New York Law Journal

Intellectual Property

Reviewing the CFAA: Second Circuit Clarifies Claim Accrual, Limitation

Stephen M. Kramarsky, New York Law Journal

September 22, 2015

Locks, the saying goes, keep honest people honest. Good physical security will keep out the curious passer-by or casual miscreant, but no lock is perfect and the determined thief will always find a way in. In recent years, it has become obvious that the same is true of the Internet. As a practical matter, no connected computer system is impenetrable, and password surveys routinely show that most people don't even have decent locks on their doors. Yet individuals and businesses place vast amounts of crucial, sensitive information online, assuming that it will remain secure. And when the locks fail, they turn to the law.

There are, of course, a number of legal protections against the misappropriation and misuse of personal data, identity or intellectual property. They include federal and state statutes, as well as common law claims of misappropriation, unfair competition and breach of duty, to name a few. But the great majority of those protections focus on the information that's taken, not the act of taking it. In the electronic universe, the damage from an intrusion often includes not only the loss of data, but the costly disruption to the system itself. There is no physical analog to that harm. A burglary victim is concerned about the assets in the safe, not the damage to the safe itself. But online, the calculation may be different: The "safe" is often a computer system or network that is vital to the victim's personal or business livelihood. When dealing with computer intrusions, the law has to address that potential loss as well.

To address these unique concerns, Congress enacted the Computer Fraud and Abuse Act (CFAA), which criminalizes the unauthorized access to certain kinds of computer systems and also creates a private right of action to remedy damage caused by such access. But the CFAA is a complex statute, and its language is not a model of clarity. Practitioners and courts alike have consistently disagreed about the scope of conduct it addresses and the accrual of actions arising out of that conduct. A recent Second Circuit decision clarifying the latter issue offers an opportunity to examine the CFAA, its function and limitations, and its utility as a tool for protecting electronic assets.

Computer Fraud and Abuse Act

The CFAA traces its origins to the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984,[1] which was largely aimed at protecting government computers from the challenges posed by increased public and commercial access to the Internet. The 1984 legislation was enacted after it became apparent that the mail- and wire-fraud statutes, long on the books, were not always capable mechanisms for prosecuting computer-based crimes, which were of growing concern.[2] Through amendments over the years, the Act has been adapted and expanded in various ways, including by broadening the scope of covered computer systems. Initially, the Act provided only for criminal penalties, but in 1994 Congress amended it to add a private right of action for the first time.[3]

With the addition of §1030(g) (codified in Title 18 of the U.S. Code), the CFAA authorized civil remedies for certain CFAA violations: "Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief."[4] The CFAA thus creates a civil cause of action, and a path to federal court, for violations that meet the modest threshold of causing $5,000 in harm.[5] Violations themselves appear to be expansively defined and include, for example, "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] … information from any protected computer."[6] Any computer system "used in or affecting interstate or foreign commerce or communication"—which is to say any computer connected to the Internet—is protected by the Act.

The CFAA was thus born from a criminal law designed to combat what was traditionally described as "hacking," but it has since found much broader use in ordinary commercial litigation. It has even (in the words of one commentator) "found its way into the realm of employment law in the past decade as a means for employers to protect sensitive business resources from rogue employees."[7] This is hardly surprising: The language of the statute is broad, and the modern business environment invites these kinds of claims. Valuable business information and trade secrets, once stored in locked cabinets or files stamped "confidential" or "eyes only," now live on corporate networks that are often protected by only a password. These materials are emailed around the corporate network—and even beyond it—in the ordinary course of business, frequently with little regard for the company's paper policies. One click by a disgruntled employee and the information may find its way into the hands of a competitor. In such cases, employers have turned to the CFAA for a civil remedy against the employee for "exceeding authorized access"—or sometimes, even against the new employer.[8]

In light of the CFAA's broad language, these cases are not surprising. But that broad language has also created ambiguity, and practitioners have to be aware that statute's limits may not be clear on its face. Courts are split, for example, on what "exceeding authorization" actually means. A New York trial court recently dismissed an action against an employee brought under the CFAA, reminding plaintiff that, according to the First Department, "the CFAA does not encompass an alleged misappropriation of information from an employer's computer while the employee was working for the employer."[9] In other words, in the First Department, if an employee has authorized access to information and later decides to misuse that information, that does not, standing alone, state a claim under the CFAA—whatever other claim it may state. The First Department came to this conclusion in 2012, yet litigants continue to bring CFAA cases on those facts.

As the CFAA becomes a staple of commercial litigation, the federal courts have begun to weigh in with increasing frequency, supplying important guidance on the substantive and procedural contours of CFAA claims. One such decision came out earlier this summer from the Second Circuit.

'Sewell v. Bernardin'

In *Sewell v. Bernardin*, the Second Circuit addressed, for the first time, the critical issue of how actions accrue under the CFAA's two-year statute of limitation. In reversing the district court, the Circuit demonstrated that the CFAA's seemingly standard limitation period is not always obvious in application. Notably, what may appear to be one "hack" can give rise to numerous claims with very different accrual dates.

