, No. 4:13-CR-3075, 2013 WL 5676874, at *6 (D. Neb. Oct. 18, 2013).

[49] B & B Microscopes v. Armogida, 532 F. Supp. 2d 744 (W.D. Pa. 2007).

[50] *Id.* at 746.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

could not be retrieved.[51] The court held that despite being authorized to access the computer in question, the defendant's knowing and intentional deletion of computer files constituted a violation of § 1030(a)(5)(A)(i), which is predicated upon unauthorized damage to a protected computer.[52] Cases like *Citrin*, *Stratman* and *Armogida* clearly indicate that even though deletion of computer data or files can and should be done, in order to free disk space and optimize the performance, not any deletion by legitimate users is authorized.

The transfer of operational or confidential information may also be successfully claimed under § 1030(a)(5)(A)(i). In *Black & Decker (US), Inc. v. Smith*, for instance, the defendant, a project engineer, had access to plaintiff's computer systems, including e-mail and Internet access.[53] The Defendant's Employee Access Agreement stipulated that the defendant "will maintain the confidentiality of all information of a confidential, proprietary or other legally sensitive nature" and "will not send, share, or publish any such information on the Internet without prior approval."[54] The defendant, however, shared confidential information with one competitor of his employer.[55] The court reasoned that even though the defendant had permission to access the information in question, the transfer to a non-secure drive, as means to share it with the competitor, supported the CFAA damage claim, because the intentional rendering of a computer less secure should be considered damage.[56]

Proscribed transmission also includes malicious software updates. In one putative class action, *In re Apple & AT & TM Antitrust Litigation*, plaintiffs alleged damage to their iPhones, inflicted via a software update.[57] The iPhones were offered to consumers upon signing a two-year service agreement with AT&T Mobility (AT&T).[58] Consumers were not aware that Apple, Inc. ("Apple") and AT&T had agreed to technologically restrict voice and data service after the initial

[51] *Id.* at 753.

[52] *Id.* at 758.

[53] Black & Decker (US), Inc. v. Smith, 568 F. Supp. 2d 929 (W.D. Tenn. 2008).

[54] *Id.*

[55] *Id.*

[56] *Id.*

[57] *In re* Apple & AT & TM Antitrust Litigation, 596 F. Supp. 2d 1288, 1296 (N.D. Cal. 2008). For a discussion of how modern cellular phones qualify as computers under the CFAA, see J.C. Lundberg, *When is a Phone a Computer?*, 8 WASH. J.L. TECH. & ARTS 473 (2013).

[58] *In re* Apple, 596 F. Supp. 2d at 1303.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

two-year service period expired.[59] This exclusivity was enforced through SIM card program locks.[60] Some consumers unlocked their iPhones, which allowed for them to install unapproved third-party applications and use the SIM cards of other wireless providers that had not been agreed to by the defendants.[61] In response to consumers unlocking the phones, Apple issued an update for the iPhone operating software, ostensibly intended to improve it.[62] The update, however, was issued as a form of retaliation against consumers who had unlocked their iPhones.[63] Apple knew prior to the release of the update that the update would render completely inoperable ("brick") or otherwise damage unlocked iPhones.[64]

The court determined that the plaintiffs' contention that they had authorized a software update, not damage to their iPhones, sufficiently stated a claim under § 1030(a)(5)(A)(i).[65] Furthermore, the court rejected Apple's contention that plaintiffs should not be permitted to aggregate damage to their individual iPhones to meet the CFAA's $5,000 minimum in damages requirement.[66] The CFAA permits aggregation of damages as long as the "damages arose from the same act by the defendant."[67] In effect, *In re Apple & AT & TM* exemplifies the conflicting interest between manufacturers' attempt to create or maintain revenue streams and consumers' desire to maximize the use or utility of their products. *In re Apple & AT & TM* further illustrates that contracts, exclusivity or dominant market power cannot be enforced by means of nefarious software that damages computers.[68]

The software update issue allows for an interesting contrast between the above case and a putative class action against Sony, which involved the release of an update for the PlayStation 3 ("PS3") gaming system.[69] Though allegedly

---

[59] *Id.* at 1296.

[60] *Id.* at 1295.

[61] *Id.*

[62] *Id.* at 1296.

[63] *In re* Apple, 596 F. Supp. 2d at 1296.

[64] *Id.*

[65] *Id.* at 1308.

[66] *Id.*

[67] *Id.*

[68] *See* Matt McMurrer, *Exclusive Gadget: Apple & AT&T Antitrust Litigation and the iPhone Aftermarkets*, 36 J. CORP. L. 495 (2011) (providing an extended discussion on this case); *see also* Jeffrey Paul Jarosch, *Reassessing Tying Arrangements at the End of AT&T'S iPhone Exclusivity*, 2 COLUM. BUS. L. REV. 296 (2011).

[69] *In re* Sony PS3 Other OS Litigation, 828 F. Supp. 2d 1125, 1125 (N.D. Cal. 2011).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

intended to enhance security and protect intellectual property, the update also intentionally disabled a PS3 feature.[70] Nonetheless, the installation of the update was at the users' discretion, and occurred *only* with the consent of the PS3 owners.[71] The court concluded that because Sony provided PS3 owners with a choice, whereby the PS3 feature was removed only upon users affirmatively electing to install the update, the plaintiffs had not stated a CFAA claim.[72]

A related transmission issue is represented by the download, delivery, insertion, or embedding of malicious code (also known as *malware*)[73] into protected computers.[74] For instance, in one class action, the plaintiff alleged intentional transmission of software code that acted like a "time bomb."[75] That transmission disabled or rendered all versions of the software inoperable after a preset date, unless an upgrade was installed.[76] Although the defendant argued that the malfunction was caused by a software defect (referred to as a "glitch"), the court partially granted the motion for class certification with regards to the CFAA claim.[77]

Code injection attacks, such as Structured Query Language ("SQL") strings or series of instructions,[78] also fall within subsection 1030(a)(5)(A)(i). These attacks are usually carried out to enable the perpetration of other offenses.[79] Another important transmission subcategory is represented by the Distributed Denial of

---

[70] *Id.* at 1128.

[71] *Id.* at 1129–30.

[72] *Id.* at 1132.

[73] For definitions, attributes and classes of malicious software, see MCAFEE, *Small Business Security Glossary*, *available at* http://www.mcafee.com/us/small-business-security/glossary.html; CISCO, *What Is the Difference: Viruses, Worms, Trojans, and Bots?*, http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html (last visited Oct. 23, 2013); BITS, *Malware Risks and Mitigation Report* (June 2011), *available at* http://www.nist.gov/itl/upload/BITS-Malware-Report-Jun2011.pdf.

[74] *See* PQ Labs, Inc. v. Qi, No. 12-0450 CW (N.D. Cal. Jan. 29, 2014); United States v. McGraw, No. 3:09-CR-0210-B, 2012 WL 6013258, at *1 (N.D. Tex. Nov. 30, 2012); United States v. Makwana, 445 F. App'x 671 (4th Cir. 2011) (per curiam).

[75] *See* Kalow & Springut, LLP v. Commence Corp., 272 F.R.D. 397, 405 (D.N.J. 2011).

[76] *Id.* at 400.

[77] *Id.*

[78] SQL is a programming language, used to manage data in relational database management systems. SQL vulnerabilities allow a perpetrator to exploit web software and introduce malicious code into victim's computer system.

[79] *See* United States v. Gonzalez, 08 CR 10223 PBS, 2009 WL 1543798 (D. Mass. May 26, 2009); *see also* Indictment, United States v. Albert Gonzalez, 09-cr-00626-JBS (D.N.J. 2009), *available at* http://datalossdb.org/attachments/0000/0514/gonzales_nj.pdf.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

Service ("DDoS") attacks.[80] DDoS attacks aim to render the attacked websites unavailable, or at least diminish their performance, and are often carried out via "zombie" computers or botnets.[81] Some DDoS attacks are carried out as a form of hacktivism.[82]

"Transmission" may also regard unsolicited text messages sent to cell phones or bulk e-mails ("UBE," also referred to as *spam*). In *Czech v. Wall Street on Demand, Inc.*,[83] for instance, the plaintiff alleged damage caused by the transmission of unwanted text messages to her cell phone.[84] Even though certain fees were incurred on receipt of messages, and the memory of the cell phone was depleted, the court found the plaintiff failed to state a transmission claim under the CFAA.[85]

Conversely, UBE, if sent in large quantities, can have a result very similar to DDoS attacks. UBE can overload systems' storage and processing capacity and

---

[80] *See generally* Bryan Harris, Eli Konikoff & Phillip Petersen, *Breaking the DDoS Attack Chain*, INST. FOR SOFTWARE RESEARCH CARNEGIE MELLON UNIV. (Aug. 2013), http://www.cmu.edu/mits/files/breaking-the-ddos-attack-chain.pdf (A history of real DDoS attacks). *See also Ten Days of Rain*, MCAFEE (2011), http://blogs.mcafee.com/wp-content/uploads/2011/07/McAfee-Labs-10-Days-of-Rain-July-2011.pdf (last visited Dec. 1, 2013) (DDoS attacks use a high number of computers to simultaneously request data, effectively bombarding the targeted system with digital projectiles. Done on a large scale, these requests overwhelm or flood the victim, exhausting its resources, thereby rendering it inaccessible or unable to properly handle legitimate requests or network traffic. Examples of such attacks are *SynFlood* [which involves a large number of SYN data packets sent to a computer system], *HTTPFlood* [which involves a large number of HTTP requests sent to a computer system], *UDP Flood* [which involves an interrupted stream of UDP data packets], *smurf* [which exploits the Internet Protocol broadcast addressing] or *ping flood*.).

[81] *Microsoft, the FBI, Europol and industry partners disrupt the notorious ZeroAccess botnet*, MICROSOFT (Dec. 5, 2013), http://www.microsoft.com/en-us/news/press/2013/dec13/12-05zeroaccessbotnetpr.aspx (Sets of geographically dispersed and infected computers are controlled remotely by the perpetrators via a master computer, known as the "command and control" server. They are used to attack other computer systems. For instance, the Sirefef botnet (also referred to as ZeroAccess) contained about 2 million infected computers, with more than 800,000 of them active on any given day).

[82] For discussions on hacktivism, *see* Molly Sauter, *Distributed Denial of Service Actions and the Challenge of Civil Disobedience on the Internet* (2013) (unpublished M.Sc. thesis, Massachusetts Institute of Technology), *available at* http://cmsw.mit.edu/distributed-denial-of-service-actions/ (last visited Feb. 21, 2014); Brian B. Kelly, *Investing in a Centralized Cybersecurity Infrastructure: Why "Hacktivism" Can and Should Influence Cybersecurity Reform*, 92 B.U. L. REV. 1663 (2012). *See* cases in Part II, section B, *infra*.

[83] Czech v. Wall Street on Demand, Inc., 674 F. Supp. 2d 1102, 1107 (D. Minn. 2009).

[84] *Id.* at 1123 (The court noted that "[t]here is no dispute that Czech's cell phone (as well as the various similar wireless devices used by the proposed class members) would constitute such a 'computer' as further defined in 18 U.S.C. § 1030(e)(1)").

