Oklahoma Journal of Law and Technology

Volume 7 | Number 1

January 2011

Terms of Service and the Computer Fraud and Abuse Act: A Trap for the Unwary?

David A. Puckett

7 OKLA. J.L. & Tech. 53 (2011)
www.okjolt.org

TERMS OF SERVICE AND THE COMPUTER FRAUD AND ABUSE ACT: A TRAP FOR THE UNWARY?

I. *United States v. Lowson* and *Facebook v. Power Ventures*

Technological development poses a unique challenge to Congress. Regardless of how far-sighted Congress attempts to be in its legislation, the law of unintended consequences may manifest. Policy effects which are positive, for instance, can be accompanied by unexpected detriments due to ignorance, error, or contrary intermediate interests. When technological development proceeds at the pace that has characterized the development of computers in the past thirty years, these dangers are magnified even more. The Computer Fraud and Abuse Act (CFAA) presents an interesting case of unintended legislative consequences.[1] As a product of the computer systems of the 1980s, the CFAA has proceeded into the Web 2.0 age with comparatively few modifications. As might be expected from the pace of technological development in the interim, the interaction between the CFAA and computer systems has produced some possibly detrimental consequences.

Two cases have recently come before the courts that raise serious concerns about the future viability and desirability of the CFAA in the face of continuing technological development. The first of these cases, *United States v. Lowson*, was recently filed on the federal

[1] 18 U.S.C.A. § 1030 (West 2008).

criminal docket of the District of New Jersey.[2] In *Lowson*, the defendants were able to bypass a CAPTCHA[3] and were subsequently allowed to use an automated web browser to purchase a large number of event tickets from Ticketmaster's ticket sale website, an action in violation of Ticketmaster's terms of service agreement (TOS).[4] The defendants later resold these tickets at inflated prices, an action also in violation of Ticketmaster's TOS.[5] As a result of these acts, the federal prosecutor alleges twenty-three violations of the CFAA, in addition to other federal crimes.[6] If convicted,[7] the defendants in *Lowson* could face sentences upwards of five years in prison and sizable fines on each count.[8] All of this punishment could be inflicted even though Ticketmaster was unaffected by the mass purchases. The interface[9] accessed by the defendants was the same as that accessible to the general public, and the price the defendants paid for the tickets was the price at which the tickets were being sold to the public.[10] This begs the question of whether such violations of contract should have compulsory power.

The second case, *Facebook v. Power Ventures* from the Northern District of California, poses many of the same questions as *Lowson*, but from a civil, rather than criminal,

---

[2] United States v. Lowson, No. 10-114 (D.N.J. filed Feb. 23, 2010) (indictment).
[3] *Id.* at 9 (defining CAPTCHA as a "Completely Automated Public Turing test to tell Computers and Humans Apart").
[4] *Id.* at 9-12.
[5] *Id.* at 2.
[6] *See id.* at 49-54.
[7] As of Nov. 18, 2010, three of four defendants in *United States v. Lowson* have accepted plea deals. Two defendants, Kenneth Lowson and Kristofer Kirsch, pled guilty to a single count of conspiracy to commit wire fraud. The third defendant, Joel Stevenson, pled guilty to a misdemeanor charge under the CFAA. The remaining counts were dismissed and United States District Court Judge Hayden agreed to sentencing limits for the two felony charges. While the fourth defendant, Faisal Nahdi, has not accepted any plea deal, there may not be any final judgment on the merits of *Lowson* as Faisal Nahdi "remains at large." *See generally* David Voreacos, *Two 'Wiseguys' Plead Guilty to Hacking Computers in Ticket Scalping Case*, BLOOMBERG (Nov. 18, 2010), http://www.bloomberg.com/news/2010-11-18/-wiseguys-to-plead-guilty-to-ticket-scalping-charges-prosecutor-says.html.
[8] 18 U.S.C.A. § 1030(c) (West 2008).
[9] While the software on the defendant's computers was not the software expected by Ticketmaster, it interacted with Ticketmaster's website in the same way as the web browsers used by the general public. The defendants did not alter the functioning of Ticketmaster's website in any way.
[10] *See Lowson*, No. 10-114, at 1-10.

perspective.[11] Similar to *Lowson*, the defendants in *Power Ventures* engaged in acts which involved accessing a website through automated means.[12] Specifically, the defendants provided an online service through which social network content could be aggregated.[13] Users provided the defendants with their Facebook passwords, which allowed the defendants to download the user's content from Facebook and post it on Power Venture's website, alongside similar content from other social networks.[14] Facebook's TOS expressly prohibits such solicitation of passwords.[15] As in *Lowson*, the automated system used to access Facebook's website used the same interface as the general public.[16] The main difference between the cases is that the only compulsion sought in *Power Ventures* was injunctive relief.[17] While injunctive relief may be less objectionable than prison terms and fines, both cases pose the same question of whether criminal statutes should provide such contracts with teeth.

In order to fully comprehend this proposition, it is necessary to first understand the enforcement options which are available. Under the CFAA, access to federally protected computer systems beyond one's authorized level of access is a federal crime.[18] To meet the definition of a "federally protected computer system," a computer need only meet the CFAA requirement that the computer be used in interstate communication.[19] As a result, essentially any computer communicating over the Internet, manifestly all computers in the United States, would potentially fall within this category. Punishments of unauthorized access ranges from fines and

[11] Facebook, Inc. v. Power Ventures, Inc., No. 08-5780 (N.D.Cal. filed Dec. 30, 2008) (complaint).
[12] *See id.* at 9-10.
[13] *Id*.
[14] *Id.*
[15] *Id.* at 6-7.
[16] *Id.*
[17] *Id.* at 18.
[18] 18 U.S.C.A. § 1030(a) (West 2008).
[19] *Id.* § 1030(e)(2).

misdemeanor prison terms up to lifetime incarceration. The level of punishment imposed depends upon (1) the damage caused, (2) the circumstances of the unauthorized access, and (3) the type of computer system accessed.[20] In addition to criminal proceedings, the CFAA also allows for civil remedies if there are damages or losses exceeding $5000.[21] Nowhere in the CFAA is negligent or reckless access prohibited, only intentional or knowing access.[22] Overall, there are three requirements for a successful action under the CFAA. The offender must (1) intentionally or knowingly access (2) a federally protected computer (3) without authorization or beyond his or her limits of authorization.[23] Depending on the acts alleged, some form of loss may also be required.[24] In other words, the CFAA could potentially make any use of a website in a manner not strictly complying with the website's TOS a federal crime. The sizable range of provisions that could appear in a website's TOS lends itself to wide federal authority, which could subsequently harm many unwary users for actions that have no consequential social harm.

