A Little Bird Tells Me the FTC Finalized the Twitter Privacy-Breach Settlement & That Ashton Kutcher Got Twitter-Punk'd

Reminders That Your "Private" Web Activity May Not Be Private After All

By Robert J. McGuire, Esq.

On March 11, 2011, five Commissioners of the Federal Trade Commission (FTC) unanimously voted to finalize a settlement with the social networking site, Twitter, that arose from the FTC's conclusion that defects in Twitter's security measures had permitted hackers to gain administrative control over the site on two occasions in 2009. The hackers were able to access non-public user information and tweets that consumers had designated as private. The hackers also had the ability to send out phony tweets from any account.

To gain access on the first occasion, the hackers used a "brute force hacking tool," which tries various combinations of words or numbers from a preset "library" of terms and phrases until a valid password is entered. To gain access the second time, the hackers apparently used a much more basic and disquieting method – they simply guessed correctly an administrator's password. The accounts to which the hackers had access included those of then-President-elect Barack Obama and Kim Kardashian. One can imagine the potential firestorms that could result from fake tweets from either of those accounts. (Ms. Kardashian recently claimed that her Twitter account had been hacked in February 2011, blocking her from logging into her Twitter account from her home computer.) The FTC asserted that the hackers actually accessed fifty-five accounts.

The FTC charged that Twitter "deceived consumers and put their privacy at risk by failing to safeguard their personal information." The FTC had reached a preliminary settlement with Twitter in June 2010. This final settlement is a "consent agreement," meaning that, in entering the settlement, Twitter did not admit that it had violated any laws. Under the settlement, Twitter will be barred for twenty years from "misleading consumers about the extent to which it protects the security, privacy, and confidentiality of nonpublic consumer information, including the measures it takes to prevent unauthorized access to nonpublic information and honor the privacy choices made by consumers." Twitter also must establish and maintain a comprehensive information security program "reasonably designed to protect the security, privacy, confidentiality, and integrity of nonpublic information." Twitter must also ensure that any service providers it employs maintain appropriate data security safeguards. Further, it must

designate one of more employees to coordinate and be accountable for the company's information security program. Twitter's security measures will be assessed by an independent auditor every other year for 10 years. The FTC may fine Twitter up to $16,000 for every violation of the consent agreement.

The settlement was finalized shortly after another high-profile incident of alleged Twitter account hacking on March 3, 2011 – this one featuring Ashton Kutcher, one of the first celebrities to exploit Twitter as a promotional tool (he has over six million Twitter followers) and himself known for his celebrity-prank television show *Punk'd*. On that date, the following tweet was posted from Kutcher's feed: "Ashton, you've been Punk'd. This account is not secure. Dude, where's my SSL?" ("SSL" is short for "Secure Sockets Layer," a security technology that establishes an encrypted link between a web server and a browser and that ensures the privacy of data passed between a web server and browsers.)

Some speculate that Kutcher's account may have been hacked when he used an unencrypted link at a WiFi hotspot. Most people do not realize that, because many free WiFi hotspots employ unsecured networks, information transmitted from those hotspots is typically not secure unless a user is: (1) connected to a virtual private network, (2) remotely connected to a computer network through a service like LogMeIn or GoToMyPC, (3) using an SSL connection, or (4) encrypting transmissions. At an unsecured WiFi hotspot, it is very easy for someone sitting nearby, using certain readily-available technology, to "hitch a ride" into another person's wireless connection. The "hitcher" thereby can gain access to the user's Facebook or Twitter session, or can capture other information shared during that WiFi session, including user names and passwords. (If you have to ask whether you have been using a VPN or an SSL connection while on the WiFi connection at your local coffee shop, you almost certainly are not.) Because of the lack of security at such free WiFi hotspots, it is wise not to send or receive sensitive e-mails, or to transmit personal data (especially user names and passwords) or financial data from those locations.

The lesson to be taken from these recent news items is one that has often been repeated of late – consider carefully what you transmit electronically, where you do it, and how you do it.

Rob McGuire is a partner at Podvey, Meanor, Catenacci, Hildner, Cocoziello & Chattman in Newark, New Jersey. His practice includes commercial and products liability litigation, insurance coverage, and data security and privacy issues.