[85] *Id.* at 1121.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

result in delays or otherwise adversely affect the victims.[86] For example, in *America Online v. National Health Care Discount*, the court found that defendant's contract e-mailers sent 135 million pieces of UBE to AOL members.[87] Even though the e-mailers' intent was to generate leads, the court held that the defendant had violated the CFAA because the quantity of UBE sent caused substantial loss, expressed as degradation of systems' performance and disruption of services.[88]

Pulte Homes, Inc. v. Laborers' International Union of North America, on the other hand, presents a case where the defendant's unmistakable intent was to cause damage.[89] Following the firing of one of its members by the plaintiff, the defendant attacked the plaintiff with massive auto-dialing phone calls and e-mails.[90] The court held that because the volume of intentional communications prevented the plaintiff from receiving calls and accessing or sending e-mails, the plaintiff had alleged a valid CFAA transmission claim.[91]

The malicious modification of hardware design (also referred to as hardware Trojans) viewed by computer security experts as a major security threat[92] would fall within this subsection, as well. The research conducted for this study found no such cases in federal courts. However, it revealed analogous cases involving defective microcode brought to courts before the USA PATRIOT Act amended the CFAA: according to § 1030(g), actions may no longer be brought over the negligent design or manufacture computer hardware, software or firmware.[93]

In the class action *Shaw v. Toshiba America Information Systems, Inc.*, plaintiffs claimed that faulty floppy-diskette controllers ("FDC"), produced by defendants, resulted "in the storage of corrupt data or the destruction of data

---

[86] *See* Complaint For Damages and Injunctive Relief at ¶¶ 11–15, Microsoft Corp. v. Rockin Time Holdings, Inc., No. 03-2-27977-3SEA (Wash. Super. Ct. June 12, 2003), 2003 WL 25284515 at *11-15; *see also Sanford Wallace Indicted for Spamming Facebook Users*, FED. BUREAU OF INVESTIGATION (Aug. 4, 2011), http://www.fbi.gov/sanfrancisco/press-releases/2011/sanford-wallace-indicted-for-spamming-facebook-users.

[87] *See* America Online v. National Health Care Discount, 174 F. Supp. 2d 890, 897 (N.D. Iowa 2001).

[88] *Id.* at 899.

[89] Pulte Homes, Inc. v. Laborers' International Union of North America, 648 F.3d 295, 303 (6th Cir. 2011).

[90] *Id.* at 299.

[91] *Id.* at 303.

[92] *See* Seetharam Narasimhan et al., *Hardware Trojan Detection by Multiple-Parameter Side-Channel Analysis*, 62 IEEE TRANSACTIONS ON COMPUTERS 2183 (2013); Ramesh Karri et al., *Trustworthy Hardware: Identifying and Classifying Hardware Trojans*, 43 IEEE COMPUTER 39 (2010).

[93] USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 384 (2001).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

without the user's knowledge."[94] Defendants argued there was no transmission involved, since the command or code originated and ended within a computer, and that the CFAA was intended to criminalize hacking, not to reach manufacturers.[95] The court held however, that there is no transmission exemption for manufacturers and that the word "hacking" does not appear in the CFAA.[96] Consequently, the court embraced a broad view of transmission, one that includes electronic inter- and intra-computer transmissions, as well as the marketplace transfer of the code.[97] The case settled for approximately $2.1 billion.[98]

An interesting comparison is available in *Thurmond v. Compaq Computer Corp.*, a similar class action, regarding infected microcode.[99] In the *Compaq* case, plaintiffs alleged that Compaq "designed, sold, manufactured, transmitted or created" computers that contained infected FDC.[100] The court, however, emphasized that because there was no class certification, thereby refusing loss aggregation, claims should be treated as though brought by individual plaintiffs.[101] The court underlined that because the CFAA section refers to "*a* protected computer" (that is, not to more or all protected computers), the loss threshold was not met, even when considering the full price paid for the computers in cause or the cost involved in repairing the individual computers.[102]

In conclusion, access to a protected computer is not necessarily an element of these offenses, as perpetrators can inflict damage by transmission, without actually gaining access to computer systems.[103] This point of view is also supported by the UNOCD study, which argues that the installation of malicious software on a computer system can amount to illegal data or system interference.[104] The CFAA, however, also comprehends forms of computer damage associated with the intentional unauthorized access to a protected computer.

---

[94] Shaw v. Toshiba America Info. Sys., Inc., 91 F. Supp. 2d 926, 928 (E.D. Tex. 1999).

[95] *Id.* at 936.

[96] *Id.*

[97] *Id.* at 941.

[98] *See id.* at 946.

[99] Thurmond v. Compaq Computer Corp., 171 F. Supp. 2d 667, 667 (E.D. Tex. 2001).

[100] *Id.* at 669.

[101] *Id.* at 680.

[102] *Id.* at 681.

[103] United States v. Stratman, No. 4:13-CR-3075, 2013 WL 5676874, at *2 (D. Neb. Oct. 18, 2013).

[104] UNODC, *supra* note 5, at 32.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

C. Access Without Authorization under Subsections 1030(a)(5)(B)–(C)

Subsections 1030(a)(5)(B) and (C) concern intentional access to a protected computer without authorization.[105] Professor Orin Kerr of the George Washington University Law School defines "access" as "any successful interaction with the computer."[106] This definition does not work for all situations, as certain actions can be regarded as successful interactions, but not regarded as "access" to a computer system (for instance, the synchronization with an Internet time server or the use of the *ping* command, to check if computers can communicate via a network or the Internet). A more elaborated definition found in a National Institute of Standards and Technology ("NIST") publication defines "access" as the "ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions."[107] This article proposes to understand "access" as the *ability to successfully read, execute, or write computer files*.[108] A fundamental attribute of access is the *scope*.

Authorized users may have certain restrictions to computer objects (i.e. data or files) or services. Authorization sets the type of access and regards the granting of permission or access privileges to a specific user to execute or carry out a predetermined action or command, or set of actions or commands, on certain computers. The limitation of the authorization can be explained by an analogy from the physical world: if one is permitted to enter the wine tasting room, that does not imply permission to enter the cellar, let alone alter or remove wine bottles. Authorization is enforced through authentication methods.[109]

According to computer crime specialist Charles Doyle, subsections 1030(a)(5)(B) and (C) of the CFAA should be construed to mean that only outsiders can violate the reckless and simple damage clauses.[110] However, insiders can also fall within the proscribed conduct, specifically in situations in which they circumvent access control or security measures. An example would include

---

[105] 18 U.S.C. § 1030(a)(5)(B)–(C).

[106] Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1647 (2003).

[107] *Glossary of Key Information Security Terms*, NIST (2011), *available at* http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf (last visited Jan. 14, 2013).

[108] "Write," in the computing context, includes the ability to delete computer files.

[109] The means used to confirm the identity of a user. Authentication can be based on what the user knows (*e.g.*, the password), what the user has (*e.g.*, a card or a key), or on user's physical characteristics (such as facial image or fingerprints).

[110] DOYLE, *supra* note 29, at 30.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

obtaining access outside or beyond the scope of their authorization or for a purpose that is impermissible or unapproved.[111] One court gave the following hypothetical example of employee's access outside the scope of authorization: if an employee was authorized to login to server X, but not to server Y, accessing the latter would be outside the scope of authorization.[112]

The lack of a definition as to what constitutes "access without authorization" in the CFAA was grounds for a defendant to contend that the CFAA allows for conflicting interpretations, thereby rendering it unconstitutionally vague.[113] Relying on the common meaning of "authorization," the court disagreed and held that someone accesses a computer without authorization when doing so *without sanction or permission*.[114] Accordingly, defendants are "without authorization" if they act without having received permission or if they do so after their permission was affirmatively repealed, rescinded, or annulled. When a person that lacks such authority grants the permission, access is also construed as "without authorization," and the subjective belief of the accessor is deemed irrelevant.[115] In *Power Equipment Maintenance, Inc. v. Airco Power Services, Inc.*, it was alleged that the defendant accessed files via an administrative assistant, who printed a confidential contract on his behalf, after his access privileges were revoked.[116] The court, however, held that the claim fails under the CFAA, as the allegation does not include computer access.[117]

Analysis of the "access without authorization" element reveals a major split of authority. Three different interpretations have emerged over time. Based on the cessation of agency theory, in *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, the court embraced a broad interpretation of authorization and reasoned that, based on the *Restatement (Second) of Agency* §§ 112, 387 (1958), employees' authorization terminates when they violate the fiduciary duty of loyalty

---

[111] *See* H. Marshall Jarrett et al., *Prosecuting Computer Crimes* (2010), *available at* http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf. *See also* Part II, *infra*.

[112] *See* Advanced Micro Devices, Inc. v. Feldstein, No. 13-40007-TSH, 2013 WL 2666746, at *3 (D. Mass. June 10, 2013).

[113] *See* United States v. Auernheimer, No. 11-cr-470 (SDW), 2012 WL 5389142 (D.N.J. Oct. 26, 2012).

[114] *Id.*

[115] *See* Clinton Plumbing and Heating of Trenton, Inc. v. Ciaccio, No. 09-2751, 2010 WL 4224473 (E.D. Pa. Oct. 22, 2010).

[116] Power Equip. Maint., Inc. v. Airco Power Servs., Inc., No. CV413-55, 2013 WL 3422779 (S.D. Ga. June 28, 2013).

[117] *Id.*

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

to their employer.[118] A similar approach can be found in other cases. For example, authorization ceased in *International Airport Centers, L.L.C. v. Citrin* when the defendants destroyed the agency relationship by acting for personal gain and against the employer's interests.[119] Similarly, in *Ervin & Smith Advertising and Public Relations, Inc. v. Ervin*, where the defendants e-mailed trade secrets to their home computers with the intent to use the information for their own personal gain.[120] The *Ervin* court held that it would be "nonsensical to conclude that Congress did not intend to create a remedy for circumstances such as those the plaintiff has pled in this matter."[121]

The agency approach has been explicitly rejected in numerous cases. For example in *United States Bioservices Corp. v. Lugo*, the court held that there was no basis to graft a portion of the Restatement or other agency law onto the CFAA.[122] Similarly, in *LVRC Holdings LCC v. Brekka*, the court held that CFAA violations depend upon defendant's unauthorized use of access, not upon the unauthorized use of information obtained.[123]

A second interpretation of "access without authorization" emerged from a number of cases involving access that conflicted with contractual relationships or confidentiality or use agreements. The use of agreements to define criminal activity is by no means new or computer specific. Some courts have held that the breach of non-competition, non-disclosure or operating agreements satisfies the CFAA requirement. For instance, in *United States v. Rodriguez*, the notice to employees that prohibited access to information outside the scope of normal business reasons was construed to make such access unauthorized.[124] In contrast to that reasoning, the court in *WEC Carolina Energy Solutions LLC v. Miller* held that employer's policies regulated the *use* of information, not access to information, and did not establish the violation of policies with respect to access.[125]

---

[118] Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

[119] *See* Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 419–21 (7th Cir. 2006).

[120] Ervin & Smith Adver. & Pub. Relations, Inc. v. Ervin, No. 8:08CV459, 2009 WL 249998 (D. Neb. Feb. 3, 2009).

[121] *Id.* at *9.

[122] US Bioservices Corp. v. Lugo, 595 F. Supp. 2d 1189 (D. Kan. 2009).

[123] LVRC Holdings LCC v. Brekka, 581 F.3d 1127, 1132 (9th Cir. 2009).

[124] United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010).