There is some precedent supporting the proposition that breach of a website TOS alone is sufficient to support a conviction under the CFAA.[25] Agreement with this precedent is by no means unanimous;[26] the issue of using the CFAA to enforce website TOS has not yet reached the United States Supreme Court. Presently, there lies a dispute as to when a TOS breach alone is sufficient grounds for a federal criminal action. Regardless of the opinions of the lower courts on the fitness of TOS to inform criminal law, congressional intent must govern the CFAA's final

[20] *See id.* § 1030(c).
[21] *Id.* § 1030(g).
[22] *See id.* § 1030.
[23] *Id.*
[24] *E.g., id.* § 1030(g).
[25] *E.g.*, America Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444 (E.D. Va. 1998); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000).
[26] *E.g.*, United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009) (holding that the use of a TOS agreement as the basis for a prosecution under the CFAA would render the CFAA unconstitutionally vague).

interpretation.[27] In addition, such an interpretation must simultaneously be consistent with the demands of the United States Constitution.[28] Four questions must therefore be answered in determining whether the holdings desired in *Lowson* and *Power Ventures* are indicative of the future of the CFAA. First, what federal actions under the CFAA are consistent with the intent of Congress? Second, are federal actions to enforce website TOS under the CFAA consistent with the requirements of due process? Regardless of the result, it must further be asked whether it is desirable to enforce website TOS with the CFAA. If not, what means might be employed to bring the law into accord with the public need?

This note analyzes the interaction between the CFAA, from its initial drafting in 1984 and its substantial amending in 1986 up to the present, and modern developments in Internet-based computer services. Specifically, this note highlights the risks posed by using the CFAA to enforce website TOS agreements without giving due consideration to the peculiarities of the TOS contract regime. Part II provides an overview of the origins of the CFAA in light of the computer security environment that existed in the 1980s and, more importantly, the security environment that exists today. Part III analyzes the congressional record to determine the actions Congress intended to criminalize with the CFAA. Part IV traces judicial expansions of the CFAA, which cover actions not originally conceived by Congress. Part V illustrates problems that could be created by applying the CFAA to violations of TOS agreements through examples taken from modern Internet services. Lastly, Part VI concludes this note with a presentation of possible solutions to the problems posed by the interaction of the CFAA and TOS agreements.

[27] United States v. Ron Pair Enters., Inc., 489 U.S. 235, 242 (1989).
[28] Marbury v. Madison, 5 U.S. (1 Cranch) 137, 137 (1803).

II. The Best of Intentions: The Origins of the CFAA

The Internet seemed a dangerous place in October of 1984. Criminals ran rampant in America's computer systems, stealing hundreds of millions of dollars every year, potentially irradiating cancer patients and absconding with information vital to national security.[29] The present looked grim and the future looked even grimmer. In retrospect, this sort of nightmare futurism appears slightly unrealistic. Losses due to computer security incidents show no sign of increasing exponentially with time.[30] On the contrary, per capita computer crime losses appear to have peaked in 2001, then significantly declined.[31] The contamination of the anticoagulant heparin[32] has injured far more people than any medical device security breach.[33] Moreover, the release of war logs by Wikileaks, the most prominent case of leaked national security information in recent memory, was attributable to a disgruntled employee, rather than computer intrusion.[34] These inaccuracies are only obvious through hindsight, however. At the time of the passage of the CFAA, the general public's use of computers was a new development. In light of this, Congress did have good reasons for enacting the CFAA.

---

[29] S. REP. NO. 99-432, at 2 (1986), *reprinted in* 1986 U.S.C.A.C.A.N. 2479, 2480 (citing Joseph Tompkins, *Report on Computer Crime*, 1984 A.B.A. SEC. CRIM. JUST., 16-44).

[30] *See* Robert Richardson, *2008 CSI Computer Crime and Security Survey*, COMPUTER SEC. INST., at 16, http://www.cse.msstate.edu/~cse6243/readings/CSIsurvey2008.pdf (last visited Jan. 20, 2011).

[31] *See id.*

[32] *See* Gardiner Harris, *Heparin Contamination May Have Been Deliberate, F.D.A. Says*, N.Y. TIMES (Apr. 30, 2008), http://www.nytimes.com/2008/04/30/health/policy/30heparin.html (explaining that heparin, a blood thinner used by many, may have been deliberately adulterated by an upstream supplier to save money, resulting in eighty-one deaths).

[33] *See generally* John Murray, *Testimony by John Murray for the Subcommittee on Privacy and Confidentiality*, NAT'L COMM. ON VITAL AND HEALTH STATISTICS (Nov. 19, 2004), http://www.ncvhs.hhs.gov/041119p1.htm (citing statement of John Murray Jr., software compliance expert for the United States FDA Center for Devices & Radiological Health).

[34] Steven Lee Myers, *Charges for Soldier Accused of Leak*, N.Y. TIMES (July 6, 2010), http://www.nytimes.com/2010/07/07/world/middleeast/07wikileaks.html (providing information that American soldier Bradley Manning, alleged source of the logs released on Wikileaks, "complained of personal discontent with the military and American foreign policies" to an online friend).