In *Sewell*, the plaintiff brought civil claims against her former boyfriend, Bernardin, under the CFAA and the Stored Communications Act (SCA).[10] Sewell alleged that, after she ended her nine-year relationship with Bernardin, he accessed her AOL and Facebook accounts from his computer, changed her passwords, accessed her electronic communications and personal information, and used the accounts to circulate emails and public messages containing malicious statements about her sex life. Sewell alleged (importantly) that she never knowingly shared her passwords with Bernardin or anyone else. She claimed that Bernardin had obtained her passwords at some point while in her home. He was thus not an authorized user.[11]

Sewell's claims relied on two particular dates. On Aug. 1, 2011, Sewell discovered that her AOL password had been changed, thus preventing her from accessing her account. On Feb. 24, 2012, she discovered that she was unable to log into her Facebook account. Shortly after each of theses instances, lurid sexual messages were posted to her inaccessible account.[12]

On May 15, 2013, Sewell filed a suit against Bernardin's wife and five "John Doe" defendants for claims based on allegations of accessing Sewell's accounts without permission. The suit was settled months later. Then, on Jan. 2, 2014, Sewell filed a similar action against Bernardin himself. Sewell sought a minimum of $350,000 in damages.[13]

Judge Arthur D. Spatt of the U.S. District Court for the Eastern District of New York dismissed Sewell's complaint for asserting time-barred CFAA and SCA claims.[14] On appeal, the Second Circuit reversed in part and remanded the action, recognizing that "the operation of the statutes of limitations applicable under the civil enforcement provisions" of the CFAA and SFA was "a matter of first impression in this Circuit."[15]

The CFAA requires that civil suits be filed "within 2 years of the date of the act complained of or the date of the discovery of the damage," with damage defined as "any impairment to the integrity or availability of data, a program, a system, or information."[16] The SCA provides a similar limitation period requiring that civil suits be filed within two years of "the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation."[17]

The Second Circuit held that Sewell's claims under both the CFAA and SCA were time barred with respect to her AOL accounts, because the claims "were premised on damage and unauthorized access … which she had or should have discovered some two and five months earlier." The CFAA claim accrued when Sewell learned that "the integrity of her account had been impaired"—i.e., when she could not log on to her AOL email account. And the SCA claim accrued when Sewell had a "reasonable opportunity to discover" that someone had "intentionally access[ed] [her AOL account] without authorization."[18] Both occurrences fell outside of the two-year statutes of limitations and were therefore barred.

But Sewell's Facebook claims fared better. Those claims accrued on Feb. 24, 2012, when Sewell found that she could no longer access her account because her password had been changed. Sewell's complaint alleged no facts "from which to infer that anyone gained unauthorized access to her Facebook account before then." Therefore, based on the facts in the complaint, there was not any "damage, for CFAA purposes, or violation, for SCA purposes, for Sewell to discover … before that date."[19]

The court explicitly held that Sewell's discovery several months earlier that her AOL account had been compromised did not commence the limitation periods of either the CFAA or SCA on her Facebook-based claims. For her CFAA claim in particular, the court held that when Sewell found out about her AOL account, she "discovered only that the integrity of her AOL account had been compromised of that time"—not that the integrity of her own physical computer had been compromised. Whereas the district court assumed "that a plaintiff is on notice of the possibility that all of her passwords for all of the Internet accounts she holds have been compromised because one password for one Internet account was compromised," the Second Circuit held that such an assumption was incorrect ("[a]t least on the facts as alleged by the plaintiff"), and the court took notice that often people use different passwords for different accounts (something not addressed by Sewell's complaint).[20] With her Facebook claims surviving, Sewell's case was remanded to the district court for further proceedings.

Conclusion

It is important to note that, although the Second Circuit eventually reversed it, the District Court in *Sewell* was not taking a particularly controversial position. Other courts have also held that once a plaintiff becomes aware of a data breach, the CFAA clock begins to run—and even if the plaintiff later uncovers more extensive damage, the limitation period is calculated from the date of the first discovery. That view of the law comports with the best practical advice in these situations: if you become aware that *one* of your accounts has been compromised it is a good idea to change *all* of your passwords. Doing so may well save substantial headaches, but the Second Circuit has now clarified that failure to do so does not necessarily extinguish a subsequent CFAA claim.

Endnotes:

1. Pub. L. No. 98-473, 98 Stat. 2190.

2. See generally Deborah F. Buckman, "Validity, Construction, and Application of Computer Fraud and Abuse Act (18 U.S.C.A. §1030)," 174 A.L.R. FED. 101 §2(a).

3. Pub. L. 103-322, 108 Stat. 2097-2099. See S. Rep. No. 104-357, §IV(1)(E); H.R. Conf. Rep. No. 103-711, §290001(d), 1994 U.S.C.C.A.N. 1839.

4. 18 U.S.C.A. §1030(g).

5. 18 U.S.C.A. §§1030(g) & (c)(4)(A)(i)(I).

6. 18 U.S.C.A. §1030(a)(2)(C).

7. Matthew Kapitanyan, "Beyond Wargames: How the Computer Fraud and Abuse Act Should Be Interpreted in the Employment Context," 7 I/S: J.L. & POL'Y FOR INFO. SOC'Y 405, 406 (2012) (citing cases).

8. See, e.g., *Shurgard Storage Centers v. Safeguard Self Storage*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

9. *Charles A. Barragato & Co. v. Wong*, No. 156158/2015, 2015 WL 4778349, *2 (Sup. Ct. N.Y. Cnty. Aug. 12, 2015) (citing *MSCI v. Jacob*, 96 A.D.3d 637 (1st Dep't 2012)).

10. 795 F.3d 337, 338 (2d Cir. 2015). See 18 U.S.C.A. §2701, et seq. (SCA).

11. Id. at 338-39.

12. Id. at 338-39.

13. Joint Appendix at A8, *Sewell v. Bernardin*, 795 F.3d 337 (2d Cir. 2015).

14. *Sewell*, 795 F.3d at 339.

15. Id. at 338.

16. 18 U.S.C.A. §§1030(g); (e)(8).

17. 18 U.S.C.A. §2707(f).

18. *Sewell*, 795 F.3d at 340-41.

19. Id.

20. Id. at 340-42.

Stephen M. Kramarsky, a member of Dewey Pegno & Kramarsky, focuses on complex commercial and intellectual property litigation. Joseph P. Mueller, an associate at the firm, provided substantial assistance with the preparation of this article.
