;login:

THE MAGAZINE OF USENIX & SAGE
June 2002 volume 27 • number 3

inside:

THE WORKPLACE

Evolving Behavioral Boundaries in Cyberspace

by Erin Kenneally

USENIX & SAGE
The Advanced Computing Systems Association &
The System Administrators Guild

evolving behavioral boundaries in cyberspace

Lowering the Barrier to Hacking Charges

by Erin Kenneally

Erin Kenneally is a Forensic Analyst with the Pacific Institute for Computer Security (PICS), San Diego Supercomputer Center. She is a licensed Attorney who holds Juris Doctorate and Master of Forensic Sciences degrees.

erin@sdsc.edu

The most widely known and applied federal law enacted to prevent abuse to computer systems is the Computer Fraud and Abuse Act (CFAA), referred to in legal source code as 18 U.S.C. § 1030. Although branded as the nation's primary anti-hacking law, the CFAA is quietly drawing the boundaries of acceptable behavior for IT professionals engaged in business activities. That is to say, the law is being applied to punish more than the hacker miscreants who break into machines and damage networks or steal intellectual property. The CFAA's prohibition on unauthorized access to computer systems is being interpreted by courts to govern the actions of Jane and Joe Employee – which hold nontrivial implications for computer security and infosec professionals.

This article examines trends in recent judicial applications of the CFAA as they may affect business cyber-risk exposure and remediation efforts. On a macro level, this analysis helps illustrate how the CFAA is shaping social expectations and notions of "reasonable" behavior in this neoteric cybersociety within which the legality of our actions are increasingly being judged.

Recent CFAA cases are both shaping and reflecting judgments of acceptable cyberbehavior. By ordering criminal penalties or civil relief for computer-related misbehavior, courts are transitioning standards of right and wrong behavior from the physical to the digital society. Whereas judges and juries can draw upon personal experiences when they adjudge the reasonableness of someone's actions – that it is unreasonably dangerous to drive drunk, for example – the context to make value determinations in the cyberworld is immature.

The CFAA has been applied relatively freely in recent cases, thereby expanding the scope of what constitutes criminal behavior as well as lowering the threshold of damages needed to raise a claim. Specifically, the elements of "exceed[ing] authorization" and "loss" have been interpreted rather broadly. Significant precedent was set by the US Court of Appeals in *EF Cultural v. Explorica* (9 I.L.R. (P&F) 3040 (1st Cir., 2001)), which agreed with the lower court that (1) the defendant's use of a scraper program to access information from EF's Web site could be construed as unauthorized access; and (2) money spent by the plaintiff-business to assess whether the software robot had caused damage to its systems was enough to satisfy the "loss" requirement under CFAA.

By What Standard Does Computer Access "Exceed Authorization"?

In a nutshell, the section of the CFAA used by *EF Cultural* prohibits the knowing access of a protected computer without authorization (or in excess of authorization) with the intent to defraud, and the value of the thing obtained must exceed $5,000 in

Realizing that IT professionals need to advance their knowledge in step with technology, it may be a challenge to sanitize the technical, business, or financial information that they take from job to job.

any one-year period. Whereas this is the black-and-white law, some actions may fall into a gray area where its illegality is questionable. Here the defense argued that its use of the robot software to parse through the data on EF's Web site and extract information did not violate the CFAA because it was not unauthorized.

This court defined the contours of unauthorized access by referencing the "reasonable expectations" standard to judge Explorica's "gray" actions. In other words, Explorica violated the CFAA when it used EF's Web site in a manner outside the "reasonable expectations" of both EF and its ordinary users. The court reasoned that because of a confidentiality agreement between the defendant-employee and EF Cultural (one of the defendant employees who helped design the scraper had formerly worked for EF), the defendant exceeded authorization by abusing proprietary information needed to create the scraper.

This carries significance to both the individual and the business enterprise in the face of current business climate – where non-competition and non-disclosure agreements are passed like currency, the IT workforce is increasingly job-mobile, and the web of outsourced partners and third-party affiliates are ever important. What's more, competition is forcing businesses to find new ways to extract value from data that openly resides throughout the Internet. Software technologies offer the capability to identify, collect, and contextualize this data more efficiently and at a competitive advantage.

Furthermore, realizing that IT professionals need to advance their knowledge in step with technology, it may be a challenge to sanitize the technical, business, or financial information that they take from job to job. Even assuming Pat Sysadmin can subjectively segregate this "proprietary" information, the slope is slippery, nonetheless. What is to prevent a Web-based company from alleging CFAA violations in light of the default rule that "conduct is without authorization if it is not in line with the reasonable expectations of the Web site owner and its users"? This may be an instance of the cart driving the horse, thereby enticing a competitively disadvantaged company to "rethink" how its reasonable expectations can lead to civil compensation under the CFAA.

This raises perhaps the most underestimated aspect of this case, which lies in the arguments that the court sidestepped. The travel codes and corresponding tour price data were all publicly accessible through normal browsing of the Web site. The court even admitted that the tour codes could be correlated to actual tours and cost data by manually searching and deciphering the URLs to extract pricing information. However, the scraper program automated this search to allow the pricing information to be extracted quickly, and this was then utilized by the defendant (a competitor of EF Cultural) to set competitive prices. The real question becomes: would the use of the scraper alone render access unauthorized under the CFAA?