Congress was quite explicit that the wrong it was attempting to address through the passage of the CFAA was credit card fraud.[35] The House stated, "[O]ur society is increasingly becoming dependent on numerous credit cards and other plastic devices, all of which eventually involve use of computers and other electronic devices which also are subject to criminal attack."[36] Due to Congress' inability to predict the future course of technological development, the CFAA was laced with broad provisions dealing with access to information instead of narrower clauses focused on financial transactions.[37] History has shown Congress to be correct in its presumption of prognostic incompetence. In 1978, six years *prior* to the passage of the CFAA, approximately five thousand computers existed in the world.[38] By 1990, six years *after* the passage of the CFAA, twenty million personal computers were being sold every year.[39] The World Wide Web[40] was not in existence in 1984, nor was it even seriously contemplated for another five years.[41] In 2008, 71.6% of adult Americans adults had regular access to the World Wide Web.[42] Clearly the penetration of the computer into society has deepened significantly since Congress first considered the CFAA. Whether Congress' broadening of an anti-fraud statute into a general computer crime statute was necessary to deal with such an uncertain future, however, remains to be proven.

---

[35] H.R. REP. NO. 98-894, at 4 (1984), *reprinted in* 1984 U.S.C.A.C.A.N. 3689, 3689.
[36] *Id.*
[37] *See id.*
[38] *Id.*
[39] Jeremy Reimer, *Total Share: 30 Years of Personal Computer Market Share Figures*, ARS TECHNICA (Dec. 14, 2005), http://arstechnica.com/old/content/2005/12/total-share.ars/6.
[40] While the terms are often used interchangeably, the World Wide Web is distinct from the Internet. The term "Internet" refers to a collection of interconnected computer networks. The term "World Wide Web" refers to a system of interlinked hypertext documents hosted on computers connected to the Internet.
[41] Tim Berners-Lee, *Information Management: A Proposal*, WORLD WIDE WEB CONSORTIUM, http://www.w3.org/History/1989/proposal.html (last visited Mar. 7, 2011).
[42] *See Internet Access and Usage: 2008*, U.S. CENSUS BUREAU, http://www.census.gov/compendia/statab/2010/tables/10s1120.pdf (last visited Jan. 20, 2011).

III. Congressional Intent

The intent of Congress in its drafting of the CFAA in 1984, and its later revising of the CFAA in 1986, seems relatively clear. Congress explicitly did not intend for the CFAA to cover all possible computer misconduct.

> Throughout its consideration of computer crime, the Committee has been especially concerned about the appropriate scope of Federal jurisdiction in this area. It has been suggested that, because some States lack comprehensive computer crime statutes of their own, the Congress should enact as sweeping a Federal statute as possible so that no computer crime is potentially uncovered. The Committee rejects this approach and prefers instead to limit Federal jurisdiction over computer crime to those cases in which there is a *compelling Federal interest* …. [43]

A question is thus raised as to what behavior Congress considered to be a case of "compelling federal interest." The language of the CFAA, as well as the congressional record, shed light on this subject.

A clearer picture of the behavior Congress intended to address can be seen by analyzing the CFAA in its separate parts. The intent behind most of the provisions of the CFAA is evident from the plain language of the statute. Subsection (a)(1) of the CFAA, for instance, covers computers containing information protected against "disclosure for reasons of national defense, [] foreign relations, … [or] the Atomic Energy Act of 1954 …."[44] Clearly Congress intended to protect computers vital to national security. Subsections (a)(4), (a)(6), and (a)(7) are similarly straightforward. All three subsections apply explicitly and unequivocally to the use of a computer in furtherance of fraud or extortion.[45] Subsection (a)(3) of the CFAA is likewise explicit in its protection of federally owned computers, where intrusion would implicate national

[43] S. REP. NO. 99-432, at 3 (1986), *reprinted in* 1986 U.S.C.A.C.A.N. 2479, 2482 (emphasis added).
[44] 18 U.S.C.A. § 1030(a)(1) (West 1986) (current version at 18 U.S.C.A. § 1030(a)(1) (West 2008)).
[45] *See* 18 U.S.C.A. § 1030(a)(4) (West 1986) (current version at 18 U.S.C.A. § 1030(a)(4) (West 2008)); *see* 18 U.S.C.A. § 1030(a)(6) (West 1986) (current version at 18 U.S.C.A. § 1030(a)(6) (West 2008)); *see* 18 U.S.C.A. § 1030(a)(7) (West 1996) (current version at 18 U.S.C.A. § 1030(a)(7) (West 2008)).

security interests or the administration of justice.[46] If all of the provisions of the CFAA were as textually unambiguous as subsections (a)(1), (a)(3), (a)(4), (a)(6), and (a)(7), the risk of inconsistent judicial interpretations would be lessened. However, the plain meaning of the remaining provisions of the CFAA is not as clear, leaving room for disagreement.

Subsection (a)(2) of the CFAA appears, at first glance, to be broader than the rest of the CFAA. The plain words of subsection (a)(2) indicate a prohibition of all unauthorized access of any data held on any federal interest computer, all computers in interstate or international communication,[47] in addition to all data held on any computers owned by the federal government or financial institutions.[48] The congressional record, however, indicates that Congress did not intend subsection (a)(2) to be so broadly construed. The senate report on the amending of the CFAA reflects this conclusion, stating, "The premise of 18 U.S.C. 1030(a)(2) will remain the protection, for privacy reasons, of computerized credit records and computerized information relating to customers' relationships with financial institutions."[49] The general protections of subsection (a)(2), therefore, seem to be aimed entirely at countering financial fraud, Congress' stated purpose in enacting the CFAA.[50] Despite this clear evidence of congressional intent, a court could easily come to the conclusion that subsection (a)(2) of the CFAA covers virtually every incidence of computer misuse. All that would be required to reach such a conclusion is for the text of the statute to be considered alone, an entirely reasonable approach for a court to use.

