

Under Scrutiny:

SHB's Government Enforcement & Compliance Update

AUGUST 1, 2008



CRIMINAL EXPOSURE FOR COMPETITIVE INTELLIGENCE GATHERING ON THE INTERNET: LESSONS FROM THE FALLOUT OF THE MYSPACE SUICIDE CASE

No one would be surprised that it is a crime of computer fraud for a corporate employee to use the Internet to hack into the protected computers of the employer's competitors to gather competitive intelligence. Indeed, a company's general counsel was criminally charged for this very offense. See *U.S. v. Moen*, Information, (D. Minn. Jan. 22, 2004).

It would surprise most people, however, that the same criminal statute could apply to surfing for competitive intelligence on a competitor's public Web site. That possibility is underscored by a case that has nothing to do with competitive intelligence gathering—the indictment of a mother, Lori Drew, who, along with others, posed as a teenage boy on MySpace to torment a neighboring teenage girl, allegedly leading to the girl's tragic suicide. As a result of this case, companies may want to reexamine their policies on competitive intelligence gathering as well as the terms and conditions for use of their own public Web sites.

At the heart of the matter is the federal statute concerning computer fraud, 18 U.S.C. § 1030. Most of that statute involves hacking into computers of the government or financial institutions. But section 1030(a)(2)(C) applies more generally, making it a felony to “intentionally access a computer without authorization or exceeds authorized access, and thereby obtains ... (C) information from any protected computer if the conduct involved an interstate or foreign communication.”

In short, using an interstate or foreign communication to obtain information from a “protected computer” without authorization is illegal. Almost every Internet viewing involves an interstate communication, and a “protected computer” is defined as any computer “which is used in interstate or foreign commerce or communication.” 18 U.S.C. § 1030(e)(2)(B). Thus, section 1030(a)(2)(C) literally makes it a crime to use any computer to obtain information over the Internet where the user does not have authorization to obtain the information. Many of those who have read the federal computer fraud statute have argued that the statute cannot mean what it says. But the *Drew* indictment arising out of the MySpace suicide shows to the contrary.

GOVERNMENT ENFORCEMENT & COMPLIANCE

Our clients face unprecedented enforcement scrutiny and novel legal theories. Today, government enforcement actions can include civil as well as criminal investigations and litigation. They can involve a host of independent actors including federal and state prosecutors, regulators, whistleblowers and their counsel, and class-action attorneys. These cases must be defended under the watchful eye of investors and the public.

Our Government Enforcement & Compliance Practice consists of former prosecutors – including a former U.S. Attorney, former Justice Department officials and even former corporate executives – who counsel and defend companies, their executives and employees in the full range of criminal, civil and regulatory government enforcement actions at the state and federal level. We counsel clients on how to avoid enforcement scrutiny. When investigations do arise, however, we work with our clients to resolve it as efficiently, cost-effectively and quietly as possible.

Under Scrutiny:

SHB's Government Enforcement & Compliance Update

AUGUST 1, 2008 - PAGE 2

The facts of the *Drew* indictment are fairly straightforward. The defendant and her unnamed co-conspirators decided to play a prank on a neighborhood teenage girl. Posing as a teenage boy, they created a MySpace account and, communicating by instant messaging, commenced an Internet romance with the teenage girl. When they later broke off the romance, the girl committed suicide.

Drew was indicted for conspiracy to commit computer fraud—she allegedly conspired with others to obtain information (communications from the girl) on a protected computer without authorization in violation of Section 1030(a)(2)(C). Drew is alleged to have lacked authorization because the MySpace Web site terms and conditions of service prohibited use of the Web site by any one who failed to provide truthful registration information (the registrant was a fictitious teenage boy) or any one who sought to use the site to communicate with a minor (the deceased was a teenage girl). Moreover, the registration process required any prospective member to click a box indicating that the applicant had reviewed and agreed to accept the terms and conditions of service. *U.S. v. Drew*, Cr. 08-582- GW, Indictment (C.D. Cal. May 15, 2008).

A review of section 1030(a)(2)(C) and the *Drew* indictment might suggest that criminal liability is a strong possibility for anyone who obtains information from a Web site knowing that the terms and conditions of the Web site deny authorization for that use. But is there a possibility of liability for someone who intentionally surfs a Web site, not knowing that the use of the Web site is unauthorized? The statute clearly requires an intent to access a computer, but on the face of the statute it is unclear whether the intent requirement extends to authorization so that the prosecutor must prove that the defendant knew he or she did not have authorization to access the computer.

Fortunately, the legislative history answers this question: Congress believed the intent requirement was broad, requiring an intent to access in an unauthorized manner. See S. Rep. 432, 99th Cong, 2d Sess., at 5 (Sept. 3, 1986), *reprinted at* 1986 U.S. Code Cong. & Admin. News 2479, at 2483 (“intentional acts of unauthorized access—rather than mistaken, inadvertent, or careless ones—are precisely what the Committee intends to proscribe.”). The issue, then, is not as bad as first may appear. Liability requires some knowledge that access was unauthorized, and the *Drew* case should help define the intent requirement.

