Online Social Networks and Cyber Risk

--by: Robert T. Horst and John F. Mullen, Nelson, Levine, de Luca and Horst

As anyone with teenage children will confirm, social networking websites continue to be one of the fastest-growing e the cyberworld. During 2009, 50 million users of the micro-blogging service Twitter posted 8 billion "tweets."[1] Faceb approximately 350 million active users, 50% of which log onto the website in any given day.[2]

Given the vast amount of active and potential users, social networking websites present a tempting forum for unethi conduct. For example, in two recent high-profile trials, jurors were found to have posted ongoing comments about th cases on websites such as Facebook and Twitter, leading to calls for a mistrial (which, in both cases, were denied).[3] an appellate court reversed a burglary conviction after it was learned that a juror posted detailed accounts of deliber blog, in addition to bragging about his failure to disclose his background as a licensed attorney during jury selection.[4]

However, the potential misuse of social networking websites can endanger far more than the integrity of the judicial These websites have proven to be valuable tools for acquiring sensitive personal information for use in identity theft unlawful schemes. This article addresses how these schemes operate and analyzes whether, and to what extent, suc may expose social networking websites and their liability insurers to liability.

I. Malware

The majority of unlawful attempts to procure confidential information from social networking websites are bas upon convincing unsuspecting individuals to visit websites or download files that install "malware" on the indiv computer that provide criminals with access to data stored on the individual's computer — or, in some cases, allow the criminals to actually operate the individual's computer from a remote location.

While social networking websites are primarily intended as a forum for original content posted by individual us an increasing percentage of blog postings are devoted to links to other websites — including websites containi malware. By providing tools to shorten web addresses so as to fit into the space limitations of postings, Twitte proven to be a particularly attractive method of encouraging users to click on hyperlinks to websites without revealing web addresses that could arouse suspicion in savvy users.[5] According to a recent study by Kaspersk Labs, approximately 26% of Twitter postings contain links to websites, with 1 in every 500 of these links leadi websites hosting malware.[6]

Even the seemingly secure Facebook website has not been immune to malware attacks. Initially, malware wa spread to Facebook users through E-mail "worms" that spread by obtaining control of victims' Facebook accou the purpose of forwarding the worms to the users' designated "friends."[7] Of course, the fact that these messa were apparently sent by "friends" on a supposedly secure website provided additional encouragement for Face users to open the messages.[8] Attempts to spread malware through Facebook have recently become more sophisticated, including the creation of accounts supposedly held by non-existent individuals for the purpose o distributing "worms."[9]

II. "Phishing"

In addition, social networking websites such as Facebook have been subject to so-called "phishing" attacks, in individuals receive E-mails directing them to websites that have been designed to resemble websites that the individuals frequently visit to input personal information (such as websites for financial institutions with which individuals regularly do business). Of course, the goal of these schemes is to encourage individuals to input th personal information into these phony websites, which can then be used for unlawful means. In the case of so networking websites, "phishing" attacks typically take the form of E-mails directing website users to a page de to resemble the website's log-in page, thereby enabling the so-called "phisher" to acquire individual password The passwords are then utilized to visit individuals' pages on the website for the purpose of acquiring personal information.[11] In addition, as many individuals use the same passwords for other password-protected website "phishers" may obtain unauthorized access to websites containing these individuals' financial information and sensitive data.[12]

III. Potential Exposure

A. Communications Decency Act

All of these efforts may raise the specter of litigation against social networking websites based upon the

contention that these websites have failed to adequately protect its members against such attacks. However, such lawsuits may be difficult to maintain in light of the federal Communication Decency Act,[13] which establishes that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[14] The term "information content provider" is defined as "any person or entity that is responsible, in whole or in part, for the creation and development of information provided through the Internet or any other interactive computer service."[15] The Act further provides that "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."[16]

Taken together, these provisions have been uniformly interpreted to preclude "state-law plaintiffs from holding interactive computer service providers legally responsible for information created and developed by third parties."[17] Courts have applied the Communications Decency Act to shield social networking websites from lawsuits based upon the contention that a website failed to implement adequate security procedures to protect members from harm. For example, in *Doe v. MySpace, Inc.*,[18] the United States Court of Appeals for the Fifth Circuit held that the Communications Decency Act precluded parents from suing the popular social networking website MySpace after their daughter was sexually assaulted by an individual she met through the service. In arguing that the protections of the Communications Decency Act should not apply to their claims, the plaintiffs in *Doe* contended that they were not seeking to impose liability upon MySpace for publishing the messages from the sexual predator, but for the website's "failure to implement basic safety procedures to protect minors."[19] The Court rejected this argument, noting the trial court's observation that "'[i]f MySpace had not published communications between [the victim and attacker], including personal contact information, Plaintiffs assert they never would have met and the sexual assault never would have occurred.'"[20] Accordingly, the Fifth Circuit concluded that the plaintiffs' allegations were "merely another way of claiming that MySpace was liable for publishing the communications and they speak to MySpace's role as a publisher of online third-party generated content."[21]