Subsection (a)(5) of the CFAA seems similarly broad compared to subsection (a)(2). By its plain terms, subsection (a)(5) of the CFAA covers *any* actual damage and *any* federal interest

---

[46] *See* 18 U.S.C.A. § 1030(a)(3) (West 1986) (current version at 18 U.S.C.A. § 1030(a)(3) (West 2008)).
[47] 18 U.S.C.A. § 1030(a)(2) (West 1986) (current version at 18 U.S.C.A. § 1030(e)(2) (West 2008)).
[48] *Id*.
[49] S. REP. NO. 99-432, at 6 (1986), *reprinted in* 1986 U.S.C.A.C.A.N. 2479, 2484.
[50] H.R. REP. NO. 98-894, at 4 (1984), *reprinted in* 1984 U.S.C.A.C.A.N. 3689, 3689.

computer systems.[51] This subsection is better understood with reference to the punishment provisions in subsection (c) of the CFAA. In brief, felony punishments are available when damage is caused that impairs medical treatment, causes injury or death, creates a threat to public health or safety, harms the administration of justice or national security, or that meets certain scope requirements, namely damage to ten or more computers or damage in excess of $5,000.[52] The congressional record elaborates further on this subsection by noting that, "[T]his subsection will be aimed at 'outsiders,' i.e., those lacking authorization to access any Federal interest computer."[53] Thus, the congressional intent behind subsection (a)(5) seems to be the punishment of trespasses that would ordinarily be punishable under state law were it not for the involvement of computers and interstate communication. However, a literal reading of this statute could result in one reaching the conclusion that the CFAA covers a broader range of actions than the range intended by Congress. For example, the text of subsection (a)(5) fails to reference outsiders entirely.

Congress intended to do the following when it drafted the CFAA in 1984 and later amended it in 1986: (1) protect national security, (2) protect consumer financial data, (3) punish computerized fraud and extortion, and (4) punish computerized trespasses against persons and chattels.[54] None of the amendments to the CFAA subsequent to 1986, consisting largely of grammar and diction changes in addition to the provision of a civil cause of action under the CFAA, evidence any significant alterations to this congressional intent.[55] Imprecise language,

[51] 18 U.S.C.A. § 1030(a)(5) (West 1986) (current version at 18 U.S.C.A. § 1030(a)(5) (West 2008)).
[52] 18 U.S.C.A. § 1030(c) (West 1986) (current version at 18 U.S.C.A. § 1030(c) (West 2008)).
[53] S. REP. NO. 99-432, at 10 (1986), *reprinted in* 1986 U.S.C.A.C.A.N. 2479, 2488.
[54] *See* 18 U.S.C.A. § 1030 (West 1986).
[55] *See* 18 U.S.C.A. § 1030 (West 1988); *see* 18 U.S.C.A. § 1030 (West 1989); *see* 18 U.S.C.A. § 1030 (West 1990); *see* 18 U.S.C.A. § 1030 (West 1994); *see* 18 U.S.C.A. § 1030 (West 1996); *see* 18 U.S.C.A. § 1030 (West 2001); *see* 18 U.S.C.A. § 1030 (West 2002); *see* 18 U.S.C.A. § 1030 (West 2008).

however, has given the judiciary great leeway to expand the CFAA beyond what Congress intended in 1984 and 1986. As a result, the current version of the CFAA could potentially characterize a greater number of individuals as criminals than Congress desired when it enacted the CFAA.

IV. Judicial Expansion of the CFAA

It must be noted that the actions of the defendants in *Lowson* and *Power Ventures* do not closely coincide with those intended by Congress to be made criminal through the CFAA.[56] In *Lowson*, the defendants paid Ticketmaster's requested price for the tickets and in doing so neither physically harmed a computer system, nor injured an individual, and furthermore perused no private information.[57] In *Power Ventures,* the defendants had the content owner's permission to collect the data they aggregated and, as in *Lowson*, did no physical damage to any computer system, or injury to any individual.[58] In both cases, the computer systems allegedly misused were accessed in largely the same manner as was intended by the owners of the system.[59] Certainly, the TOS in both cases prohibited automated access, but neither the federal prosecutor in *Lowson*, nor the plaintiff in *Power Ventures* allege that this automated access caused any damage itself.[60] Instead, the alleged damage was caused by the breach of the TOS and the efforts to remedy this breach, as would be standard in any breach of contract case.[61] Despite this break with Congress, both *Lowson* and *Power Ventures* are set to be tried on the merits of their

[56] 18 U.S.C.A. § 1030 (West 2008).
[57] United States v. Lowson, No. 10-114, at 14-28 (D.N.J. filed Feb. 23, 2010) (indictment).
[58] *See* Facebook, Inc. v. Power Ventures, Inc., No. 08-5780, at 9 (N.D. Cal. filed Dec. 30, 2008) (complaint).
[59] *Id.* at 17-18; *Lowson*, No. 10-114, at 1-10.
[60] *Id.*
[61] *Id.*

CFAA claims.[62] The reason for this disconnect is not simply because more actions are being prosecuted as crimes under subsections (a)(2) or (a)(5) of the CFAA than Congress intended, though this expansion does play a prominent role.[63] Judicial interpretation of ambiguous terms also has some significance.[64] Specifically, judicial interpretation of the term "authorization" in the CFAA and a judicial focus on the plain language of the CFAA over Congressional intent have resulted in the door being opened for claims considerably broader than Congress may have intended.[65]

A. Judicial Interpretation of "Authorization" in the CFAA

By its terms, the CFAA only prohibits unauthorized access to computer systems or access that exceeds authorization.[66] Cases of unauthorized access do not generally present any linguistic problem for the courts.[67] If there is any modicum of authorization then, tautologically, either access is authorized or in excess of authorization. Therefore, cases where access exceeded authorization are the main interpretive problem before the courts. Congress attempted to aid in this endeavor by defining "exceeds authorized access" in 18 U.S.C. § 1030(e)(6).[68] Unfortunately, Congress did so with reference to the term "authorization," which they did not

[62] Facebook, Inc. v. Power Ventures, Inc., No. 08-5780, at 2 (N.D. Cal. filed July 20, 2010) (order denying defendant's motion for summary judgment); United States v. Lowson, No. 10-114 at 2 (D.N.J. filed Oct. 12, 2010) (order denying motion to dismiss).
[63] *See generally* United States v. Drew, 259 F.R.D. 449, 466 (C.D. Cal. 2009) (showing the prosecution theory based on TOS violation and 18 U.S.C.A. § 1030(a)(2)(c) was ultimately rejected at trial).
[64] *E.g.*, Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1123 (W.D. Wash. 2000).
[65] *Id.*
[66] 18 U.S.C.A. § 1030(a)(2) (West 2008).
[67] *See* United States v. Ron Pair Enters., Inc., 489 U.S. 235, 242 (1989) (standing for the premise that the plain meaning of a statute governs); 18 U.S.C.A. § 1030(a)(2) (West 2008) (defining the phrase "without authorization" having the plain meaning of a complete lack of authorization).
[68] 18 U.S.C.A. § 1030(e)(6) (West 2008) ("[T]he term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter").

also define.[69] As a result, some courts have substituted definitions of general use from other areas of law.