[125] WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 206–07 (4th Cir. 2012).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

In *United States v. Phillips*, the defendant, an incoming University student, signed the computer-use policy and was granted certain privileges on the University computer system.[126] However, he engaged in prohibited conduct, such as port scanning, intrusion in restricted areas of the system, and extraction of confidential data.[127] The court found that these acts obviously fell well outside the scope of his authorization or the use intended by the access grantor.[128]

In *Hewlett-Packard Company v. Byd:Sign, Inc.*, the defendants, employees and contractors, agreed to the ethical standards set out in the plaintiff's "Standards of Business Conduct."[129] Even though terms of the Standards document restricted the sending or accessing of messages on the plaintiff's computer systems for personal gain, the defendants obtained and sent trade secrets and other proprietary information to an entity founded by them.[130] The court held the plaintiff successfully alleged actual access without or in excess of authorization and rejected defendant's motion to dismiss.[131]

In *eBay Inc. v. Digital Point Solutions, Inc.*, the plaintiff alleged a cookie-stuffing[132] scheme.[133] While eBay is a public website, accessible to anyone, access beyond the terms of the User Agreement, resulting in the improper payment of advertising fees, constitute unauthorized use.[134] The court held that access was unauthorized, as it was done to defraud the plaintiff by corrupting the advertising affiliate data.[135]

---

[126] United States v. Phillips, 477 F.3d 215, 217–18 (5th Cir. 2007).

[127] *Id.* at 218.

[128] *Id.*

[129] Hewlett-Packard Co. v. Byd:Sign, Inc., No. 6:05-CV-456, 2007 WL 275476, at *1 (E.D. Tex. Jan. 25, 2007) (order denying motion to dismiss).

[130] *Id.*

[131] *Id.*

[132] This is a scheme where the fraudster places cookies on a third party computer in order to "get paid a commission that the fraudster didn't earn legitimately by doing the things that the marketer wanted to pay for"—*see* Eric Goldman, *eBay Cracks Down on Cookie Stuffing—eBay v. Digital Point Solutions* (2008), *available at* http://blog.ericgoldman.org/archives/2008/09/ebay_cracks_dow.htm (last visited Feb. 23, 2014).

[133] eBay Inc. v. Digital Point Solutions, Inc., 608 F. Supp. 2d 1156, 1159 (N.D. Cal. 2009).

[134] *Id.*

[135] *Id.* at 1160, 1164.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

Cvent, Inc. v. Eventbrite, Inc. is an interesting case in which the plaintiff alleged the unauthorized employment of web scraping techniques.[136] The defendant argued that because Cvent's website is publicly available and requires no login or other individualized grant of access, there was no unauthorized access to it.[137] Cvent's CFAA claim was based on the provisions of its Terms of Use, which stated, "[n]o competitors or future competitors are permitted access to our site or information, and any such access by third parties is unauthorized."[138] However, the link to the Terms of Use was buried at the bottom of the first page, requiring users to affirmatively scroll down to the bottom of the page to see the link.[139] The court held that its Terms of Use did not protect Cvent in any meaningful way because they were posted in a manner that was unnoticeable to the reasonable user, and granted defendant's motion to dismiss the CFAA claim.[140] Clearly, in order to support CFAA claims, visible links to the terms of use and mandatory click-through should be placed on every important webpage or point of assent. While the unauthorized use of the Cvent material may have caused loss, the data stripped was public and therefore authorized access that would not support a claim under the CFAA.

An interesting contrast to the *Cvent* case can be found in in *Southwest Airlines Co. v. Farechase, Inc.*, where the defendant accessed and obtained data from plaintiff's website via a robot or other automated scraping device.[141] Southwest stated that their Use Agreement, accessible from all webpages, in addition to direct "repeated warnings and requests to stop scraping," makes defendant's access unauthorized.[142] Even though defendant argued that accessing fare and scheduling information, which Southwest publishes on Southwest.com, is not improper as a matter of law, the court admitted a cause of action under the CFAA because the defendant knew about the prohibited use of "any deep-link, page-scrape, robot, spider or other automatic device, program, algorithm or methodology which does the same things."[143]

---

[136] Cvent, Inc. v. Eventbrite, Inc., 739 F. Supp. 2d 927, 934 (E.D. Va. 2010).

[137] *Id.* at 932.

[138] *Id.*

[139] *Id.* at 933.

[140] *Id.* at 934.

[141] *See* Southwest Airlines Co. v. Farechase, Inc., 318 F. Supp. 2d 435, 439–40 (N.D. Tex. 2004).

[142] *Id.* at 439.

[143] *Id.*

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

The third approach to determine if access was unauthorized is code-based.[144] Professor Kerr's definition of "access without authorization" embraces this interpretation: "access that circumvents restrictions by code."[145] Kerr even argues that courts should "reject contract-based notions of authorization, and instead limit the scope of unauthorized access statutes to cases involving the circumvention of code-based restrictions,"[146] although this approach is not implied by the CFAA. Legal commentators are split with respect to Kerr's proposed unauthorized access definition or approach. While some commentators view this approach as suitable and more appropriate than the agency and contract approaches,[147] others consider it flawed and reject it.[148]

According to the code-based approach, individuals act without or outside permission only if they circumvent or bypass the access control mechanism in place (i.e. software features in place). According to this approach, where it is affirmatively alleged that defendants had full access to systems, therefore acting with authorization, allegations, although potential claims for other offenses, such as theft of trade secrets and breach of fiduciary duties or unfair competition, there will not be a claim under the CFAA's (a)(5)(ii) or (iii) subsections.[149] For instance, in *Poller v. Bioscrip, Inc.*, the court held that because access was granted in connection with performing job duties, that access, though disloyal, exploitative and in breach of the Restrictive Covenant Agreement, cannot be considered unauthorized under the CFAA.[150] Even if the CFAA would be regarded as

---

[144] *See* Kerr, *supra* note 106, at 1596; Andrew T. Hernacki, *A Vague Law in a Smartphone World: Limiting the Scope of Unauthorized Access Under the Computer Fraud and Abuse Act*, 61 AM. U. L. REV. 1543, 1560 (2012); Thomas E. Booms, *Hacking into Federal Court: Employee "Authorization" Under the Computer Fraud and Abuse Act*, 13 VAND. J. ENT. & TECH. L. 543, 551–52 (2011).

[145] Kerr, *supra* note 106, at 1649.

[146] *Id*. at 1600.

[147] *See, e.g.*, Kelsey T. Patterson, *Narrowing It Down to One Narrow View: Clarifying and Limiting the Computer Fraud and Abuse Act*, 7 CHARLESTON L. REV. 489, 530 (2013); Garrett D. Urban, Note, *Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act*, 52 WM. & MARY L. REV. 1369, 1402 (2011); Katherine Mesenbring Field, Note, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 841 (2009).

[148] *See* Thaw, *supra* note 16, at 927 (suggesting that this approach "is flawed and overlooks practical, theoretical, and normative problems"); Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass and Privacy*, 62 BUS. LAW. 1395, 1408 (2007) ("[M]achines alone cannot supply the law with a system of norms").

[149] *See* Condux Int'l, Inc. v. Haugum, No. 08-4824 ADM/JSM, 2008 WL 5244818, at *6 (D. Minn. Dec. 15, 2008); Trademotion, LLC v. Marketcliq, Inc., 857 F. Supp. 2d 1285, 1291 (M.D. Fla. 2012).

[150] Poller v. Bioscrip, Inc., No. 11 Civ. 1675 (JPO), 5354753 (S.D.N.Y. Sept. 25, 2013).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

ambiguous with respect to insiders that breach contractual obligations, such as keeping certain information confidential, the rule of lenity mandates that ambiguity is resolved in favor of the defendant.[151]

Employee's access under the code-based approach can be construed as unauthorized only if or when it occurs after an employee is terminated or resigned. This could be the case where the defendants accessed plaintiff's computer system after the plaintiffs no longer employed them.[152] Similarly, access after authorization had been revoked or following suspension from work have been construed as without authorization.[153]

The code-based approach is seriously challenged in situations where the authentication mechanism malfunctions, or where access permission or privileges are obtained fraudulently, granted in error, or used without the knowledge or consent of the access permission authority. This study revealed a number of cases where the code-based approach raised interesting questions or interpretations. For instance, in a case involving the circumvention of access, the defendant used his wife's password to view and delete data that he was not authorized to access.[154] The court held that because he was authorized to access the system his conduct concerned misuse of data rather than unauthorized access of a protected computer.[155] *IMS Inquiry Manag. Systems, Ltd. v. Berkshire Inform. Systems, Inc.* is another case where the defendant used access credentials issued to a third party, which constituted a breach of contract that the third party had with the plaintiff.[156] The defendant accessed the plaintiff's system without authorization and copied formats, with a view to create his own competing system.[157] Indirect access is also likely to be considered unauthorized access, based on access instructions issued to

[151] *See* Black & Decker (US), Inc. v. Smith, 568 F. Supp. 2d 929 (W.D. Tenn. 2008).

[152] *See* Beta Tech., Inc. v. Meyers, No. H-13-1282, 2013 WL 5602930 (S.D. Tex. Oct. 10, 2013); Hat World, Inc. v. Kelly, No. S-12-01591, 2012 WL 3283486 (E.D. Cal. Aug. 10, 2012).

[153] *See* Craigslist, Inc. v. 3Taps Inc., 942 F. Supp. 2d 962 (N.D. Cal. 2013) (regarding access after authorization revoked). *See* United States v. Kim, 677 F. Supp. 2d 930 (S.D. Tex. 2009) (regarding access following suspension from work).

[154] Wentworth-Douglass Hosp. v. Young & Novis Prof'l Ass'n, No. 10-cv-120-SM, 2010 WL 3023331 (D.N.H. July 8, 2010).

[155] *Id.*

[156] I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521 (S.D.N.Y. 2004).

[157] *Id.* at 523.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

a third party agent of the defendant, as the CFAA explicitly allows for liability under a conspiratorial theory.[158]

As this section demonstrates, "access without authorization" involves diverse situations and is open to conflicting interpretations. A clear and irrefutable definition of what "access without authorization" should mean is difficult to provide. Perhaps Congress realized that and left this element without definition so that the courts would infer the nature of access from precise circumstances or merits of each case.

D. Damage

The CFAA provisions relating to computer damage require the unauthorized transmission or access to cause damage to a protected computer. The CFAA defines the terms "damage" and "loss" differently.[159] "Damage" is defined in § 1030(e)(8) as "any impairment to the integrity or availability of data, a program, a system, or information."[160] Although the CFAA definition of damage is inclusive, it cannot be considered as unclear.[161] "Impairment" means deterioration or an "injurious lessening or weakening."[162] Impairment occurs only in circumstances resulting in "some diminution in the completeness or usability of data or information on a computer system."[163] The CFAA uses the singular of "impairment" to limit the damages threshold to a single act or event.[164] The damage amount, however, can be aggregated across time and individual computers.[165] Perpetrators need only intend to impair computer data or systems, not to inflict a specific damage or other harm.

Damage claims can include absconding with confidential computer data,[166] copying trade secrets onto a CD or PDA,[167] downloading, printing or e-mailing[168]

---

[158] *See* Energy Power Co. v. Wang, No. 13-11348-DJC, 2013 WL 6234625 (D. Mass. Dec. 3, 2013).

[159] *See* section E *supra* regarding definition of "loss."

[160] 18 U.S.C. § 1030(e)(8) (2012). Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121 (W.D. Wash. 2000) emphasized the importance of the word "any" in the definition.

[161] *See* United States v. Roque, No. 12-540 KM, 2013 WL 2474686 (D.N.J. June 6, 2013).

[162] Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295, 301 (6th Cir. 2011).

[163] *See* Garelli Wong & Assocs., Inc v. Nichols, 551 F. Supp. 2d 704, 709 (N.D. Ill. 2008).

[164] Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1158 (W.D. Wash. 2001).