In a just-filed motion, Drew argues that the indictment never alleges that she actually knew the terms and conditions of the MySpace Web site. *U.S. v. Drew*, Cr. 08-582- GW, Motion to Dismiss the Indictment for Failure to State An Offense, (C.D. Cal. July 23, 2008). The motion argues that, because the key requirement of section 1030(a)(2)(C) is that the defendant obtains information from a computer knowing the access is unauthorized, the indictment must—but does not—allege that the defendant knew what the terms of the authorized access are.

Under Scrutiny:

SHB's Government Enforcement & Compliance Update

AUGUST 1, 2008 - PAGE 3

The government has not yet responded to this motion but the response is predictable: the indictment charges a conspiracy to violate section 1030(a)(2)(C), so it is only necessary to show that one of the conspirators knew of the MySpace terms and conditions of use, and the indictment makes that showing by alleging that, when registering for the fictitious account, an unnamed, perhaps unknown, conspirator clicked a box indicating review and acceptance of the terms and conditions.

The decision on this motion may provide important guidance on the intent issue in the conspiracy context—an issue that is likely to arise when a subordinate is directed to get information from a competitive Web site by a superior who happens to know that competitor access to the Web site is not authorized.

No matter how the motion is resolved, the *Drew* case highlights the danger of using the Internet to obtain information. Companies need to examine their policies on Internet usage and on competitive intelligence gathering to see if they adequately protect the company and its employees from criminal liability under section 1030(a)(2)(C). In doing so, they should consider several issues.

First, do the policies recognize that any Web site involving a click-through agreement to the terms and conditions of the Web site's use raises red flags that likely require attorney review before information is accessed on the Web site?

Second, do the policies address the situation where there is no click-through agreement, but the main page of the Web site states that obtaining any information from any subsequent pages of the Web site signifies acceptance to the terms and conditions of use?

Third, do the policies encourage the employee to study the terms of use of the Web site before gathering information from the Web site? On the one hand, since Congress wanted to protect the person who obtained information by an act of unauthorized access that was inadvertent or careless, there might be some protection in ignorance of those terms of use; on the other hand, given the possibility of co-conspirator liability for situations where the conspirator does not know the scope of authorization to use of the Web site, the best protection may be to instruct every employee to know the terms of use of any Web site before using it.

Drew is also relevant to other company policies. Although it seems most likely to apply to competitive intelligence gathering, it may implicate other areas as well. For example, given the possibility that a company's Web site could impose as a term of use that the site will not be used for the purpose of litigating with the company, it may be necessary to revise outside counsel guidelines to deal with use of the Internet to gather intelligence on litigation adversaries.

Companies may also need to review the terms and conditions of their own public Web sites. While an exhaustive list is beyond the scope of this Update, following are just a few issues companies may wish to address in reviewing the terms and conditions: Does the company want to limit the ability of competitors and litigation adversaries to access their Web site? Could a prospective

Under Scrutiny:

SHB's Government Enforcement & Compliance Update

AUGUST 1, 2008 - PAGE 4

antitrust plaintiff allege that the company's Web site was a conspiracy-facilitating device since the company could, but did not, restrict competitors from having access to its public Web site? Would restricting access to the company's Web site set off reciprocal restrictions by competitors, thereby depriving the company of crucial sources of information?

Drew underscores another important point. Because there is nothing inherently bad about competitive intelligence gathering over the Internet, one would expect prosecutors to exercise significant restraint when considering charging a section 1030(a)(2)(C) violation for getting information through unauthorized access. *Drew* does not undercut that expectation, but it does demonstrate that prosecutorial discretion is often exercised based on facts that are unrelated to the crime. The prosecutor did not indict Ms. *Drew* because she was a flagrant computer hacker, but because they believed her actions caused a teenage girl to commit suicide.

Companies must recognize that, unless they have implemented careful policies on Internet usage and intelligence gathering, they have a vulnerability to prosecutorial discretion. The prosecutor is unlikely to indict under section 1030(a)(2)(C) just because someone in the company improperly accessed a Web site; much more likely, the prosecutor will indict under section 1030(a)(2)(C) because the prosecutor is convinced the company has done something illegal in an entirely unrelated area. The company's Internet usage may tempt prosecutors to indict for computer fraud because they believe but cannot prove the company has committed some other wrong, and a review of its related policies and public Web site terms and conditions may minimize such risks.

Analysis prepared by SHB Partner [James Eiszner](#).

The choice of a lawyer is an important decision and should not be based solely upon advertisements.

For additional information on SHB's Government Enforcement & Compliance Practice, please contact

David Douglass
Washington, D.C.
(202) 783-8400
ddouglass@shb.com

Paul C. Harris, Sr.
Washington, D.C.
(202) 783-8400
pcharris@shb.com

Jim Hurd
Houston
(713) 546-5658
jhurd@shb.com

Mike Koon
Kansas City
(816) 559-2285
mkoon@shb.com

Carol Poindexter
Kansas City
(816) 559-2391
cpoindexter@shb.com

www.shb.com



OFFICE LOCATIONS

Geneva, Switzerland
011-41-22-787-2000

HOUSTON, TEXAS
(713) 227-8008

Irvine, California
(949) 475-1500

KANSAS CITY, MISSOURI
(816) 474-6550

London, United Kingdom
011-44-207-332-4500

Miami, Florida
(305) 358-5171

San Francisco, California
(415) 544-1900

Tampa, Florida
(813) 202-7100

WASHINGTON, D.C.
(202) 783-8400