Bloomberg BNA

Electronic Commerce & Law Report™

Reproduced with permission from Electronic Commerce & Law Report, 18 ECLR 695, 04/10/2013. Copyright © 2013 by The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com

COMPUTER CRIME

A recently floated draft of proposed legislative changes to the Computer Fraud and Abuse Act reflects a desire to increase the penalties available for violations of the federal government's main anti-hacking statute. However, the draft bill fails to address issues that have split the federal circuits, unwisely lifts some CFAA violations from a misdemeanor to a felony, and fails to address growing calls to remove violations of terms of service agreements from the CFAA's reach. The author suggests that legislative revisions to the Economic Espionage Act or the enactment of a federal trade secrets law offer a better policy direction for Congress.

# Amending the Computer Fraud and Abuse Act

By Peter J. Toren

The calls for amending the Computer Fraud and Abuse Act (CFAA), which, in general, makes it illegal to gain access to a computer ''without authorization'' or ''in excess of authorization,'' have grown louder. Internet activists alarmed by the suicide of Aaron Swartz, who was facing a prison term for downloading research materials from an academic website, have argued that the CFAA must be amended so that individuals do not face prison for violating a company's terms of service (TOS). A growing number of commentators have also argued that the CFAA should be strengthened to reflect the increased threat of international computer hackers, especially from China. Finally, others have stressed that the CFAA should be amended to address a number issues that have divided courts over the interpretation of the CFAA.

*Peter J. Toren is a partner with Weisbrod Matteis & Copley PLLC in Washington D.C. Prior to entering private practice as a partner in the New York office of Sidley Austin, he was a federal prosecutor with the Computer Crime & Intellectual Property Section of the Justice Department where he handled a number of high profile investigations and prosecutions under the Computer Fraud and Abuse Act and the Economic Espionage Act. He is also the author of Intellectual Property & Computer Crimes (Law Journal Press).*

## Recent Proposals

In response, a number of bills have been introduced in Congress offering amendments to the CFAA. The question is whether Congress will amend the CFAA to address these legitimate concerns about the scope and breadth or whether it will simply strengthen the CFAA to appear tough on crime. Early returns are not encouraging. According to Rep. Jim Sensebrenner (R. Wis), the chairman of the Subcommittee on Crime Terrorism, Homeland Security and Investigations, which held a hearing on amending the CFAA, while it may be time for Congress to ''augment and improve'' the CFAA to address international criminal groups, he would be concerned with any proposal that would decriminalize computer abuse that is currently illegal.

Part of the problem with the CFAA is that it has been amended five times since being enacted in 1986 in response to changes in technology and Congressional perception of what constitutes a crime, without any apparent understanding of how the changes will impact the law as a whole. In the last 25 years, the CFAA has evolved from a statute narrowly targeted towards those who break into computer systems and steal valuable data or cause damage to those systems into a much

COPYRIGHT © 2013 BY THE BUREAU OF NATIONAL AFFAIRS, INC. ISSN 1098-5190

broader law that includes felony provisions for those who violate the terms of service agreements. These are the several pages of fine print included with almost all computer software and services that you are asked to agree by ''clicking here'' and almost nobody reads. Certainly very few Americans are aware that by violating such terms, they are possibly committing a felony.

The Department of Justice has repeatedly taken the position that a user's breach of a terms of service may be a federal crime. For example, in a highly-publicized cyberbullying case, *United States v. Drew*, a government prosecutor asserted that violating MySpace's terms of service is a federal felony.[1] However, as Judge Alex Kozinski of the Ninth Circuit has noted, ''Minds have wandered since the beginning of time and the computer gives employees new way to procrastinate, by g-chatting with friends, playing games, shopping or watching sports highlights. Such activities are routinely prohibited by many computer use policies, although employees are seldom disciplined for occasional use of work computers for personal purposes. Nevertheless, under the broad interpretation of the CFAA, such minor dalliances would become federal crimes.''

Responding to the suicide of Aaron Swartz, Rep. Zoe Lofgren (D-Calif.) circulated a draft bill that became known ''Aaron's Law'' which, among other things, would have excluded ''breaches of terms of service or user agreements as violations of the CFAA and wire fraud statute.'' Partly in response to industry opposition, the bill has not gained traction.

More recently, the House Judiciary Committee circulated a draft bill that would amend the CFAA in a number of important ways.[2] First, it would increase maximum statutory penalties under the CFAA and, in particular, would make any violation of § 1030(a)(2) a felony. This is the CFAA's broadest provision, which criminalizes ''exceed[ing] authorized access, and thereby obtain . . . information from any protected computer.'' At present, that subsection is a felony crime only where (1) ''the offense was committed for purposes of commercial advantage or private financial gain,'' (2) ''the offense was committed in furtherance of any criminal or tortuous act,'' or (3) ''the value of the information obtained exceeds $5,000.'' In all other situations, the subsection is treated as a misdemeanor.