[165] *Id.*

[166] *See* E.R. James Real Estate Servs., LLC v. Spinell, No. 11 C 4476, 2011 WL 5078873 (N.D. Ill. Oct. 26, 2011).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

or misappropriating trade secrets.[169] Such acts are legitimate business concerns and can rightly be regarded as disloyal and deceitful.[170] However, such acts do not give rise to claims for relief under the CFAA, as the acts do not impair computer data or systems and plaintiffs can still access the same data existing prior to defendants' actions.

For a damage claim to be successful it does not suffice for plaintiff to claim that information is personal or valuable (i.e., information concerning web browsing and shopping habits or purchases); there must be a showing that damage was actually inflicted.[171] Violations of privacy, such as online tracking[172] or the unauthorized collection and use or disclosure of personal identifiable information ("PII"), fall within that reasoning and are generally rejected by courts. For instance, in *In re Google Android Consumer Privacy Litigation*, the plaintiffs argued that code hidden in applications collected without their knowledge or consent PII, such as name, gender, zip code, geo-location, and the universally unique device identifier.[173] The court, however, dismissed the CFAA claim for failure to show the necessary damage or loss.[174]

A number of other privacy infringement claims brought under the CFAA were also dismissed for failure to show damage under the statute.[175] However, in

---

[167] *See* Lockheed Martin Corporation v. Speed, No. 6:05-CV-1580-ORL-31, 2006 U.S. Dist. LEXIS 53108, at *27 (M.D. Fla. Aug. 1, 2006).

[168] *See* Del Monte Fresh Produce, N.A. v. Chiquita Brands Int'l, 616 F. Supp. 2d 805, 828 (N.D. Ill. 2009). *See also* Garelli Wong & Assocs, Inc. v. Nichols, 551 F. Supp. 2d 704, 709 (N.D. Ill. 2008).

[169] *See* Andritz, Inc. v. Southern Maint. Contractor, LLC, 626 F. Supp. 2d 1264, 1266 (M.D. Ga. 2009).

[170] *See* Mintel Int'l Grp., Ltd. v. Neergheen, No. 08-cv-3939, 2010 U.S. Dis. LEXIS 2323, at *33 (N.D. Ill. Jan. 12, 2010).

[171] *See* Del Vecchio v. Amazon.com, Inc., No. C11-366RSL, 2011 WL 6325910, at *3 (W.D. Wash. Dec. 1, 2011) (dismissing a Computer Fraud and Abuse Act claim where plaintiffs did not allege facts showing devaluation of their data).

[172] For discussions on use of cookies for online tracking, see Christine Suzanne Davik, *We Know Who You Are and What You Are Made Of: The Illusion of Internet Anonymity and Its Impact on Protection from Genetic Discrimination*, 64 CASE W. RES. L. REV. 17 (2013); Chris Jay Hoofnagle et al., *Behavioral Advertising: The Offer You Can't Refuse*, 6 HARV. L. & POL'Y REV. 273 (2012); Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814 (2011).

[173] *In re* Google Android Consumer Privacy Litig. No. 11-MD-02264 JSW, 2013 WL 1283236 at *6 (N.D. Cal. Mar. 26, 2013).

[174] *Id.*

[175] *In re* Google Inc. Cookie Placement Consumer Privacy Litig., No. 12-2358-SLR, 2013 WL 5582866 (D. Del. Oct. 9, 2013); *In re* iPhone Application Litig., No. 11-MD-02250-LHK, 2011 WL

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

the class action case *Mortensen v. Bresnan Commc'n, LLC*, the plaintiffs withstood the defendant's motion to dismiss for failure to state sufficient damages.[176] In that case, the plaintiffs alleged that the defendant, an Internet Service Provider, diverted nearly all of plaintiffs' Internet communications to a third-party Internet advertising company.[177] The communications diversion was accomplished without the customers' consent and allowed the third-party advertiser to target the plaintiffs with preference-sensitive advertisement.[178] The court held that plaintiffs could aggregate their damages, which consisted of costs related to the investigation and repair of their computers, because the defendant's single act resulted in damages of a uniform nature exceeding $5,000 during any one-year period.[179] As such, plaintiffs' alleged damages were sufficient to survive the dismissal motion.

Under certain circumstances, terms of service or use agreements can prevent or enforce damage claims under the CFAA. For instance, in *Serrano v. Cablevision Systems Corp.*, the Plaintiff claimed violation of section 1030(a)(5)(A)–(C) based on severely downgraded speed of services received.[180] However, defendant's Terms of Service provided that, in order to protect the integrity of their network and resources, certain actions deemed necessary could be employed.[181] Such actions would include "port blocking, e-mail virus scanning, denying e-mail from certain domains, and putting limits on bandwidth and e-mail."[182] The Acceptable Use Policy further stated that "[e]xcessive use of bandwidth, that in Cablevision's sole opinion, goes above normal usage or goes beyond the limit allocated to the user" is a "network security violation."[183] Consequently, the court held that the defendant did not act "without authorization" when it restricted the bandwidth and rejected the claim as defeated by the Terms of Service and Acceptable Use Policy.[184]

4403963 (N.D. Cal. Sept. 20, 2011); Opperman v. Path, A-12-CA-219-SS, 2012 WL 4105189 (W.D. Tex. Aug. 23, 2012); *In re* DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497 (S.D.N.Y. 2001); *In re* Intuit Privacy Litigation, 138 F. Supp. 2d 1272 (C.D. Cal. 2001).

[176] Mortensen v. Bresnan Commc'n, LLC, No. 10-13-BLG-RFC, at *1 (D. Mont. Dec. 13, 2010).

[177] *Id.*

[178] *Id.*

[179] *Id.* at *7.

[180] Serrano v. Cablevision Sys. Corp., 863 F. Supp. 2d 157 (E.D.N.Y. 2012).

[181] *Id.* at 161–62.

[182] *Id.* at 162.

[183] *Id.*

[184] *Id.* at 167.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

The *Serrano* case shows that valid contractual provisions can defeat what would otherwise be a legitimate damage claim for diminishing or denying the ability to receive and transmit computer data. In *Craigslist, Inc. v. Naturemarket, Inc.*, however, the defendants developed, advertised and sold products and services that enabled users to circumvent security measures and access parts of the copyright-protected website without authorization.[185] Such actions constituted a violation of the plaintiff's Terms of Use Agreement, which imposed certain website access and use restrictions.[186] Consequently, the claims brought under § 1030(a)(5)(B) and (C) for willful, malicious, and fraudulent conduct, were considered sufficient under the CFAA.[187]

In *Clinton Plumbing and Heating of Trenton, Inc. v. Ciaccio*, the plaintiff alleged unauthorized transfers from bank accounts to defendant's personal credit card account.[188] Specifically, the plaintiff claimed that these transfers impaired the integrity of the bank account's information by changing the balance reflected in the account from almost $150,000 to $0.[189] Though the court found the argument creative, however, held that it went too far: "plaintiffs do not allege that the integrity of *data* was impaired; instead, they allege the integrity of their *bank funds* was impaired."[190] Consequently, the court held that "this claim does not allege damage for the purposes of the CFAA."[191] Clearly, this was a computer fraud case to be pleaded under § 1030(a)(4), not a computer damage case to be pleaded under § 1030(a)(5).

Damage can be inflicted in a number of ways. For instance, via a "time bomb" program;[192] changing the firewall and employees' passwords;[193] or accessing and password protecting the wireless antennae assigned to customers by a former employer, thereby obtaining exclusive use of businesses' MAC

---

[185] Craigslist, Inc. v. Naturemarket, Inc., 694 F. Supp. 2d 1039 (N.D. Cal. 2010).

[186] *Id.* at 1048.

[187] *Id.*

[188] Clinton Plumbing & Heating of Trenton, Inc. v. Ciaccio, No. 09-2751, 2010 WL 4224473 (E.D. Pa. Oct. 22, 2010).

[189] *Id.* at *6.

[190] *Id.* (emphasis added).

[191] *Id.*

[192] *See* United States v. Lloyd, 269 F.3d 228 (3d Cir. 2001) (where the malicious code was installed by the perpetrator while an employee, by direct access, and detonated after the perpetrator was fired).

[193] *See* United States v. Fowler, No. 8:10-cr-65-T-24AEP, 2010 WL 4269618 (M.D. Fla. Oct. 25, 2010).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

addresses.[194] Allegations not supported by convincing evidence, however, are legally insufficient. For example, in *Eagle v. Morgan*, plaintiff, while President of Edcomm, set up a LinkedIn account to promote Edcomm's banking education services; foster her reputation as a businesswoman; reconnect with family, friends, and colleagues; and build social and professional relationships.[195] Following her termination from Edcomm, the employer changed the LinkedIn password and Eagle was no longer able to access the account.[196] Plaintiff claimed that the inability to respond to actual or potential clients damaged her goodwill and resulted in much less services sold by her.[197] The court held, however, that the plaintiff failed to show a "clear and unbroken causal connection" between her alleged losses and her damages relating to her inability to use Linkedln and rejected the CFAA claim.[198]

In a number of other cases involving serious allegations, the plaintiffs' right to relief on the claims were denied as they failed to produce convincing evidence of damages under the CFAA. Such claims included: computer infected with a virus;[199] impaired ability of customers to log in to computers and impaired integrity of certain data;[200] remote placement of spyware and removal of data;[201] transmission of a Trojan horse to plaintiffs' computer, with a view to destroying evidence of unauthorized access;[202] deleted files and altered access passwords;[203] uploaded malicious files to server;[204] and denial of access to personal e-mail accounts.[205]

In one case the plaintiff alleged threats to public health or safety, based on the use of computers containing faulty microcode in hospitals, banks and medical

---

[194] *See* United States v. Schuster, 467 F.3d 614 (7th Cir. 2006).

[195] *See* Eagle v. Morgan, No. 11-4303, 2012 WL 4739436 at *6 (E.D. Pa. Oct. 4, 2012).

[196] *Id.*

[197] *Id.*

[198] *Id.*

[199] Ryan v. Harlan, No. 10-CV-626-ST, 2011 WL 711110 (D. Or. Feb. 22, 2011).

[200] Oracle Corp. v. SAP AG, 734 F. Supp. 2d 956 (N.D. Cal. 2010).

[201] JBCHoldings NY, LLC v. Pakter, 931 F. Supp. 2d 514 (S.D.N.Y. Mar. 20, 2013).

[202] Expert Bus. Sys, LLC v. Bi4ce, Inc., 411 F. Supp. 2d 601 (D. Md. 2006).

[203] LaBovick & LaBovick, PA v. Simovitch, No. 12-80061-CV, 2012 WL 920767 (S.D. Fla. Mar. 19, 2012).

[204] Ground Zero Museum Workshop v. Wilson, 813 F. Supp. 2d 678 (D. Md. 2011).

[205] Modrowski v. Pigatto, 712 F.3d 1166 (7th Cir. 2013).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

laboratories; but the court found the evidence presented unpersuasive.[206] Plaintiffs, however, offered no evidence that the FDC microcode caused damage that "modifies, impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals."[207] Furthermore, plaintiffs failed to produce evidence that the FDC caused damage that "threatens public health or safety."[208]

The number of cases dismissed on plaintiffs' failure to show cognizable evidence that their computers were damaged or suffered the required loss is much larger.[209] In one case, the court not only dismissed the plaintiff's damage allegations, but also considered the allegations as rising to the level of the delusional, irrational and incredible.[210]

---

[206] Thurmond v. Compaq Computer Corp., 171 F. Supp. 2d 667, 678 (E.D. Tex. 2001).

[207] *Id.* at 679.