The case of *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.* presents one of the most influential instances of this type of interpretation in the area of federal actions under the CFAA. In *Shurgard*, an employee e-mailed files containing trade secrets to a future employer from a company computer.[70] At all relevant moments, the defendant was actually permitted to use the computer in question and access the files sent, but the court still found that the access was unauthorized.[71] The court made this finding by referring to section 112 of the Restatement (Second) of Agency,[72] which states, "Unless otherwise agreed, the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal."[73] In short, all the *Shurgard* interpretation of the CFAA requires to support a finding of access "in excess of authorization" is a violation of any condition of authorization.

Support for the precedent in *Shurgard* is by no means unanimous. The court in *International Ass'n of Machinists & Aerospace Workers v. Werner-Masuda*,[74] for instance, expressly rejected the reasoning in *Shurgard* altogether when applied to similar circumstances. In *Werner-Masuda*, an agent of the plaintiff forwarded confidential files to a competitor using a computer owned by the plaintiff.[75] Like in *Shurgard*, at all relevant points in time the defendant was expressly permitted to access the computer and the files he forwarded at the time of the

[69] *See id.* § 1030(e).
[70] Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1123 (W.D. Wash. 2000).
[71] *Id.* at 1123-25.
[72] *Id.* at 1125.
[73] RESTATEMENT (SECOND) OF AGENCY § 112 (1958).
[74] Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479 (D. Md. 2005).
[75] *Id*. at 483.

occurrence.[76] In both cases, the defendants were prohibited from disclosing confidential information through either a condition of the employment as in *Shurgard*, or an explicit registration agreement as found in *Werner-Masuda*.[77] However, the court in *Werner-Masuda* did not follow *Shurgard* and its use of the Restatement (Second) of Agency.[78] Instead, the court referred to the plain language of the CFAA and the legislative history of its drafting in arriving at a decision,

> Although Plaintiff may characterize it as so, the gravamen of its complaint is not so much that Werner-Masuda improperly accessed the information contained in VLodge, but rather what she did with the information once she obtained it. The SECA and the CFAA, however, do not prohibit the unauthorized disclosure or use of information, but rather unauthorized access. Nor do their terms proscribe authorized access for unauthorized or illegitimate purposes.[79]

Thus, under the reasoning in *Werner-Masuda*, when a person consents to the use of their computer system by another, they cannot later claim that such use was beyond authorization. Despite the differing lines of reasoning in *Shurgard* and *Werner-Masuda*, neither approach has been expressly overruled by a higher court.[80] Until such a ruling is made, both approaches must be considered relevant law. As a result, there is confusion as to which actions are criminally punishable versus adequately handled by mere termination of employment.

B. Judicial Focus on the Plain Language of the CFAA

While it is true that congressional intent must govern the judicial interpretation of statutes, it is also true that "[t]he plain meaning of legislation should be conclusive …."[81] In the case of subsection (a)(2) of the CFAA, the intent of Congress and the plain meaning of the

[76] *Id.* at 497.
[77] *Id.* at 483.
[78] *Id.* at 499.
[79] *Id.*
[80] *See generally* Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 964 (D. Ariz. Feb 20, 2008) (recognizing the disagreement between *Shurgard* and *Werner-Masuda*).
[81] United States v. Ron Pair Enters., Inc., 489 U.S. 235, 242 (1989).

statute appear to be in conflict. As a result, judicial interpretation of the CFAA has broadened this provision of the statute enough to render the rest of the statute surplus.[82] As previously mentioned, the congressional intent behind subsection (a)(2) of the CFAA was to protect financial privacy.[83] However, nowhere in the actual text of the CFAA is this restriction present.[84] As a result, courts have allowed for actions under the CFAA on nothing more than an allegation that some information was intentionally obtained from a protected computer without authorization.[85] As the court stated in *Shurgard:*

> Nowhere in [the] language of § 1030(a)(2)(C) is the scope limited to entities with broad privacy repercussions. The statute simply prohibits the obtaining of information from "*any* protected computer if the conduct involved an interstate or foreign communication." According to the statute, a protected computer is a computer used in interstate or foreign commerce. This language is unambiguous. There is no reasonable implication in any of these terms that suggests only the computers of certain industries are protected.[86]

As might be imagined, since manifestly all computer transactions involve the exchange of some information, this construction of the CFAA might allow for actions under the CFAA in virtually any circumstance of unauthorized access, rendering the rest of the statute altogether superfluous. There seems to be little disagreement on this interpretation of the language of the CFAA.[87] Thus, until Congress acts to properly implement its stated intent, the broad interpretation of the CFAA as articulated in *Shurgard* looks to hold the weight of precedent.