The Fifth Circuit's decision in *Doe* followed a similar holding reached by the United States Court of Appeals for the Third Circuit in *Green v. America Online (AOL)*,[22] in which a member of the popular service provider sued AOL for failing to prevent a fellow user from allegedly posting derogatory comments about the member in chat rooms, and from purportedly sending the plaintiff a "signal" through the service that damaged his computer. The Court held that by claiming that "AOL was negligent in promulgating harmful content and in failing to address certain harmful content on its network," the plaintiff sought to "hold AOL liable for decisions relating to the monitoring, screening, and deletion of content from its network—actions quintessentially related to a publisher's role."[23] The Court concluded that the Communications Decency Act "'specifically proscribes liability' in such circumstances."[24] The Court also held that the signal allegedly transmitted to the plaintiff's computer constituted "information" for the purpose of applying the Communications Decency Act, rejecting the plaintiff's contention that this term should be limited to the "communication or reception of knowledge or intelligence."[25]

As cases such as *Doe* and *Green* demonstrate, the Communications Decency Act should provide social networking websites (and their liability insurers) with a significant degree of protection from lawsuits based upon a website's failure to control attacks on members by third parties that are initiated through electronic mail messages, blog postings, or other forms of communication.

B. "Hacking"

However, the Communications Decency Act is unlikely to shield websites from litigation arising from the "hacking" of social networking websites to procure personal information. Unlike "phishing," the installation of malware, or other methods of obtaining personal information that rely upon convincing an individual to click on a link or fill out a form, hacking involves efforts to defeat a website's security controls to obtain unauthorized access to the site. As this would involve no "communication" between the third party and the victims of the data breach, the Communications Decency Act would not appear to apply.

While the major social networking websites have so far avoided a large-scale data breach, they are certainly not immune from such a potential. For example, a Canadian computer technician was able to exploit a security flaw in Facebook to obtain access to private photographs of high-profile Facebook members such as Paris Hilton and Facebook founder Mark Zuckerberg.[26] Regardless of the extensive security measures put into place by these websites, it may only be a matter of time before a social networking website becomes the victim of a large-scale breach affecting millions of members.

Indeed, such large-scale breaches have already begun to plague the makers of applications that have

become a popular element of social networking websites such as Facebook and MySpace. At the end of 2009, a putative class action complaint was filed against third-party application manufacturer RockYou, contending that the company failed to properly secure its customer data, allowing a hacker to obtain the e-mail addresses and passwords of approximately 32 million registered users.[27]

This action follows a recent wave of putative class actions filed against retailers and financial institutions alleging insufficient measures to protect against large-scale data breaches. These actions have typically proven problematic, given the fact that usually only a small percentage of individuals affected by a data breach actually suffer a financial loss as a result of the breach. In an effort to maximize the value of these cases and eliminate individualized inquiries into damages that would necessarily prove fatal to class certification, plaintiffs and their attorneys have urged courts to recognize alternate theories of damages for these individuals. Such theories include consequential damages for the time allegedly spent by class members responding to the breaches, as well as "credit monitoring" to alert affected individuals if and when unauthorized use of the compromised information has had an impact on credit histories. Courts have typically declined to impose these alternate theories of damage.[28] Accordingly, courts have generally refused to certify such large-scale data breach cases as class actions.[29]

The outcome of these putative class actions suggests that the potential exposure for social networking websites from incidents of data breach will be limited to monetary losses directly resulting from incidents of data breach. While this could mitigate the potential exposure faced by social networking websites and their liability insurers, such exposure may nonetheless remain significant. For example, ir *In re TJX Companies Retail Sec. Breach Litigation*,[30] the United States Court of Appeals for the First Circuit allowed a bank seeking to represent a putative class to pursue a claim under the Massachusetts unfair trade practices statute against a retailer (as well as the bank that processed credit/debit card transactions on the retailer's behalf) for damages sustained due to a large-scale data breach, including damages arising from the reimbursement of fraudulent charges resulting from the data breach. Regardless of how the issue of class certification is ultimately decided, *In re TJX Companies* suggests that the risk of liability exposure arising from losses to customers affected by a data breach may be overshadowed by the risk of exposure arising from banks that compensated customers for these losses. As a large-scale data breach incident may easily result in thousands of fraudulent charges to customers of a single bank, an action by a single bank seeking compensation for such charges may result in losses that rival or exceed any potential verdict in a consumer class action.