[208] *Id.*

[209] *See, e.g.*, Global Fleet Sales, LLC v. Delunas, No. 12-15471 (E.D. Mich. Feb. 18, 2014); Wichansky v. Zowine, No. CV-13-01208-PHX-DGC (D. Ariz. Jan. 24, 2014); Harley Auto. Grp., Inc. v. AP Supply, Inc., No. CIV. 12-1110 DWF/LIB, 2013 WL 6801221 (D. Minn. Dec. 23, 2013); Metabyte, Inc. v. NVIDIA Corp., No. 12-0044 SC, 2013 WL 1729808 (N.D. Cal. Apr. 22, 2013); Vehicle Valuation Servs. v. DiMaria, No. 13 C 5094, 2013 WL 5587089 (N.D. Ill. Oct. 10, 2013); New S. Equip. Mats, LLC v. Keener, No. 3:13CV162TSL-JMR, 2013 WL 5946371 (S.D. Miss. Nov. 5, 2013); Reynolds & Reynolds Company v. Superior Integrated Solutions, Inc., No. 1:12-cv-848, 2013 WL 2456093 (S.D. Ohio June 6, 2013); Ocean Tomo, LLC v. Barney, No. 12 C 8450, 2013 WL 4804980 (N.D. Ill. Sept. 9, 2013); Schatzki v. Weiser Capital Mgmt., LLC, No. 10 CIV. 4685, 2012 WL 169779 (S.D.N.Y. Jan. 19, 2012); PNC Mortgage v. Superior Mortgage Corp., No. CIV.A. 09-5084, 2012 WL 628000 (E.D. Pa. Feb. 27, 2012); Oracle Am., Inc. v. Serv. Key, LLC, No. C 12-00790 SBA, 2012 WL 6019580 (N.D. Cal. Dec. 3, 2012); Bashaw v. Johnson, No. 11-2693-JWL, 2012 WL 1623483 (D. Kan. May 9, 2012); Alliantgroup, L.P. v. Feingold, 803 F. Supp. 2d 610 (S.D. Tex. 2011); 1st Rate Mortgage Corp. v. Vision Mortgage Servs. Corp., No. 09-C-471, 2011 WL 666088 (E.D. Wis. Feb. 15, 2011); Devine v. Kapasi, 729 F. Supp. 2d 1024 (N.D. Ill. 2010); ReMedPar, Inc. v. AllParts Med., LLC, 683 F. Supp. 2d 605 (M.D. Tenn. 2010); Clinton Plumbing & Heating of Trenton, Inc. v. Ciaccio, No. CIV. 09-2751, 2010 WL 4224473 (E.D. Pa. Oct. 22, 2010); Von Holdt v. A-1 Tool Corp., 714 F. Supp. 2d 863 (N.D. Ill. 2010); Mintel Int'l Grp., Ltd. v. Neergheen, No. 08-cv-3939, 2010 U.S. Dis. LEXIS 2323 (N.D. Ill. Jan. 12, 2010); Oce N. Am., Inc. v. MCS Servs., Inc., 748 F. Supp. 2d 481 (D. Md. 2010); Hillsboro Dental, LLC v. Hartford Cas. Ins., Co., 410-CV-271CEJ, 2010 WL 5184956 (E.D. Mo. Dec. 14, 2010); Lasco Foods, Inc. v. Hall & Shaw Sales, Mktg. & Consulting, LLC, 600 F. Supp. 2d 1045 (E.D. Mo. 2009); Modis, Inc. v. Bardelli, 531 F. Supp. 2d 314 (D. Conn. 2008); Joe N. Pratt Ins. v. Doane, No. CIV.A. V-07-07, 2009 WL 3157337 (S.D. Tex. Sept. 25, 2009); Am. Family Mut. Ins. Co. v. Rickman, 554 F. Supp. 2d 766 (N.D. Ohio 2008); Bansal v. Russ, 513 F. Supp. 2d 264 (E.D. Pa. 2007); Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479 (D. Md. 2005); SecureInfo Corp. v. Telos Corp., 387 F. Supp. 2d 593 (E.D. Va. 2005); Register.com, Inc. v. Verio, Inc., 356 F.3d 393 (2d Cir. 2004); Christian v. Sony Corp. of Am., 152 F. Supp. 2d 1184 (D. Minn. 2001).

[210] Arbino v. Microsoft, No. 1:12-CV-566, 2012 WL 3234279 (S.D. Ohio Aug. 7, 2012) (The plaintiff, unable to obtain the code required to reinstall Windows, asked $500,000 in damages, claiming that "[a]ctivating your computer and this whole business with getting numbers is unnecessary to the

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

It is appropriate to conclude this section with one court's reflection: "[g]ood lawyering does not require pleading every cause of action that may even remotely appear possible. Rather, it requires careful analysis and selectivity."[211]

E. Loss

While all of the CFAA provisions require there be damage to a protected computer, one of the provisions requires "damage and loss." The CFAA defines "loss" in section 1030(e)(11) as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring 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."[212] "Loss" includes harms such as lost advertising revenue, lost sales due to a website outage, and lost salaries of employees who are unable to work due to computer system impairment or interruption.[213] Losses can also include the cost of forensic analysis and remedial measures associated with retrieving and analyzing data,[214] including forensic attempts to restore deleted files and obtaining duplicate financial records; costs to restore financial information;[215] and costs pertaining to goodwill,[216] as all are economic damages. However, lost revenue due to misappropriation of proprietary information is not recoverable under the CFAA.[217]

The court in *Fidlar Technologies v. LPS Real Estate Data Solutions, Inc.* noted that the common interpretation of "loss" ignores the opening clause—"any reasonable cost to any victim"—and argued that the two examples after the word "including" are nonexclusive.[218] The court further argued that the CFAA provides two ways in which loss could be experienced, but found these cannot be the only

---

proper functioning of the computer and is only being carried out by the defendant to pla[y] the satanic game *ride 'em*.").

[211] DocMagic, Inc. v. Ellie Mae, Inc., 745 F. Supp. 2d 1119, 1155 (N.D. Cal. 2010).

[212] 18 U.S.C. § 1030(e)(11) (2012).

[213] *See* Jarrett, *supra* note 111, at 43.

[214] *See* Lasco Foods, Inc. v. Hall & Shaw Sales, Mktg. & Consulting, LLC, 600 F. Supp. 2d 1045 (E.D. Mo. 2009).

[215] *See* Patrick Patterson Custom Homes, Inc. v. Bach, 586 F. Supp. 2d 1026 (N.D. Ill. 2008).

[216] *See* Creative Computing v. Getloaded.com LLC, 386 F.3d 930 (9th Cir. 2004).

[217] *See* ES & H, Inc. v. Allied Safety Consultants, Inc., No. 3:08-CV-323, 2009 WL 2996340 (E.D. Tenn. Sept. 16, 2009).

[218] Fidlar Technologies v. LPS Real Estate Data Solutions, Inc., No. 4:13-CV-4021-SLD-JAG, 2013 U.S. Dist. LEXIS 159929, at *16 (C.D. Ill. Nov. 8, 2013).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

ways, because viewing the opening clause "any reasonable cost" to read otherwise would render the clause meaningless.[219] However, the court in *Von Holdt v. A-1 Tool Corp.*, reasoned that all loss must be the result of "interruption of service."[220] Otherwise, it would appear that the second half of the "loss" definition is surplusage.[221] The court reasoned that if the loss could be any reasonable cost without any interruption of service, then the legislature would have had no reason to include a second half to the definition, which limited some costs to an interruption of service.[222] Rather, the court determined the better reading would be that all "loss" must be the result of an interruption of service.[223]

Numerous costs are excluded in the calculation of loss. For instance, litigation costs, as emphasized in a number of cases, cannot be considered compensable under the CFAA.[224] These costs are excluded as not being related to the investigation or a remedy of the damage suffered, which can lead to situations where the prevailing party's litigation costs exceed the awarded damages. Costs related to testifying on behalf of the government or assisting the Federal Bureau of Investigation ("FBI") in the investigation of these offenses are also excluded.[225] Additionally, emotional distress claims in cases of privacy invasion[226] and lost profits due to unfair competitive advantage[227] also fall outside loss redressable under the CFAA provisions.

In *Chance v. Avenue A, Inc.*, the attempt to circumvent the statute's $5,000 threshold by contending that loss, as opposed to damages, is not subject to that requirement, received some merit from the court.[228] Even though the court remarked that the section is inconsistent regarding the interrelationship of damage and loss, the court nevertheless held that CFAA's context requires the inclusion of

---

[219] *Id.*

[220] Von Holdt v. A-1 Tool Corp., 714 F. Supp. 2d 863 (N.D. Ill. 2010).

[221] *Id.*

[222] *Id.*

[223] *Id.*

[224] Brooks v. AM Resorts, LLC, No. 11-995, 2013 U.S. Dist. LEXIS 93372 (E.D. Pa. July 3, 2013); Mintz v. Mark Bartelstein and Assocs., Inc., 906 F. Supp. 2d 1017 (C.D. Cal. 2012); Wilson v. Moreau, 440 F. Supp. 2d 81 (D.R.I. 2006).

[225] United States v. Schuster, 467 F.3d 614, 619 (7th Cir. 2006).

[226] Frees, Inc. v. McMillian, No. 05-1979, 2007 U.S. Dist. LEXIS 57211, at *14 (W.D. La. Aug. 6, 2007).

[227] Civic Ctr. Motors, Ltd. v. Mason St. Imp. Cars, Ltd., 387 F. Supp. 2d 378, 380 (S.D.N.Y. 2005).

[228] Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153 (W.D. Wash. 2001).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

loss within the $5,000 threshold.[229] The *In re DoubleClick Inc. Privacy Litigation* court also admitted that the CFAA is ambiguous about whether "loss" under § 1030(g) is subject to § 1030(e)(8)'s $5,000 threshold.[230]

Loss calculation can be complex,[231] the inclusion of certain costs being outside the alleged CFAA violation[232] or excessive (such as certain travel expenses, not required in the computer investigation or repair).[233] In *Fink v. Time Warner Cable*, for instance, the plaintiffs alleged "throttling" practices that interfered with and limited the performance of their systems.[234] The alleged acts resulted in lost work opportunities and wasted time and effort to determine the cause for the slow connection.[235] The court held, however, that the loss pleaded, although sufficiently specific, fell outside the kind of loss that the CFAA requires.[236]

The analysis of the "loss" element shows another split of legal authority. Some courts have held that it is necessary for a plaintiff to plead both damage and loss, in order to properly allege a civil CFAA violation,[237] whereas other courts have held that plaintiffs can recover for either "damage" or "loss,"[238] because there is no requirement for a civil plaintiff to allege damage if they can state a loss aggregating at least $5,000.[239] Utilizing the fact that the word "or" was present in the CFAA, the court reasoned that the plaintiff needs to allege damage *or* loss, not both.[240]

Dice Corporation v. Bold Technologie contains a lengthy examination of whether the word "and" in the CFAA definition is disjunctive, and should, in fact, be understood as "or."[241] The court cited the following hypothetical example of loss

---

[229] *Id.* at 1159–60 (the court held that a different interpretation "would yield the absurd result that any 'loss' different from pure economic damages would not be subject to any threshold amount").

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

[231] *See* NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1074–76 (S.D. Iowa 2009).

[232] *See* Global Policy Partners, LLC v. Yessin, 686 F. Supp. 2d 642, 651–52 (E.D. Va. 2010).

[233] *See* Nexans Wires S.A. v. Sark-USA, Inc., 319 F. Supp. 2d 468, 476–77 (S.D.N.Y. 2004).

