

**UNDER SCRUTINY:
SHB's Government Enforcement
& Compliance Update**



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 them as efficiently, cost-effectively and quietly as possible.

**STATUTE CRIMINALIZING INTENTIONALLY
ACCESSING WEB SITE WITHOUT AUTHORIZATION
HELD TO BE UNCONSTITUTIONAL:
MYSPACE MOM IS ACQUITTED**

In a high-profile case, *United States v. Drew*, a federal district court recently dismissed the indictment of the “MySpace Mom” because the statute under which she had been convicted was unconstitutionally vague. So holding, the court provided some comfort to companies whose employees use the Internet to gather information for business purposes—but that comfort may be short-lived if the prosecution appeals the ruling.

Mom's Misuse of MySpace Makes for Misdemeanor Mayhem

The MySpace Mom case facts have been well-publicized. Lori Drew wanted to learn if one of her teenage daughter's classmates was speaking ill of Drew's daughter. Drew, her daughter and a friend were alleged to have conspired to create a fictitious profile for a teenage boy on MySpace—an act that was contrary to the MySpace terms and conditions—and to use the fictitious character to flirt with the classmate. Through MySpace, they conducted a fictitious romance with the classmate, then abruptly terminated that romance, purportedly causing the classmate to take her own life.

Drew was indicted for conspiracy, as well as felony and misdemeanor violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030). At trial, the jury found for Drew on the conspiracy and felony Computer Fraud and Abuse Act charges, but convicted her of the misdemeanor statutory count. Specifically, she was convicted of violating 18 U.S.C. § 1030(a)(2)(C), which makes it a misdemeanor (albeit one with a jail term of up to one year) to intentionally access a computer involved in interstate communication without authorization or in excess of authorization.

Following her conviction, Drew filed a motion under Fed. R. Crim. P. 29(c) challenging her conviction and seeking entry of a judgment of acquittal. As the district court framed the issue, the question presented by Drew's motion was “whether an intentional breach of an Internet website's terms of service, without more, is sufficient to constitute a misdemeanor violation of” the Computer Fraud and Abuse Act, and

UNDER SCRUTINY: SHB's Government Enforcement & Compliance Update

SEPTEMBER 14, 2009

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

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



For additional information on this topic,
please contact

Jim Eiszner
Kansas City
(816) 559-2140
jeiszner@shb.com



"if so, would the statute, as so interpreted, survive constitutional challenges on the grounds of vagueness and related doctrines." *United States v. Drew*, No. CR 08-0582-GW, slip op. at 2 (C.D. Cal. Aug. 28, 2009).

Liability Implications for a Plain-Meaning Reading of the Statute

Construing 18 U.S.C. § 1030(a)(2)(C), Judge George Wu of the U.S. District Court for the Central District of California meticulously evaluated the case law, legislative history and statutory language and determined that no construction was possible other than the statute's plain meaning: section 1030(a)(2)(C) condemns intentionally accessing a Web site and reading the content posted when the reader did not have authorization to use the Web site. In other words, so long as the Web surfer had not accessed the Web site by mistake and was aware that the Web site use was contrary to the Web site's terms and conditions of use, the reading of any content on the site is a violation.

The liability consequences of this construction are enormous. It criminalizes the reading of a Web site where the reader knows he or she lacks authorization to use the site. This has implications for every Internet surfer and for companies whose employees use the Internet in furtherance of company business. To protect against liability from this statutory reading, many companies have developed Internet usage policies that require employees to review and ensure compliance with the terms and conditions of every Web site they visit on company business.

The district court was acutely aware that its statutory interpretation had serious implications for Internet use. It considered these implications in connection with Drew's challenge to section 1030(a)(2)(C) as a due process violation. As the court explained, due process requires that criminal statutes give citizens fair warning of the conduct that is illegal. Under the fair warning doctrine, a criminal statute will be void if it does not clearly delineate what conduct is prohibited and thus protect citizens from arbitrary law enforcement.

Vagueness Analysis of the Statute's Plain Meaning

Applying the void-for-vagueness analysis, the court seized on five issues:

- First, no ordinary citizen would expect criminal liability to arise from unauthorized use of a Web site merely because of a lack of authorization, as opposed to unauthorized use of the Web site which resulted in monetary (or other) harm.
- Second, by criminalizing every unauthorized use of a Web site, the statute gave unrestrained power to law enforcement.
- Third, because the conduct's criminality depended on a Web site's terms and conditions, if there were any guidelines for law enforcement, those guidelines were established by private parties—the Web site owners—who could unilaterally change the sites' terms and conditions and establish terms and conditions that were unclear.

**UNDER SCRUTINY:
SHB's Government Enforcement
& Compliance Update**

SEPTEMBER 14, 2009

- Fourth, criminal enforcement could become dependent on private contract remedies—the terms and conditions for MySpace, for example, provided that any disputes over its terms and conditions needed to be resolved by arbitration—so that citizens might not know whether criminal liability could attach before the contract issues were resolved.
- Lastly, the absence of law enforcement guidelines was highlighted by the facts of Drew's case: she was indicted under section 1030(a)(2)(C) for unauthorized access, but she was prosecuted because of the *consequences* of her access—the suicide of the teenage classmate.

Accordingly, the district court concluded that section 1030(a)(2)(C) was unconstitutionally vague and dismissed Drew's indictment. There is a significant risk, however, that the decision may be appealed and perhaps reversed (the district court's interpretation of the statute's plain meaning conflicts with its conclusion that the statute is so vague as not to give fair notice to ordinary citizens).

What Next for the Computer Fraud and Abuse Act?

If the decision stands and the statute is deemed unconstitutional, there are several consequences. First, companies will want to reassess their policies on business use of the Internet. Second, because section 1030(a)(2)(C) will be unconstitutional, businesses may want to lobby Congress for a new statute: while limiting section 1030(a)(2)(C) so that it does not criminalize use of a Web site in contravention of the Web site's terms and conditions may make good policy sense, section 1030(a)(2)(C) also criminalized unauthorized use of a password-protected Web site by hacking through the password protection, conduct that *should* be prohibited.

On the other hand, if the decision is reversed, companies will need to be aggressive in ensuring that their employees use Web sites for business purposes only when their use is consistent with the Web sites' terms and conditions. And those companies that have not already done so may find it prudent to reevaluate, and possibly revise, their employee Internet usage policies. ■

Analysis provided by Jim Eiszner.