Under the draft bill, § 1030(a)(2) would be rewritten and would be treated as a felony crime if the defendant ''exceed[ed] authorized access'' and obtained information and the offense: (1) ''involves information that exceeds $5,000 in value; (2) was committed for purposes of obtaining ''sensitive or non-public information of an entity or another individual,'' including ''medical records, wills, diaries, private correspondence . . . photographs of a sensitive and private nature, trade secrets, or sensitive or non-public commercial business information;'' (3) was committed in furtherance of any federal or state crime or; (4) involves information obtained from a computer used by or for a government entity.''

Second, it broadens the type of property subject to criminal or civil forfeiture.

Third, the draft bill would create a new section to punish those who attempt to cause damage or inflict damage on a computer that powers critical infrastructure, such as water supply systems or telecommunications networks. It would impose a maximum 30-year sentence and a person convicted of violating that section would be ineligible for probation. Fourth, the draft bill would require companies and other ''covered entities'' that acquire, store or use personal information to report a security breach to its customers within 14 days, with certain law enforcement or national security exceptions. Third parties and service providers would be also required to notify a covered entity about a breach, which would then be required to notify its customers.

The draft bill would also require a company to notify federal law enforcement within 72 hours of a ''major security breach,'' which is defined as a security breach in which it is ''reasonably believed'' that the ''means of identification'' of 10,000 or more individuals have been obtained. ''Means of identification'' is defined by reference to 18 U.S.C. § 1028, which defines the term, in general, as ''any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual.'' The section provides for a civil penalty of not more than $500,000 for a violation, and a maximum penalty of $1,000,000, where the violation is ''intentional.'' It also does not provide for a private cause of action and ''supersedes'' any state law.

## Problems With House Judiciary Draft

Many of the supporters of Aaron Swartz have been quick to criticize the draft bill noting among other things that, instead of decriminalizing Mr. Swartz' conduct, it would have increased the statutory maximum penalty he faced by three years. As discussed in more detail below, the increase in the statutory maximum penalties for existing felonies, however, should not be viewed as the biggest concern with the draft bill. The mainstream press loves to report that defendant X is facing 120 years in prison. While this may make a great headline for the press, it is not how sentences for federal crimes are determined.

While discretionary, defendants in the federal system, are generally sentenced pursuant to the Federal Sentencing Guidelines, which take into account a variety of factors relating to the defendant's crime, such as the financial gain to the defendant or economic loss to the victim, and defendant's criminal history. In practice, the actual sentence based on the Federal Sentencing Guidelines is almost always substantially less than the permitted statutory maximum.

In the case of the CFAA, there does not appear to be single case in which a judge sentenced the defendant to a current maximum statutory sentence and was constrained by the existing statutory maximum from sentencing the defendant to a longer prison term. Thus, Congress is either unaware that this has not been an issue or Congress is increasing the statutory maximum to simply send a message that it takes computer crime seriously. Accordingly, an increase in the statutory maximum with a single exception discussed below is not

[1] 259 F.R.D. 449 (C.D. Ca. 2009). The District Court acquitted the defendant of her misdemeanor conviction for violating 18 U.S.C. § 1030(a)(2). The court found that a conviction based only on defendant's intentional violation of the provisions of a website's terms of service would violate the void-for-vagueness doctrine since an individual would not be on notice that such a breach could be crime and normally breaches of contract are not the subject of criminal prosecution.

[2] It would also increase the statutory penalty under 18 U.S.C. § 1831 for economic espionage from a maximum of 15 years imprisonment to 20 years and would make 18 U.S.C. §§ 1029 and 1030 predicate acts for a RICO violation.

 COPYRIGHT © 2013 BY THE BUREAU OF NATIONAL AFFAIRS, INC.  ISSN 1098-5190

likely to have much of an impact, because the Guidelines determine the sentence and defendants are not maxing out even under the current regime.

The single exception, however, is potentially a big deal. By turning § 1030(a)(2) from a being charged as a felony crime under limited circumstances to being charged as a felony under all circumstances is likely to lead in an increase of the number of prosecutions brought under the CFAA. Government prosecutors are reluctant to charge misdemeanors for a variety of reasons, including the understanding that ''misdemeanors are not real crimes.'' By making conduct that previously only could be prosecuted as a misdemeanor crime into a felony crime, the draft bill would create a far greater incentive to charge a defendant with a ''garden variety'' CFAA crime. Again, Congress is considering amending the CFAA in the absence of any record that such a drastic step is necessary.