[234] Fink v. Time Warner Cable, 810 F. Supp. 2d 633, 639 (S.D.N.Y. 2011).

[235] *Id.*

[236] *Id.* at 639.

[237] *See* Garelli Wong & Assocs., Inc v. Nichols, 551 F. Supp. 2d 704, 708 (N.D. Ill. 2008).

[238] Grubb v. Bd. of Trustees of the Univ. of Illinois, 730 F. Supp. 2d 860, 866 (N.D. Ill. 2010).

[239] Southwest Airlines Co. v. Farechase, Inc., 318 F. Supp. 2d 435, 439 (N.D. Tex. 2004).

[240] Motorola, Inc. v. Lemko Corp., 609 F. Supp. 2d 760, 767 (N.D. Ill. 2009).

[241] Dice Corp. v. Bold Technologies, No. 11-13578, 2012 WL 263031 (E.D. Mich. Jan. 30, 2012).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

without actual damage: if the perpetrator replaces the log-on program to obtain a users' password and subsequently restores the program, while there has been no "damage," the victim suffers "loss" through the necessity of resources being allocated to address the security breach.[242] In the event that the required monetary threshold is met, the conduct could also be prosecuted.[243] In this hypothetical example however, the integrity or availability of the log-on program, depending on whether it was rewritten or replaced, was temporarily affected.[244] A better example, illustrating a system rendered insecure or liable to danger without producing actual damage, would be the surreptitious installation of a backdoor, which would allow the perpetrator to remotely access the system.

As one court reasoned, even if the victim could have prevented some or all harm by installing certain security software, a causal chain from the perpetrator to the victim is not broken by vulnerabilities that the victim negligently left open.[245] Determining the implications of the intrusion, or the extent of the problem, is essential to mitigating the security risk.[246] If the "prophylactic" measures required to secure the compromised system satisfies the monetary requirement, the conduct can be prosecuted as computer damage under the CFAA.[247]

The failure to provide cognoscible loss figures, even though the damage and access elements were successfully demonstrated, resulted in numerous dismissed claims. Claims were dismissed, for instance, in cases involving use of flash cookies,[248] and misappropriation of personal data or computer interference.[249] By contrast, in a case where the plaintiff convincingly alleged that the reading and forwarding of her e-mails without authorization had violated her privacy in a way that produced economic loss, including the loss of salary, income and opportunity

[242] *Id.*

[243] *Id.*

[244] *Id.*

[245] *See* Creative Computing v. Getloaded.Com LLC, 386 F.3d 930 (9th Cir. 2004).

[246] *See* United States v. Heckenkamp, 482 F.3d 1142 (9th Cir. 2007).

[247] University Sports Publ'ns. Co. v. Playmakers Media Co., 725 F. Supp. 2d 378, 388 (S.D.N.Y. 2010).

[248] Flash local shared objects ("LSOs") or flash cookies are Adobe files used by developers to store data, with a view to tracking users' online behavior.

[249] *See* Bose v. Interclick, Inc., No. 10 Civ. 9183, 2011 U.S. Dist. LEXIS 93663, at *1 (S.D.N.Y. Aug. 17, 2011); La Court v. Specific Media, Inc., No. 10-01256-GW, 2011 U.S. Dist. LEXIS 50543, at *1 (C.D. Cal. Apr. 28, 2011).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

as an elected official, surpassing $5,000 in a one-year period, the court held that subsection (a)(5)(B)(i) requirement was satisfied.[250]

Loss based on the use of confidential or proprietary information has received conflicting interpretations from courts. In *Resource Cen. for Ind. Living v. Ability Resources*, the claim alleged misconduct by defendants while employed by the plaintiff.[251] According to the complaint, the defendants intentionally accessed the plaintiff's protected computer without authorization and caused loss by obtaining confidential and proprietary information for the benefit of their competing enterprise.[252] The court found the claim valid under the CFAA and denied the defendants' motion to dismiss.[253] Conversely, in *Quantlab Technologies Ltd. (BVI) v. Godlevsky*, the defendants provided software and confidential documents to a competitor before leaving their employment.[254] The court held that the plaintiff's claim brought under § 1030(a)(5)(B)(i) provided no figures with respect to the incident, and therefore did not stand as cognizable loss under the CFAA.[255]

Abuse of Terms of Use agreements has also received conflicting interpretations in courts with regards to the loss incurred. In *Therapeutic Research Faculty v. NBTY, Inc.*, the defendant acquired a single user subscription to a service, which specifically restricted access to "one and only one person."[256] Several employees used the service thereby infringing the Terms of Use agreement.[257] The court held that the plaintiff's alleged loss, which was a result of the breach of a single user license agreement, was meritorious under the CFAA.[258]

A contrasting approach can be found in *CoStar Realty Info., Inc. v. Field*, where access to the plaintiff's database was based on licenses to authorized users.[259] Access was enforced by means of passcode, and the Terms of Use

---

[250] Steinbach v. Village of Forest Park, No. 06 C 4215, 2009 WL 2605283 (N.D. Ill. Aug. 25, 2009).

[251] Res. Ctr. for Indep. Living, Inc. v. Ability Res., 534 F. Supp. 2d 1204, 1207 (D. Kan. 2008).

[252] *Id.* at 1210.

[253] *Id.* at 1211.

[254] Quantlab Techs. Ltd. (BVI) v. Godlevsky, 719 F. Supp. 2d 766, 770–71 (S.D. Tex. 2010).

[255] *Id.* at 776.

[256] Therapeutic Research Faculty v. NBTY, Inc., 488 F. Supp. 2d 991, 993 (E.D. Cal. 2007).

[257] *Id.* at 933.

[258] *Id.* at 996–97 ("a full corporate license for NBTY and its subsidiaries would cost approximately forty thousand dollars . . . per year," as opposed to under $100 for "an annual single user limited-purpose subscription for Internet access.").

[259] CoStar Realty Info., Inc. v. Field, 737 F. Supp. 2d 496, 499–500 (D. Md. 2010).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

specifically prohibited authorized users from providing the passcode to others.[260] However, authorized users sublicensed access to the CoStar database to a third party for a fee.[261] The third party also provided other entities with access to the CoStar database.[262] The court found that the claimed lost revenue was based solely on license fees that plaintiffs would have recouped if the defendants had entered into a License Agreement.[263] The court took the restrictive interpretation of "loss," and held that violations under the CFAA must cause an interruption of service, in order for the lost revenue to constitute cognizable CFAA loss.[264]

In *Fidlar Technologies v. LPS Real Estate Data Solutions, Inc.*, the plaintiff alleged that the defendant used a "web harvester" computer program without authorization, to electronically acquire data from images, in a way not possible for the typical user of plaintiff's software, and without incurring print fees.[265] Such actions impaired the integrity of the plaintiff's technology, allowing the defendant to bypassed various controls and use the system in an unauthorized manner, which ultimately forced the plaintiff to take actions to address the problem.[266] The court considered this loss meritorious under the CFAA.[267]

Loss can include the cost of all measures necessary to restore the secure posture of the system following a break-in, although it can be argued that certain measures would have been needed anyway, regardless of the alleged conduct.[268] In *Facebook, Inc. v. Power Ventures, Inc.*, the plaintiff alleged costs associated with the implementation of technical measures to prevent users from accessing its website via other entities, as these ways of access had not been authorized by the

---

[260] *Id.* at 500.

[261] *Id.* at 501.

[262] *Id.*

[263] *Id.* at 509.

[264] *Id.* at 515.

[265] Order Denying Defendant's Motions for Injunctive Relief and Dismissal at 5, Fidlar Technologies v. LPS Real Estate Data Solutions, Inc., No. 4:13-cv-4021-SLD-JAG (C.D. Ill. Nov. 8, 2013), *available at* http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1565&context=historical.

[266] *Id.* at 6.

[267] *Id.*

[268] *See* Creative Computing v. Getloaded.Com LLC, 386 F.3d 930, 935 (9th Cir. 2004) (where defendant argued that "many of the expenses for which Creative Computing claimed damages were routine computer maintenance and upgrades they would have needed to do anyway. Getloaded also argued that, had truckstop.com installed Microsoft's free patch, which had been distributed before Getloaded hacked in, the hack would have been prevented.").

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

plaintiff.[269] In *Navistar, Inc. v. New Baltimore Garage, Inc.*, the plaintiff alleged unauthorized use and distribution of access codes to their computer system, which enabled unauthorized third parties to access proprietary and confidential materials, in violation of the parties' agreements and to plaintiff's detriment.[270] The court held that the costs incurred to investigate the extent of the unauthorized computer access, even if the alleged conduct may have caused no damage, also satisfied the CFAA's definition of loss.[271] In *United States v. Millot*, the work performed on plaintiff's behalf by a third party to respond to a security breach, exceeding the minimum amount required for loss, was also considered sufficient for the CFAA claim.[272]

In *AV ex rel. Vanderhye v. iParadigms, LLC*, the plaintiff was initially unaware that no security measures had been circumvented, the unauthorized access to the systems being obtained via a password, posted on the Internet.[273] The court remanded the claim for further consideration, without expressing an opinion on whether the evidence supported a reasonable claim under the CFAA.[274] In situations where the amount of time alleged is unreasonable or not causally related to the CFAA violation, the loss requirement is considered unsatisfied.[275]

II. PERPETRATION ASPECTS

Successful computer attacks are the result of various problems, such as poor authentication, exploitation of trust mechanisms, software bugs, or administrative errors. Successfully combating these attacks, from a legislative, law enforcement or organizational perspective, requires an understanding of the perpetration aspects, such as attack platform, method, results, and perpetrator profiles.

A. Means and Results

The "transmission" form of computer damage often involves the deletion of computer data or files. As ordinary deletion makes the space allocated for the deleted element available for future writing, in a number of cases perpetrators used

[269] Facebook, Inc. v. Power Ventures, Inc., 844 F. Supp. 2d 1025, 1027 (N.D. Cal. 2012).

[270] Navistar, Inc. v. New Baltimore Garage, Inc., No. 11-cv-6269, 2012 WL 4338816, *8 (N.D. Ill. Sept. 20, 2012).

[271] *Id.*

[272] *See* United States v. Millot, 433 F.3d 1057 (8th Cir. 2006).

[273] AV *ex rel.* Vanderhye v. iParadigms, LLC, 562 F.3d 630, 635 (4th Cir. 2009).

[274] *Id.* at 646.

[275] *See, e.g.*, Global Policy Partners, LLC v. Yessin, 686 F. Supp. 2d 642, 647 (E.D. Va. 2010).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

specialized data erasure or wiping programs, to ensure unrecoverable removal of computer data. Examples of such software include Evidence Eliminator,[276] Kill Disk,[277] SecureClean,[278] ARO 2012,[279] Eraser,[280] Window Washer[281] or unnamed special programs that write every single sector on the drive.[282] To cover wrongful acts explicitly prohibited by the employment agreement, one defendant physically destroyed the hard drive of the laptop received from his employer, then installed a new hard drive.[283] In another insider case, an administrative assistant deleted computer files and used a shredding program to destroy certain files on a laptop computer so that the frauds she perpetrated (checks to "cash" or payments to herself and her personal creditors using electronic transfers) would not be discovered or would become non-traceable.[284] In spite of malware's well-documented capacity for wiping computer data on a massive scale,[285] this study found no such cases in Unites States' federal courts.