The question remains whether the *Shurgard* interpretation satisfies the requirements of due process. *United States v. Drew* may indicate that the precedent in *Shurgard* could result in subsection (a)(2) of the CFAA being unconstitutionally vague, at least in the context of non-

[82] *See* Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F.Supp.2d 1121, 1125 (W.D. Wash. 2000).
[83] S. REP. NO. 99-432, at 6 (1986), *reprinted in* 1986 U.S.C.A.C.A.N. 2479, 2484.
[84] 18 U.S.C.A. § 1030(a)(2) (West 2008).
[85] *Shurgard*, 119 F. Supp. 2d at 1125.
[86] *Id.*
[87] *E.g.*, Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 439 (2d Cir. 2004).

compliance with a TOS agreement.[88] Due process of law requires that criminal laws such as the CFAA establish minimum guidelines to govern law enforcement.[89] The court in *Drew* asserted that this due process requirement could not be met if every breach of any TOS provision could be criminally actionable under subsection (a)(2) of the CFAA.[90] To allow such unfettered federal action would be to grant prosecutors nearly unlimited discretion "to pursue their personal predilections."[91] Similarly, reference to the Supreme Court's decision in *Grayned v. City of Rockford* reveals further concerns presented by the use of TOS as the sole basis for federal criminal actions.[92] Such vague statutes are considered to offend the Constitution for the following reasons:

> First, because we assume that man is free to steer between lawful and unlawful conduct, we insist that laws give the person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may act accordingly …. Second, if arbitrary and discriminatory enforcement is to be prevented, laws must provide explicit standards for those who apply them …. Third, but related, where a vague statute "abut(s) upon sensitive areas of basic First Amendment freedoms," it "operates to inhibit the exercise of (those) freedoms."[93]

It seems likely that the use of TOS breaches as the sole basis for prosecutions under subsection (a)(2) of the CFAA would infringe upon all three of these principles. A few examples may serve to illustrate the problems inherent in conforming TOS agreements to the constitutional requirements of criminal law.

[88] United States v. Drew, 259 F.R.D. 449, 466 (C.D. Cal. 2009).
[89] Kolender v. Lawson, 461 U.S. 352, 358 (1983).
[90] *Drew*, 259 F.R.D. at 466.
[91] *Id.* at 467 (citing Kolender v. Lawson, 461 U.S. 352, 358 (1983)).
[92] *See generally* Grayned v. City of Rockford, 408 U.S. 104, 108-09 (1972) (reciting the reasons behind the prohibition of vague statutes).
[93] *Id.*

V. A Rogue's Gallery of TOS

Determining the authorized users of a computer system was a comparatively simple matter when the CFAA was originally drafted due to the relative dearth of public access to computer networks. The first online service, "The Source," debuted in 1978.[94] This service provided subscribers access to a small variety of news sources for between $7.75 and $44.75 an hour.[95] The Source was not intended to be accessible to the general public.[96] As of 1984, the service had only "60,000 subscribers."[97] Thus, determining whether a person was authorized to access such a computer system was as simple as checking whether a subscription had been obtained.[98]

The matter of unauthorized access has become more byzantine, and further from the state of affairs expected by Congress, with modern online services accessible to the general public over the Internet.[99] Practically all of these online services implement a TOS agreement,[100] many of the terms of which can be peculiar. [101] Contracts of adhesion and unusual contract provisions used together to create criminal standards present a number of practical and constitutional problems. Such problems can be divided into four general categories: wholly unexpected TOS, utterly vague TOS, spectacularly complex TOS, and TOS that abut First Amendment freedoms.

---

[94] *See* Doran Howitt, *The Source Keeps Trying*: *Does America Need an Information Utility?*, INFOWORLD, Nov. 5, 1984, at 60.
[95] *Id.* at 59.
[96] *Id.*
[97] *Id.* at 60.
[98] *See id.* at 61 (stating that The Source sells the availability of their computer service, not strictly usage).
[99] *E.g.*, Register.com, Inc. v. Verio, Inc., 356 F.3d 393 (2d Cir. 2004).
[100] A TOS agreement being a contract of adhesion that purports to divide the accessing public into the authorized user and unauthorized user categories envisioned in the CFAA.
[101] *See, e.g.*, United States v. Drew, 259 F.R.D. 449, 466 (C.D. Cal. 2009) (specifically dealing with the MySpace computer service).

A. Google Search and Unexpected TOS

Turning first to the matter of unexpected TOS, there is perhaps no better example to that of the TOS covering the use of the Google search engine. Before the actual content of Google's TOS can even be approached, the mere fact that Google has a TOS agreement may strike one as unexpected. The company's name is in common use as a generalized verb for Internet search tools.[102] The Google search box is integrated into a number of websites and web browsers.[103] In July 2009 alone, Google served 76.7 billion searches which is more than 28,000 searches every second.[104] It seems farcical that the general public would believe that each of those searches would bind a person to a contract. Google's homepage does nothing to alleviate this lack of awareness; nowhere on its homepage is a TOS agreement even mentioned.[105] One could certainly use Google to search for Google's TOS, but this solution seems to put the cart before the horse. In a situation such as this, where a public service is accessible with no apparent TOS, it seems unreasonable to believe that a lay person would be aware of the existence of a TOS agreement, let alone the conduct required by one.

Even upon reading Google's TOS, an individual might still be taken by surprise by a number of the terms. For example, children below the age of majority who search using Google could be deemed to have accessed a computer system without authorization since Google's TOS

---

[102] Frank Ahrens, *Use Google, But Please Don't "Google," Search Engine Says*, SEATTLE TIMES (Aug. 6, 2006), http://seattletimes.nwsource.com/html/businesstechnology/2003178630_google06.html (illustrating the prevalence of the use of the term "google" to describe an Internet search).

[103] *See, e.g.*, Noam Cohen, *Will Success, or All That Money From Google, Spoil Firefox?*, N.Y. TIMES (Nov. 12, 2007) http://www.nytimes.com/2007/11/12/technology/12link.html (stating that the makers of the Firefox web browser receive revenue from Google for including the Google search tool in their product).

[104] Andrew Lipsman, G*lobal Search Market Draws More than 100 Billion Searches Per Month*, COMSCORE (Aug. 31, 2009), http://www.comscore.com/Press_Events/Press_Releases/2009/8/Global_Search_Market_Draws_More_than_100_Billion_Searches_per_Month.