Another major problem with the draft bill is the description of what type of acts would constitute ''exceeding authorized access'' under § 1030(a)(2). First, it would criminalize obtaining information from a computer where the offense ''involves information that exceeds $5,000 in value.'' In contrast, under the current version of § 1030(a)(2), it is a felony to obtain information where ''the value of the information obtained exceeds $5,000.'' Whether the draft bill's use of ''involves'' instead of ''obtained'' was intentional or simply reflects sloppy drafting by Congress, it is likely to lead to problems since it is not clear what it means for an offense to ''involve'' a type of information. For example, does it include a situation where the information obtained is worth less than $5,000, but the information is related to information (''involves'') that is worth far more. Congress should clarify this ambiguity.

Second, the categories of listed information are incredibly broad and, according to Professor Orin Kerr, ''the language would make it a felony to lie about your age on an online dating profile if you intended to contact someone online and ask them personal questions. It would make a felony crime for anyone to violate the TOS on a government website. It would also make it a federal felony crime to violate TOS in the course of committing a very minor state misdemeanor.''[3]

Third, including ''trade secrets or non-public commercial business information'' in the definition of covered information is also questionable. Neither of these terms is defined in the draft bill, however, the term ''non-public commercial business information'' is far broader than the term ''trade secrets'' which is a well defined term under the Uniform Trade Secrets Act, among other places. Under the draft bill's language, the government would be able to charge a felony for obtaining ''non-public commercial business information'' even where the information did not rise to the level of a trade secret. This is a substantial change in the law that Congress should not make without a full consideration of the consequences. In addition, prosecutors could charge a felony for theft of trade secrets without having to prove intent to convert the trade secret as required by the Economic Espionage Act.

A related problem with the draft bill is that it does not limit the definition of the term ''exceed authorized access'' which is currently defined as ''to access a computer without 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.''[4] This term is used in sections of the CFAA other than § 1030(a)(2). The ambiguity of the definition has led to a Circuit split over what it means for an employee to access an employer's computer system in excess of authorization. The First,[5] Fifth,[6] Seventh,[7] and Eleventh Circuits[8] have concluded that when an employee or former employee accesses an employer's computer with the intent to misuse the information obtained as result of such access, then the access was in excess of authorization even if the employee had the right to access the information at the time. As noted by the Ninth Circuit, under this definition, the construction of the statute goes ''far beyond computer hacking to criminalize any unauthorized use of information obtained from a computer. This would make criminals of large groups of people who would have little reason to suspect they are committing a federal crime.''[9] In contrast, the Fourth[10] and Ninth[11] Circuits have concluded that the statute is violated only when initial access or access of certain information is not authorized in the first place and the statute was enacted to penalize unauthorized procurement or alteration of information rather than its misuse. Congress should act to settle this dispute.

## A Better Way Forward

The Computer Fraud and Abuse Act has been described by a well-known cyberlaw professor as the ''most outrageous criminal law you've never heard of'' in an article in The New Yorker entitled ''Fixing the Worst Law in Technology.''[12]

While this is probably hyperbole, especially given the competition, there is no question that the CFAA should be amended. Congress would be wise, however, to consider amending the draft bill as presently rewritten. In particular, Congress should listen to the supporters of Aaron Swartz that a violation of terms of service, without more, should not be a criminal violation. Congress should also reconsider whether making § 1030(a)(2) a felony crime is necessary. There is no evidence in the record supporting such a change.

Finally, if Congress is truly serious about expanding the protection of trade secrets, it would be wise to enact a civil counterpart to the Economic Espionage Act. Federal law provides for civil remedies for patents, trademarks and copyrights. Congress over the past 15 years has considered a number of bills to add trade secrets to this list, but they have never gotten out of committee. A

[3] http://www.volokh.com/2013/03/25/house-judiciary-committee-new-draft-bill-on-cybersecurity-is-mostly-dojs-proposed-language-from-2011/ (last visited April 4, 2013).

[4] 18 U.S.C. § 1030(e)(6).

[5] *EF Cultural Travel BV v. Explorica Inc.*, 274 F.3d 577 (1st Cir. 2001).

[6] *United States v. John*, 597 F.3d 263 (5th Cir. 2010).

[7] *International Airport Centers L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006).

[8] *United States v. Rodriquez*, 628 F.3d 1258 (11th Cir. 2010).

[9] *United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012).

[10] *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012).

[11] *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012).

[12] http://www.newyorker.com/online/blogs/newsdesk/2013/03/fixing-the-worst-law-in-technology-aaron-swartz-and-the-computer-fraud-and-abuse-act.html (last visited April 4, 2012).

civil counterpart to the Economic Espionage Act would not only offer greater protection to this increasingly important form of intellectual property, but civil litigants would no longer have to shoehorn their theft of trade secret cases into a claim under the CFAA in an attempt to get jurisdiction in federal court. The CFAA could then revert to its original intent as a law designed to criminalize computer intrusions and to protect critical infrastructure from computer attacks.

 COPYRIGHT © 2013 BY THE BUREAU OF NATIONAL AFFAIRS, INC. ECLR ISSN 1098-5190