In order to misappropriate or prevent use of property, perpetrators sometimes alter[286] or encrypt computer data.[287] Other forms of computer damage encountered include web vandalism (defacing or altering the content of websites),[288] depleting

[276] KLA-Tencor Corp. v. Murphy, 717 F. Supp. 2d 895, 900 (N.D. Cal. 2010).

[277] Devon Energy Corp. v. Westacott, No. H-09-1689, 2011 WL 1157334, at *2 (S.D. Tex. Mar. 24, 2011).

[278] Position Technologies, Inc. v. Johnson, No. 10-C-3614, 2010 WL 5135905, at *1 (N.D. Ill. Dec. 10, 2010).

[279] Beta Tech., Inc. v. Meyers, No. H-13-1282, 2013 WL 5602930 (S.D. Tex. Oct. 10, 2013).

[280] Deloitte & Touche LLP v. Carlson, No. 11-C-327, 2011 WL 2923865 (N.D. Ill. July 18, 2011).

[281] Mobile Mark, Inc. v. Pakosz, No. 11 C 2983, 2011 WL 3898032 (N.D. Ill. 2011).

[282] *See* Keen v. Bovie Med. Corp., No. 8:12-CV-305-T-24-EAJ, 2013 WL 3832382, at *1 (M.D. Fla. May 7, 2013); Clarity Servs., Inc. v. Barney, 698 F. Supp. 2d 1309, 1313 (M.D. Fla. 2010).

[283] *Deloitte*, 2011 WL 2923865, at *2.

[284] Patrick Patterson Custom Homes, Inc. v. Bach, 586 F. Supp. 2d 1026, 1030 (N.D. Ill. 2008).

[285] *See* Ryan Sherstobitoff et al., *Dissecting Operation Troy: Cyberespionage in South Korea*, MCAFEE 3 (2013), http://www.mcafee.com/us/resources/white-papers/wp-dissecting-operation-troy.pdf (last visited Nov. 19, 2013) (describing a case where the disks of tens of thousands of computers were wiped by malware).

[286] *See* United States v. Dinh, No. 09 Cr. 327-01, 2011 WL 1197666, at *3 (S.D.N.Y. Mar. 29, 2011).

[287] *See* Energy Power Co. Ltd. v. Wang, Civil Action No. 13-11348-DJC, 2013 WL 6234625, at *1 (D. Mass. Dec. 3, 2013).

[288] *See Pleasant Hill, California Computer Hacker from "Deceptive Duo" Guilty of Intrusions into Government Computers and Defacing Websites*, U.S. DEPT. OF JUSTICE (2005), *available at*

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

system resources,[289] or uninstalling security features (thereby rendering systems more vulnerable to penetrations).[290] Damage can be inflicted via specialized software, such as the open source computer application Low Orbit Ion Cannon ("LOIC")[291] or other malicious code.

Access "without authorization" can be obtained in a number of ways, such as impersonating authorized users. In *United States v. Batti*, the perpetrator knew the password of a colleague.[292] After the defendant was fired, his former colleague's password was only slighted altered and through trial, he was able to guess the new password.[293] In another case, the perpetrator, who was overlooked for promotion, resigned and subsequently engaged in sabotaging the computer system of his former company.[294] The sabotage included the modification of the business calendar, which he accomplished by using the security credentials of at least one former colleague, which he had obtained following the break-in to the company's computer system.[295] In *Technology Sourcing, Inc. v. Griffin*, the defendant, after he was fired, used passcodes connected to his former employment to manipulate the computer system of a client, causing a network crash.[296]

In *United States v. Millot*, the defendant was in charge of the administration of SecureID cards or active devices that generate numbers used to access computer systems and accounts.[297] During his employment by the victim, he reassigned an account to one of the inventoried SecureID cards and then increased the access

---

http://www.justice.gov/criminal/cybercrime/press-releases/2005/lyttlePlea.htm [hereinafter U.S. DEPT. OF JUSTICE].

[289] *See* Indictment at 24, United States v. Ancheta, No. 05-1060 (C.D. Cal. Feb. 2005), *available at* http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf.

[290] United States v. McGraw, No. 3:09-CR-0210-B, 2012 WL 6013528 (N.D. Tex. Nov. 30, 2012). *See also* James T. Jacks, *Former Security Guard, Who Hacked into Hospital's Computer System, is Sentenced to 110 Months in Federal Prison*, U.S. DEPT. OF JUSTICE, http://www.justice.gov/usao/txn/PressRel11/mcgraw_jesse_sen_pr.html (Mar. 8, 2011).

[291] United States v. Collins, No. 11-CR-00471-DLJ, 2013 WL 1089908 (N.D. Cal. Mar. 15, 2013).

[292] United States v. Batti, 631 F.3d 371 (6th Cir. 2011).

[293] *Id.*

[294] U.S. Attorney's Office, *Long Island Software Programmer Arrested for Hacking into Network of High-Voltage Power Manufacturer*, FBI (May 2, 2013), http://www.fbi.gov/newyork/press-releases/2013/long-island-software-programmer-arrested-for-hacking-into-network-of-high-voltage-power-manufacturer.

[295] *Id.*

[296] *See* Technology Sourcing, Inc. v. Griffin, No. 10-C-4959, 2013 WL 1828750 (N.D. Ill. Apr. 30, 2013).

[297] United States v. Millot, 433 F.3d 1057, 1059 (8th Cir. 2006).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

level of that account to the highest level available.[298] After he left the employment, he kept the SecureID card assigned to the modified account and was able to gain remote access to the victim's system.[299]

Access "without authorization" can also be accomplished by exploiting issues that render a system to enter a non-secure state, such as software vulnerabilities (e.g., in SQL attacks).[300] To find or exploit vulnerabilities, perpetrators use dedicated software, such as Havij,[301] SpyEye,[302] or a modified Trojan.[303] Bypassing security controls can also lead to unauthorized access. For instance, an inmate with rights to access certain websites circumvented the limits of the access he was granted by accessing personnel files, which contained Social Security numbers and other personal information.[304] System administration omissions or errors, such as not changing passwords to accounts known to former employees, can also lead to unauthorized access.[305] Internet Protocol ("IP") or Media Access Control ("MAC") spoofing[306] are other methods used by perpetrators to gain unauthorized access to computer systems.[307]

---

[298] *Id.* at 1059.

[299] *Id.*

[300] *See Terminology*, COMMON VULNERABILITIES AND EXPOSURES (Feb. 27, 2013, 12:00 AM), http://cve.mitre.org/about/terminology.html (A vulnerability is a coding error in software that allows a perpetrator to execute commands as a legitimate or authorized user, to access computer data contrary to the access restrictions in place, or to conduct a denial of service attack. Vulnerability exploitation, as numerous cases prove, is an important attack vector); *see* Paul N. Stockton & Michele Golabek-Goldman, *Curbing the Market for Cyber Weapons*, 32 YALE L. & POL'Y REV. 101 (forthcoming 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2364658 (Tens of new security vulnerabilities are reported each week. Of particular concern are the so-called "zero-day" (also referred to as Øday) vulnerabilities, not known to potential victims before an attack that exploits the vulnerability is carried out)). *See also* Taiwo A. Oriola, *Bugs for Sale: Legal and Ethical Proprieties of the Market in Software Vulnerabilities*, 28 J. MARSHALL J. COMPUTER & INFO. L. 451 (2011).

[301] *See* Warrant for Arrest, United States v. Nikhil Kolbekar, 12 MAG 1566 (S.D.N.Y. 2012), *available at* http://www.justice.gov/usao/nys/pressreleases/July12/cardshop/kolbekarnikhilcomplaw.pdf (last accessed Nov. 8, 2013).

[302] Indictment, United States v. Panin, No. 1:11-CR-0557-AT-AJB (N.D. Ga. June 26, 2013), *available at* http://krebsonsecurity.com/wp-content/uploads/2014/01/Panin-Indictment.pdf (last visited Feb. 23, 2014).

[303] Indictment, United States v. Ancheta, No. 05-1060 (C.D. Cal. 2005), *available at* http://www.justice.gov/usao/cac/Pressroom/pr2005/Botnet_Indictment.pdf.

[304] United States v. Janosko, 642 F.3d 40 (1st Cir. 2011).

[305] *See* United States v. Middleton, 231 F.3d 1207 (9th Cir. 2000).

[306] An IP address is a unique numeric address, used by computers to properly direct Internet traffic. A MAC address is a unique identifier assigned to a computer network interface or device. The forging of IP or MAC address, so that when a system that receives a data packet or communication

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

Computer data can have high value, impairments causing significant problems for victims. For instance, impairment of airline reservations,[308] sophisticated computer algorithms,[309] product processes, lists of customers, product research, or development data.[310] In certain situations, improper acts can lead to a cease in business operations,[311] shutting down computer-operated phone systems,[312] system freeze up[313] or system crash. System crash can be the result of brute-force attacks[314] or the use of a data-retrieving tool.[315]

Misconduct can result in severe operational impairment or high loss. In *United States v. Lloyd*, the perpetrator purged all design and production programs, crippling the victim's manufacturing capabilities and causing millions of dollars lost in sales and contracts.[316] In *United States v. Middleton*, the defendant deleted databases and the entire billing system.[317] In *United States v. Phillips*, the plaintiff claimed $122,000 to assess the damage and $60,000 to notify the victims.[318] In *T-Mobile USA, Inc. v. Terry*, the defendant gained access to T-Mobile's wireless network and fraudulently activated SIM cards.[319] The court in *T-Mobile USA, Inc. v. Terry* awarded damages in the amount of $349,481.64.[320] In *United States v.*

---

regards it as coming from somewhere else. *See* IP spoofing in Four Seasons Hotels & Resorts BV v. Consorcio Barr, S.A., 267 F. Supp. 2d 1268, 1298 (S.D. Fla. 2003).

[307] *See* the Indictment in United States v. Swartz, 1:11-cr-10260 (D. Mass. 2011), *available at* http://www.documentcloud.org/documents/217117-united-states-of-america-v-aaron-swartz (alleging the defendant spoofed the MAC address, in an attempt to evade the blocking of his MAC address).

[308] United States v. O'Brien, 435 F.3d 36, 37–38 (1st Cir. 2006).

[309] *See* Quantlab Technologies Ltd. (BVI) v. Godlevsky, 719 F. Supp. 2d 766, 770 (S.D. Tex. 2010).

[310] *See* Bro-Tech Corp. v. Thermax, Inc., 651 F. Supp. 2d 378, 296–97 (E.D. Pa. 2009).

[311] *See* Freedom Banc Mortgage Services v. O'Harra, No. 2:11-CV-1073, 2012 WL 3862209 (S.D. Ohio Sept. 5, 2012).

[312] *See* United States v. Trotter, 478 F.3d 918, 919 (8th Cir. 2007).

[313] Eyeblaster, Inc. v. Federal Ins. Co., 613 F.3d 797, 800 (8th Cir. 2010).

[314] A brute-force attack is considered to be an exhaustive attack, often automated, covering the entire keyspace, which aims to obtain users' passwords.

[315] *See* Snap-On Bus. Solutions Inc. v. O'Neil & Assocs., Inc., 708 F. Supp. 2d 669, 678–81 (N.D. Ohio 2010).

[316] United States v. Lloyd, 269 F.3d 228, 228 (3d Cir. 2001).

[317] *See* United States v. Middleton, 231 F.3d 1207, 1209 (9th Cir. 2000).

[318] United States v. Phillips, 477 F.3d 215, 218 (5th Cir. 2007).

[319] T-Mobile USA, Inc. v. Terry, 862 F. Supp. 2d 1121, 1135 (W.D. Wash. 2012).

