CORPORATE COUNSEL
ALM Properties, Inc.
Page printed from: *Corporate Counsel*

Back to Article

Should Lying About Your Age Online Be a Federal Crime?

Peter J. Toren

Corporate Counsel

05-02-2013

The calls for amending the Computer Fraud and Abuse Act (CFAA) have grown louder. Internet activists alarmed by the January 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). Others have argued that the CFAA should be strengthened to reflect the increased threat of international computer hackers, especially from China. Finally, still others have stressed that the CFAA should be amended to address a number of issues that have divided courts over the interpretation of the CFAA.

In response, several bills have been introduced in Congress offering amendments to the CFAA. The question is whether Congress will use this opportunity to draft a law that attempts to reflect the interests of all U.S. citizens or simply increase the criminal penalties for violating the CFAA so as to appear tough on crime.

The early returns are not encouraging. According to Representative Jim Sensenbrenner (R-Wisconsin), the chairman of the House 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 about any proposal that would decriminalize computer abuse that is currently illegal.

The CFAA has been around for over 25 years and until fairly recently did not draw much attention, except from federal prosecutors, former federal prosecutors like me, computer hackers, and a relatively small cadre of Internet activists who were concerned about its impact on their right to use the Internet as they saw fit. Indeed, at the time the CFAA was originally enacted in 1986, it reflected the "Model T" computer and Internet era and was narrowly targeted toward those who break into computer systems and steal valuable data or cause damage to those systems.

Since then, however, reflecting the change in the use and importance of computers and the Internet, the CFAA has evolved into a much broader law that includes, among other things, 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 to by "clicking here"—and that almost nobody ever reads.)

Surely few Americans are aware that by violating such terms of use, they may become subject to a felony charge. The U.S. Department of Justice has repeatedly taken the position that a user's breach of a TOS agreement is a federal crime. For example, in a highly publicized cyberbullying case, *United States v. Drew*, the government asserted that violating MySpace's TOS is a federal felony. The judge properly dismissed the charges.

As Ninth Circuit Judge Alexander Kosinski has noted, under a broad interpretation of the CFAA as advanced by the government, an employee's use of his or her work computer "to procrastinate" by "G-chatting with friends, playing games, shopping, or watching sports highlights, in violation of their employers' terms of use, would become federal crimes." While most federal prosecutors want nothing to do with such minor crimes, computer users in the U.S. would probably sleep better if their chance of being charged with a federal crime did not depend on the whim of a government prosecutor.

Protecting critical infrastructure and U.S. companies from cyberattacks, and not turning many Americans into criminals for violating a TOS agreement, are not mutually exclusive. The current draft bill to amend the CFAA being circulated in the House

does include an amendment to the CFAA greatly increasing the penalties for using a computer to damage critical infrastructure, which is uncontroversial. But the bill's other provisions suggest that Congress is taking the easy way out by simply strengthening the provisions of the CFAA so as to appear tough on crime without there being any evidence that such changes are actually needed. Moreover, the bill does nothing to decriminalize a breach of a TOS agreement.

The draft bill increases the maximum statutory prison penalties under the CFAA. The media loves to report that a defendant, for example, is facing over 100 years in prison. However, these statements are based on statutory maximum penalties, and defendants in the federal system are actually sentenced pursuant to the Federal Sentencing Guidelines, which take into account a variety of factors relating to the crime, such as financial gain to the defendant or economic loss to the victim, and the defendant's criminal history. In practice, the actual sentence is almost always substantially less than the permitted statutory maximum. One study has suggested that federal sentences "max out" less than 3 percent of the time. In the case of the CFAA, there is not a single report of a federal judge being constrained by the current statutory maximum from sentencing a defendant to a longer prison term. Congress is considering, therefore, simply strengthening the maximum statutory prison penalties without a record that such changes are actually needed.

The draft bill would also turn the CFAA's broadest provision, which criminalizes "exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer" from a felony crime charge under limited circumstances to a felony crime charge under all circumstances. This is not an insubstantial change. Government prosecutors are loath to charge misdemeanors for a variety of reasons, including that "misdemeanors are not real crimes." By making conduct that previously could only be prosecuted as a misdemeanor crime into a felony crime, the draft bill would create a far greater incentive for the government to charge a defendant. Again, Congress is considering doing this in the absence of any record that such a drastic step is necessary.

Moreover, the draft bill does not adequately address the real concern that federal prosecutors can charge a CFAA violation based on simply breaching a TOS agreement. It proposes that an individual would violate the CFAA by "exceeding authorized access" to a computer and obtaining a specified type of "information." The problem is that the categories of information listed are incredibly broad and, according to George Washington University Law School 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."

The draft bill is not completely without redeeming value. Apart from creating a new section to punish those who cause damage on a computer that powers critical infrastructure, such as water supply systems or telecommunications networks, it would also require companies that acquire, store, or use personal information to report a security breach to its customers within a specified period of time. While the language and scope of this section certainly need to be revised, it is a long overdue step toward better protecting the interests of U.S. consumers.

Congress now has the opportunity to fix what has been described as "the worst law in technology"—which is saying a lot, given the competition. It can and hopefully will do a lot better than it does in the current version of the draft bill. There is a real need to better protect the critical infrastructure of the U.S. from cyberattacks. However, the rights of ordinary computer users do not have to be sacrificed. At a minimum, the amendment must make clear that simply violating a TOS agreement is not a federal crime.

Peter J. Toren is a partner with Weisbrod Matteis & Copley 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 and Intellectual Property Section of the U.S. Department of Justice, where he handled a number of high-profile investigations and prosecutions under the Computer Fraud and Abuse Act. He is also the author of Intellectual Property and Computer Crimes *(Law Journal Press).*