Although the court found the access to be unauthorized based on the confidentiality agreement, the existence of Webreaper-like programs and Web-page monitoring agents that contextualize data and use it for various e-commerce applications ensures that the courts will have to face the aforementioned issue in the future.

Interestingly, the lower court in *EF Cultural* found that the scraper circumvented technical restraints in the Web site "by operating at a warp speed that the Web site was not normally intended to accommodate." So, despite the fact that this software did not use a back door to access information or crack into a password-protected area, the district court appeared willing to label the use of a program that captures and data mines disparate data as exceeding authorization. Indeed, this conjures serious issues for a technology-driven society where capabilities outpace intentions and automation is proliferating.

Another notable case illustrating actions "without authorization" has bearing on disloyal employees who access their employer's computers to communicate proprietary information. In *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.* (119 F. Supp. 2d 1121 (W.D. Wa. 2000)), an employee of Shurgard sent an email containing trade-secret information to the defendant-competitor. Relying on principles of agency law, the court found that the employee's authority ended when he started acting as an agent of the defendant. In other words, there was an implicit revocation of authority, regardless of whether the employer had knowledge of the improper communications. This was the hook that allowed his accessing the employer's computers to be criminalized under CFAA. In short, the employee effectively met with the same treatment as a random hacker who may have compromised the company's network. So, "transitioning" employees and their future employers should pay attention to how their access and use of proprietary data may create CFAA exposures.

U.S. v. Middleton . . . allowed damages based on salaries paid to, and hours worked by, in-house employees who repaired the damage done by an unauthorized intruder.

Defining "Loss" Absent Physical Damages

Recall that unauthorized access is actionable under the CFAA if damages are shown. "Damage" is defined as "any impairment to the integrity or availability of data, a program, a system, or information that . . . causes loss aggregating at least $5,000 in value during any one-year period to one or more individuals" (18 U.S.C. § 1030 (g)). Pretty cut-and-dried, right? Well, the gray area that *EF Cultural* addressed was the contours of "loss," which are not defined in the CFAA.

Whereas it would be rational to assume that EF Cultural was stymied on this element, the court rejected the defendant's argument that only the use of the scraper program qualified as damage. Instead, the cost of diagnostic measures to assess the damage of the scraper on EF's Web site satisfied the damage threshold.

This rationale was made on the shoulders of other cases that wrestled with damage disputes. For instance, Shurgard construed damages to result from impairment to the "integrity" of Shurgard's computers. This was the case when trade-secret data was merely copied and disseminated, adding that physical modification was not necessary for integrity to be called into question.

The other referenced case stated that Congress intended "loss" to cover remedial measures borne by victims that could not be considered direct damage by a computer hacker (*In re Doubleclick, Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 521 (S.D.N.Y. 2001)).

Another case that is influential in ascribing the contours of "damage" is *U.S. v. Middleton* (35 F. Supp. 2d 1189 (N.D. Ca. 1999)). It allowed damages based on salaries paid to, and hours worked by, in-house employees who repaired the damage done by an unauthorized intruder. "As we move into an increasingly electronic world," the *EF* court reasoned, "the instances of physical damage will likely be fewer while the value to the victim of what has been stolen and the victim's costs in shoring up its security features undoubtedly will loom ever-larger."

Although *EF Cultural* permits consultant fees, recovery costs, and remediation expenses to satisfy the meaning of "loss," other courts have concluded that lost business or goodwill, by itself, could not constitute loss (*Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238, 252 (S.D.N.Y. 2000)); and loss for purposes of calculating damages

The threshold to satisfy damage requirements has been lowered and liberalized.

means "irreparable damage" (*In re Intuit Privacy Litig.*, 138 F. Supp. 2d 1272, 1281 (C.D. Ca. 2001)).

Although these narrow rulings bolster the conclusion that courts are unlikely to allow claimants to throw in the kitchen sink, the threshold to satisfy damage requirements has been lowered and liberalized. In light of this, the legal system may find CFAA opening a floodgate of potential claims.

As with the unauthorized access arguments, the *EF Cultural* court also declined to consider whether the claimed expenses related to boosting Web server security could count toward the damage tally.

This is an issue, however, whose time is drawing near. Combining the ease with which a company can cry foul that its data integrity has been compromised, along with the plethora of security consultants hit by the economic downturn, the potential for abuse is almost as strong as the likelihood of gaining relief. It is not difficult to imagine instances where a shoddily secured e-business might invoke the CFAA for less than earnest purposes, and seek reimbursement for adding state-of-the-art security that puts it in a better position than before the intrusion.

In conclusion, whether IT professionals or businesses are at the giving or receiving end of a CFAA claim, they will do well to understand how courts are interpreting cyber-behavior under the umbrella of the CFAA. Another take-away lesson is that regardless of how broad or narrow courts may construe the CFAA, the ultimate success of a claim or a defense will hinge on the evidentiary proof of wrongdoing and damages. This is where courts will undoubtedly insist on the production of reliable electronic audit trails and logs that reconstruct cyber-behavior.