[320] *Id.*

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

Dinh, the restoration of the affected system exceeded $200,000.[321] In *B&B Microscopes v. Armogida*, the defendant deleted and overwrote thousands of files from the laptop, including the only copy of an algorithm, which resulted in a loss of $1,400 related to costs incurred to assess the damage assessment and $10,000 related to lost revenue.[322] In *Multiven, Inc. v. Cisco Systems, Inc.*, the court accepted demonstrated costs of $75,000 for investigating break-ins into the network by a former employee.[323]

B. Profile of Perpetrators

This study's research revealed that perpetrators target a very wide range of victims—from small companies to important organizations, such as federal agencies,[324] Universities,[325] retail electric,[326] telecommunications,[327] or credit card companies,[328] and even celebrities such as Christina Aguilera or Scarlett Johansson.[329]

Perpetrators can have different goals, monetary or non-monetary. For instance, this study revealed that DDoS attacks are often carried out in response to public embarrassment,[330] for the purposes of damaging a former employer,[331] or to bring attention to political or social causes.[332] Revenge is often behind insider attacks, as some feel their employer has wronged them. As the facts in numerous

---

[321] United States v. Dinh, No. 09 Cr. 327-01, 2011 WL 1197666, at *4 (S.D.N.Y. Mar. 29, 2011).

[322] B & B Microscopes v. Armogida, 532 F. Supp. 2d 744, 758 (W.D. Pa. 2007).

[323] Multiven, Inc. v. Cisco Sys., Inc., 725 F. Supp. 2d 887 (N.D. Cal. 2010).

[324] *See* U.S. Attorney's Office, *Alleged Hacker Charged in Virginia with Breaching Multiple Government Agency Computers*, FBI (Oct. 28, 2013 12:00 AM), *available at* http://www.fbi.gov/washingtondc/press-releases/2013/alleged-hacker-charged-in-virginia-with-breaching-multiple-government-agency-computers.

[325] *See* United States v. Phillips, 477 F.3d 215, 217 (5th Cir. 2007).

[326] *See* United States v. Kim, 677 F. Supp. 2d 930, 942 (S.D. Tex. 2009).

[327] Tracfone Wireless, Inc. v. Cabrera, 883 F. Supp. 2d 1220, 1228–29 (S.D. Fla. 2012).

[328] *See* Indictment, United States v. Monsegur, *available at* http://www.justice.gov/usao/nys/pressreleases/March12/hackers/monsegurhectorxavierinformation.pdf (last visited Jan. 25, 2014).

[329] *See* Indictment, United States v. Chaney, CR 11 00958 (C.D. Cal. 2011), *available at* http://www.wired.com/images_blogs/threatlevel/2011/10/hackerazzi-Chaney-indictment.pdf.

[330] *See* United States v. Raisley, 466 F. App'x 125, 127 (3d Cir. 2012), *cert. denied*, 133 S. Ct. 216 (2012).

[331] *See* United States v. Schuster, 467 F.3d 614 (7th Cir. 2006).

[332] *See* United States v. Collins, No. 11-CR-00471-DLJ (PSG) (N.D. Cal. Mar. 15, 2013).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

cases prove, insider attacks are of a particular concern, due to perpetrators' increased motivation and specific knowledge of the system attacked.

This study identified a significant number of cases in which perpetrators were members of computer hacking groups, with the attacks being carried out as a form of hacktivism. For example, in Operation Payback, members of the group Anonymous protested the taking down of Pirate Bay, the website that facilitated peer-to-peer file sharing based on the BitTorrent protocol, accused of copyright infringements.[333] In the name of making all information free for all, Anonymous launched multi-day attacks against the websites of governmental bodies and other entities.[334] In another case, members of the Anonymous group again conducted the attack, this time in retribution for PayPal's termination of WikiLeaks.org's donation account.[335] Other cases involved the self-proclaimed leader of the hacking group Electronik Tribulation Army, a rival of the Anonymous group,[336] and members of the LulzSec and AntiSec groups, affiliated with the Anonymous group,[337] or the Deceptive Duo group.[338]

Cases involving members of the computer underground present organized crime and transborder aspects.[339] These cases also involve sophisticated methods by which perpetrators accomplish, conceal and launder proceeds and try to hide their misconduct. Such methods often include malware, wardriving, clickers,[340] or encryption. In a number of cases, perpetrators committed computer damage in connection with or in furtherance of other crimes, such as common-law fraud, federal trademark infringement, federal unfair competition and false advertising,

---

[333] *See, e.g.*, United States v. Dennis Owen Collins et al., No. l:13-cr-383 (E.D. Va. 2013).

[334] *Id.*

[335] *See* Indictment, United States v. Collins, No. l:13-cr-383 (E.D. Va. 2013), *available at* http://msnbcmedia.msn.com/i/MSNBC/Sections/NEWS/A_U.S.%20news/US-news-PDFs/anonymous-indictment.pdf.

[336] United States v. McGraw, No. 3:09-CR-0210-B, 2012 WL 6013528 (N.D. Tex. Nov. 30, 2012).

[337] United States v. Hammond, No. 12 Crim. 185 (LAP), 2013 WL 637007 (S.D.N.Y. Feb. 21, 2013).

[338] *See* U.S. DEPT. OF JUSTICE, *supra* note 288.

[339] *See* United States v. Gonzalez, 08 CR 10223 PBS, 2009 WL 1543798 (D. Mass. May 26, 2009).

[340] Malicious computer code or exploit that redirects the victim to an infected resource. *See* Indictment, United States v. Ancheta, No. 05-1060 (C.D. Cal. 2005), *available at* http://www.justice .gov/usao/cac/Pressroom/pr2005/Botnet_Indictment.pdf.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

wire fraud, aggravated identity theft, money laundering, access devise fraud or wiretapping.[341]

III. SUMMARY OF FINDINGS AND CONCLUSION

Considering the actual or potential financial, operational or reputational consequences or adverse effects of computer damage attacks, the phenomenon must receive appropriate attention from stakeholders. This article empirically categorized the essential aspects of computer damage cases, illustrating each aspect with the most significant issues, interpretations and arguments.

The CFAA is needed to ensure protection against computers attacks inflicting damage that traditional criminal statutes cannot properly address. Although the CFAA is a criminal statute, the majority of CFAA cases found were civil actions instituted against the perpetrators. There are a large variety of acts that inflict computer damage. The first form of computer damage involves knowing transmissions that cause intentional damage. This form can involve numerous techniques, such as the use of special erasure programs, malicious code or DDoS attacks. The other two forms of computer damage involve unauthorized access, resulting in damage or loss.

Weighing the courts' arguments illustrates that the prohibited conduct is imprecise, allowing for conflicting interpretations. While reasonable minds can disagree on these issues, the noted splits of authority creates problematic situations, as the outcome of litigation is unpredictable. Particularly open to conflicting interpretations is the access "without authorization" element, with some courts limiting the prohibited conduct to electronic trespassing, which excludes conduct by insiders. Of the three interpretations identified, none can be regarded as lacking merit or fully addressing the conduct. "Without authorization" does not refer only to the absence of any permission, but also acts as a *limit* or *scope* of authorization. The provision should therefore be understood or interpreted to mean that even in instances where the accessor is authorized to obtain or alter the same computer data for other purposes, such data should only be obtained or used when needed for legitimate operations and should not be deleted or altered in a malicious way.

Employers' right to employee loyalty cannot be discarded as irrelevant when examining damage claims. Nor can the terms of various agreements that are part of

[341] *See* United States v. Hammond, No. 12 Crim. 185 (LAP), 2013 WL 637007 (S.D.N.Y. Feb. 21, 2013); United States v. Christopher Chaney, CR 11 00958 (C.D. Cal. 2011); United States v. Gonzalez, 08 CR 10223 PBS, 2009 WL 1543798 (D. Mass. May 26, 2009); United States v. Yastremskiy, No. 08-CR-00160-SJF-AKT (E.D.N.Y. 2008).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

employment or pre-conditions for access to the system. Most often authorization is granted only after parties entered a contract or as a result or entitlement of being a party to a contract. If the contract is purposely breached, authorization can be construed as obtained fraudulently and thereby deemed implicitly revoked or void. As difficult as that may be to accomplish, the CFAA should attempt to leave as little interpretation as possible open to courts. Until this happens, the three interpretations will likely coexist.

Our research revealed that intent and motive vary significantly in these cases. Often the motivation behind these cases is revenge or retaliation. But such actions can also be a result of hacktivism, the furtherance of other offenses, usually to derive profit, or the attempt to cover, make untraceable or unrecoverable incriminating evidence of previously perpetrated crimes.

The study's examination revealed numerous types of damage claims, from deletion of data or diminished system performance to system crash or misappropriation of confidential information. Computer damage complaints need to provide factual content, or context from which the court can reasonably infer the violation of plaintiff's rights, avoiding any conjectural, implausible or speculative evidence. This article shows that because plaintiff's damage or loss elements are poorly understood or not convincingly pleaded, a high number of claims are dismissed by the courts, often because the required monetary threshold was not successfully met. Such high rates of dismissal suggest the need for a more careful consideration and presentation of facts before courts, as well as the need for clearer legal definitions for these terms.

Courts generally reject privacy invasion claims. Practices such as misappropriation of PII or online tracking without users' consent should not be condoned. However, to successfully bring a claim under this subcategory, there is a need to demonstrate cognoscible loss. This is often hard to prove, so the entitlement to relief in such cases is difficult to demonstrate. While entitlement to relief in such cases can be available, usually it is not the one provided for by the CFAA. Similarly, in cases of misappropriation or dissemination of trade secrets by insiders, the entitlement to relief should be brought under traditional crimes or under the Theft of Trade Secrets Act, 18 U.S.C. § 1832, not under the CFAA as computer damage.

Cases where no actual damage was inflicted and loss alone is alleged raise interesting questions. For example, cases in connection with break-ins that require investigation and remedial measures in order to secure the exposed system. Such cases need careful consideration whether the trespasser actually did render the computer system less secure, how serious is the danger posed by the intrusion and if the system owner should have had stronger or updated security measures in place. These situations also make the point of actually naming these offenses

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu

computer *interference*, instead of damage, as do, for instance, the Convention on Cybercrime or the UNODC study. Remedial measures should be considered loss, as the opposite approach could result in a higher number of intrusions. This aspect also raises the much discussed and delicate topic of vendor strict liability or negligence on software security losses, as well as the need to mandate federal or industry standards for more thorough testing and bug fixing for software makers and incentivize more security research.

This article evidenced the prevalence of attacks aiming to hindering data availability. However, it also presented a significant number of attacks where system resources were exhausted or data was corrupted. The article's findings reveal that computer damage attacks involve a variety of perpetration methods or tools, some very sophisticated, difficult to counter or even detect, and which pose serious challenges to the security of computer data or systems. Considering the high threat posed by malicious software and botnets, the production, possession, use or traffic of such programs, or creation and use of botnets, must be criminalized as very serious offenses.

As numerous cases demonstrate, former employees represent a very real threat to computer data and systems, often inflicting serious damage. This leads to the conclusion that there is a need for special attention and implementation of appropriate procedures for terminated or departing employees. Further, given the elevated risk presented by this category, higher levels of sentencing enhancement could also be considered in such cases.

This article extends the understanding of the computer damage phenomenon. The findings will improve the investigation, prosecution and litigation of such cases in courts, help organizations in their process of identification and mitigation of risks, and stimulate more research in this area. Finally, although this article focused exclusively on one jurisdiction, the findings can be of interest to a wider, global context.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.139 ● http://tlp.law.pitt.edu