Therefore, while federal law is likely to shield social networking websites from liability arising from data breach schemes arising from electronic mail messages, such websites and their insurers may nevertheless face significant liability from data breach resulting from the hacking of such websites. In order to protect against such liability, social networking websites should continue to be diligent in ensuring that their security procedures are state-of-the-art. In doing so, social networking websites wil help ensure that increasingly aggressive efforts of cyber-criminals do not prove to be a costly proposition.

1 Spencer E. Ante, *How Much Are Twitter's Tweets Really Worth?*, Business Week, Jan. 6, 2010, http://www.businessweek.com/magazine/ /b4163031536324.htm.

2 http://www.facebook.com/press/info.php?statistics.

3 Associated Press, *What a Twit! Twitter-Using Juror May Cause $12.6 Million Mistrial*, Mar. 13, 2009, http://www.nydailynews.com/news/ /2009/03/13/2009-03-13_what_a_twit_ twitterusing_juror_may_cause.html; Emilie Lounsberry and Craig R. McCoy, *Fumo's Bid for New T* Philadelphia Inquirer, July 10, 2009, at p. B1. *See also U.S. v. Fumo*, 639 F. Supp. 2d 544, 554 (E.D. Pa. 2009).

4 Associated Press, *Appeals Panel Voids Conviction Because of Juror's Blog*, North County Times, June 15, 2007, http://www.nctimes.com/ /2007/06/16/news/sandiego/ 16_56_576_15_07.txt.

5 Kim Zetter, *Trick or Tweet? Malware Abundant in Twitter URLs*, Wired, Oct. 29, 2009, http://www.wired.com/threatlevel/2009/10/twitter

6 *Id.*

7 Miguel Helft, Facebook Gets Friended by Malware (Aug. 26, 2008), http://bits.blogs.nytimes.com/2008/08/26/facebook-gets-friended-by

8 *Id.*

9 Barb Dybwad, Warning: New Facebook Malware Attack is Spreading (Oct. 1, 2009), http://mashable.com/2009/10/01/new-facebook-at

10 Suzanne Choney, Facebook Hit Again With E-Mail Phishing Attack (May 21, 2009), http://www.msnbc.msn.com/id/30874530.

11 *Id.*

12 *Id.*

13 47 U.S.C. § 230.

14 47 U.S.C. § 230(c)(1).

15 47 U.S.C. § 230(f)(3).

16 47 U.S.C. § 230(e)(3).

17 *Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc.*, --- F.3d ---, 2009 WL 5126224, at *2 (4th Cir. Dec. 29, 2009) (citing *Fair Hous. C Roommates.com, LLC*, 521 F.3d 1157, 1162 (9th Cir. 2008) (*en banc*)).

18 528 F.3d 413 (5th Cir. 2008).

19 *Doe*, 528 F.3d at 419.

20 *Id.* at 419-20 (quoting *Doe*, 474 F. Supp. 2d 843, 849 (W.D. Tex. 2007)).

21 *Id.* at 420.

22 318 F.3d 465 (3d Cir. 2003).

23 *Green*, 318 F.3d at 471.

24 *Id.* (quoting *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 333 (4th Cir. 1997)).

25 *Id.*

26 Vancouver Man Exposes Facebook SecurityBreach (Mar. 25, 2008), http://www.cbc.ca/world/story/2008/03/25/face-book.html; *Clari Inc.*, Case No. 3:09-cv-06032-VRW (N.D. Cal.).

27 David Kravets, Facebook App Maker Hit With Data-Breach Class Action (Dec. 30, 2009), http://www.wired.com/threatlevel/2009/12/fa app-data-breach.

28 *Stollenwerk v. TriWest Healthcare Alliance*, 254 Fed. Appx. 664, 666 (9th Cir. 2007) (applying Arizona law); *Pisciotta v. Old Nat. Bancor* 629, 638 (7th Cir. 2007) (applying Indiana law); *In re Hannaford Bros. Co. Customer Data Security Breach Litigation*, 613 F. Supp. 2d 108, 1 2009) (declining to recognize claims for emotional distress or consequential damages by claimants who did not sustain pecuniary loss due to personal information).

29 *Stollenwerk v. TriWest Healthcare Alliance*, No. CV-03-0185-PHX-SRB (D. Ariz. Jun. 10, 2008).

30 564 F.3d 489 (1st Cir. 2009).