[105] *See Google Homepage*, GOOGLE, http://www.google.com/ (last visited Oct. 13, 2010).

specifically exclude minors.[106] Furthermore, a Google search is not authorized if the user later exercises their fair use rights[107] with respect to the information obtained in a search or searches for and uses information in the public domain:[108]

> You may not modify, rent, lease, loan, sell, distribute or create derivative works based on this Content ["Content" being previously defined as, "[A]ll information (such as data files, written text, computer software, music, audio files or other sounds, photographs, videos or other images) which you may have access to as part of, or through your use of, the Services...."] (either in whole or in part) unless you have been specifically told that you may do so by Google or by the owners of that Content, in a separate agreement.[109]

It is likely Google desires merely to protect its advertising content and avoid any copyright lawsuits based on contributory infringement through these contract terms.[110] The CFAA, however, contains no provision requiring the cooperation of the owner of a computer accessed without authorization.[111] All that subsection (a)(2)(C) of the CFAA requires to support a conviction is that a person, "[I]ntentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains … information from any protected computer …."[112] Taken together with Google's TOS, this subsection of the CFAA could conceivably snare practically every minor in the United States, and potentially many others, with few being the wiser. Given the great number of users who could potentially be prosecuted under the CFAA, it seems likely that any prosecutions that actually occur would essentially be arbitrary.

---

[106] *Google Terms of Service*, GOOGLE (Apr. 16, 2007), http://www.google.com/accounts/TOS.
[107] Using information from a Google search for the purposes of archiving, commentary, criticism, reporting, research, scholarship, or teaching, all such uses being excepted from copyright protection.
[108] *Id.*
[109] *Id.*
[110] *See* Perfect 10, Inc., v. Amazon.com, Inc., 508 F.3d 1146 (9th Cir. 2007) (showing that Google has been sued under precisely such a theory in the past, albeit unsuccessfully).
[111] *See* 18 U.S.C.A. § 1030 (West 2008).
[112] *Id.* § 1030(a)(2)(C).

B. YouTube and Vague TOS

Turning second to the matter of vague TOS, YouTube.com (YouTube) provides much by way of example. The chief source of problems is YouTube's community guidelines.[113] These guidelines are specifically incorporated into YouTube's TOS through subsection 6(E) of that document.[114] Among the various provisions of YouTube's community guidelines can be found the statement, "Don't post videos showing bad stuff …."[115] A list of content types that could be considered "bad stuff" is later provided, but this list is clearly intended to be exemplary, not exhaustive.[116] The uploading of anything from videos of underage drinking to videos of ninja training could conceivably be a prohibited and, therefore, unauthorized use of the YouTube service.[117]

With such general prohibitions, all violations are essentially discretionary. YouTube's community guidelines recognize the discretionary nature of violations in the form of an admonishment, indicating that the guidelines may not mean precisely what they say. The guidelines state, "Don't try to look for loopholes or try to lawyer your way around the guidelines—just understand them and try to respect the spirit in which they were created."[118] The determination of which videos violate the spirit of the guidelines is, of course, solely the province of the YouTube staff[119] or, potentially, a federal prosecutor in a case akin to *United States v. Drew*.

---

[113] *See YouTube Community Guidelines*, YOUTUBE (June 9, 2010), http://www.youtube.com/t/community_guidelines.
[114] *Terms of Service*, YOUTUBE (June 9, 2010), http://www.youtube.com/t/terms.
[115] *YouTube Community Guidelines*, *supra* note 113.
[116] *See id.*
[117] *See id.*
[118] *Id.*
[119] *See id.*

In a purely contractual matter, broad discretion might be wholly unproblematic. Parties are certainly free to agree to almost any contract terms they choose. Since YouTube's community guidelines are incorporated into the service's TOS, a failure to comply with the community guidelines would be an unauthorized use of a computer, and therefore a violation of the CFAA.[120] Thus, lawmaking authority would be effectively entrusted to the judgment of the YouTube content review staff and federal prosecutors, a state of affairs directly implicating the fundamental principles of the void for vagueness doctrine.[121]

C. GoDaddy Web Hosting and Complex TOS

Turning third to the matter of complex TOS, the TOS for the GoDaddy.com (GoDaddy) domain registration and web hosting service can serve to illustrate the problems of excessive complexity. GoDaddy's general TOS agreement reflects this notion. At sixteen pages of twelve point, single spaced text,[122] the GoDaddy TOS agreement is 60% longer than the terms one might come across when obtaining a credit card.[123] Problems begin to arise, however, in the initial paragraph. GoDaddy's TOS agreement expressly incorporates eleven other subsidiary agreements covering subjects like trademark infringement and civil subpoenas, and totals another forty-five pages of text.[124] Furthermore, the TOS agreement states that the terms are, "in addition to (not in lieu of) any specific terms and conditions that apply to the particular Services

---

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

[121] *See* Connally v. Gen. Const. Co., 269 U.S. 385, 391 (1926) (stating that statutes "must be sufficiently explicit to inform those who are subject to it what conduct on their part will render them liable to its penalties" if they are to be enforceable).

[122] *See Go Daddy Universal Terms of Service Agreement*, GODADDY (Jan. 20, 2011), http://www.godaddy.com/agreements/ShowDoc.aspx?pageid=UTOS.

[123] *See generally Wells Fargo Secured Card Terms and Conditions*, WELLS FARGO, https://www.wellsfargo.com/credit_cards/secured/terms (last visited Mar. 7, 2011).

[124] GODADDY, *supra* note 122.

you purchase or access through Go Daddy or this Site."[125] GoDaddy has certainly taken advantage of this particular contract provision. GoDaddy's legal agreements page lists another seventy-two agreements that a service user may have agreed to depending upon the particular services purchased.[126] These subsidiary agreements add an additional 349 pages of text to the TOS agreement, bringing the total length of the contract to 410 pages.[127] In light of this length, it seems preposterous for GoDaddy to assert, "Your electronic acceptance of this Agreement signifies that you have read, understand, acknowledge and agree to be bound by this Agreement …."[128] Frankly, it would be a surprise if the average GoDaddy user even read the sixteen pages of the universal TOS, let alone the remaining 96% of the legal agreement.

The problem of complexity is worsened by the virtually limitless range of provisions that could be contained in the TOS. As a result, users cannot honestly be considered informed of the rules that apply to them if these rules are not amenable to perusal. Considering the possible criminal sanctions that could attach to a violation of the TOS, assuming users are fully aware of the terms regardless of complexity, seems patently unreasonable.

D. Tripod Web Hosting and TOS that Abut Basic Constitutional Protections

Turning fourth to the matter of potential constitutional bars to using TOS as a basis of actions under the CFAA, the TOS agreement of the Tripod web hosting service from Lycos provides an example of a TOS agreement that abuts the First Amendment. The Tripod TOS agreement contains a list of thirty-seven categories of content which users are not authorized to

---

[125] *Id.*
[126] *Policies and Agreements*, GODADDY (Jan. 20, 2011), http://www.godaddy.com/Legal-Agreements.aspx?ci=20802.
[127] *Id.*
[128] *Go Daddy Universal Terms of Service Agreement*, *supra* note 122.

post using the service.[129] Only the first category needs to be read before a possible constitutional violation is presented.

> You agree that you will not use Lycos Network Products and Services to: Upload, post, e-mail, otherwise transmit, or post links to any Content, or select any member or user name or e-mail address, that is unlawful, harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, pornographic, libelous, invasive of privacy or publicity rights, hateful, or racially, sexually, ethnically or otherwise objectionable.[130]

The chief offending phrase in this contract provision is the prohibition on posting, or even emailing "content otherwise objectionable." Lycos is perfectly within its rights to contractually control the content posted using its service, just as a publishing house can choose the books it publishes.[131] A constitutional problem only becomes apparent when federal power backs this selection of content.

As stated by the Supreme Court, "[T]he First Amendment, subject only to narrow and well-understood exceptions, does not countenance governmental control over the content of messages expressed by private individuals."[132] Does this rule allow for the enforcement of a facially neutral federal law, the CFAA, when this enforcement would give effect to a contractual restriction on content? Moreover, is a TOS agreement that abuts constitutional protections compatible with the requirements of the void-for-vagueness doctrine? It would certainly seem that all of the principles underlying the void-for-vagueness doctrine would be implicated by a law incorporating the Tripod TOS.[133] After all, a prohibition on posting "content otherwise

---

[129] *Terms of Service*, LYCOS (Sept. 2, 2009), http://info.lycos.com/tos.php.
[130] *Id.*
[131] *See* Blue Cross & Blue Shield Mut. of Ohio v. Blue Cross & Blue Shield Ass'n, 110 F.3d 318, 333 (6th Cir. 1997) (stating that freedom of contract entails the freedom not to contract, except as restricted by law).
[132] Turner Broad. Sys., Inc., v. FCC, 512 U.S. 622, 641 (1994).
[133] *See* Grayned v. City of Rockford, 408 U.S. 104, 108-09 (1972).

objectionable" provides effectively no guidance to users, establishes no guidelines to govern enforcement, and would have a great chilling effect on speech.[134]

VI. Conclusion

As described previously, the current state of the CFAA with regard to TOS is disorderly. The CFAA fills a vital role in the federal statutory arsenal. Many types of conduct rightfully prohibited would be difficult to prosecute in the CFAA's absence. However, the presence of splits in authority and potential constitutional concerns, results in the CFAA doing a disservice to the public and the courts. The public is generally unmindful of what conduct will result in criminal charges, while the courts have to decide criminal cases with little guidance in circumstances in which civil breach of contract actions may be more appropriate.

A few possible solutions to these problems readily present themselves. The judiciary could simply be given time to produce a coherent body of precedent interpreting the CFAA and its relationship with TOS. No relevant cases have yet risen through the courts to the level at which a final decision of the issue might be obtained, but it seems as though it is only a matter of time before such a case appears. However, the judicial solution to the TOS problem facing the CFAA presents a number of shortfalls. First, there is no way of telling how long it will take for the judiciary to produce a coherent body of precedent on the subject. Approximately twenty-six years have elapsed since the CFAA first entered the books. It could be many more years before settled precedent is established. Second, there is no way of predicting the end result of this litigation. It is quite possible that the courts could arrive at a decision entirely in opposition to the expectations of the public in regard to the legal status of TOS agreements.

[134] *See id*.

In light of these shortfalls, it makes sense for a representative governmental body to resolve the problems facing the CFAA before giving such responsibility to the courts. The United States Congress is certainly in the best position to address the issue of TOS and the CFAA. By simply making its intentions explicit, Congress could resolve the entire problem in one act. If Congress had stated expressly, in 1986, that subsection (a)(2) of the CFAA protected only financial data, many of the problems which face the courts today would likely never have arisen. The same is true if Congress had expressly defined "authorization" in the text of the CFAA and made it clear that subsection (a)(5) of the CFAA applied only to damage caused by outsiders to the computer system. It is not too late for such changes to be made to the CFAA. Congress has regularly shown itself willing and able to amend the CFAA when the need arises. Nine amendments to the CFAA have already been made in only twenty-six years. One more carefully phrased amendment could resolve most, if not all, of the remaining ambiguities.

If Congress fails to remedy the problems of the CFAA, pressure may grow on state legislatures to bring the legal status of TOS more in line with public expectations. While the states cannot directly amend the CFAA, TOS are contracts and contracts generally must abide by the laws of the states in which they are drafted. Many states, such as California, have consumer protection law regimes that are both broad and deep.[135] It seems as though requirements that TOS be (1) prominently displayed, (2) affirmatively agreed to, and (3) reasonably intelligible would fit into these consumer protection regimes quite well, especially when the possible penalties under the CFAA associated with breaching TOS are considered. Such modifications to consumer protection law are not without penalty, though. After all, in the absence of a

[135] *Checklist of Significant California and Federal Consumer Laws*, CAL. DEP'T OF CONSUMER AFFAIRS, http://www.dca.ca.gov/publications/legal_guides/m-1.shtml (last visited Mar. 7, 2011).

consensus amongst the states, a state-by-state approach would only serve to increase the confusion as to what conduct is made criminal by the CFAA.