THE LAW CATCHES UP WITH INTERNET HACKING

A recent case gives computer users more protection

LEGAL CORNER
HARVEY MARS, ESQ.

Harvey Mars is counsel to Local 802. Legal questions from members are welcome. E-mail them to **HsmLaborLaw@HarveyMarsAttorney.com**. Harvey Mars's previous articles in this series are archived at **www.HarveyMarsAttorney.com**. (Click on "Publications & Articles" from the top menu.) Nothing here or in previous articles should be construed as formal legal advice given in the context of an attorney-client relationship.

AS I HAVE remarked many times, the Internet has bred a whole host of legal conundrums that courts are only now catching up to. One of the more prominent problems arises when a person's personal computer is hacked or unlawfully accessed. There are several statutes that provide remedies, both civil and criminal.

The Computer Fraud and Abuse Act (CFAA) and the Stored Communications Act (SCA) are federal statutes that are meant to impose criminal penalties upon individuals who impermissibly infiltrate another individual's private computer without permission. These statutes were intended to impose severe criminal penalties on computer hackers. However, like many criminal statutes, these laws also have civil enforcement provisions that allow the individual whose computer is hacked to obtain monetary damages from the hacker. Unfortunately, the civil enforcement provisions of these laws have very short statute of limitations. They both possess a two-year statute of limitations that begins to run from the date that the infiltration is discovered. This leads to a whole host of problems. What if the hacker is unknown? How do you commence a suit against an individual whose identity you have yet to learn?

Recently, I litigated a suit in which the U.S. Court of Appeals for the Second Circuit grappled with these issues for the first time. The case involved a young lady whose romantic relationship with a co-worker eventually soured. Rather than bowing out gracefully, the defendant, a man named Phil Bernadin, stole his former paramour's AOL and Facebook account passwords and send horrible sexually-oriented comments to her contacts list. He also changed her passwords so that she could not access her accounts to purge them of these false sexually explicit comments. She discovered that she could not access her computer during the summer of 2011. At that point, she decided to pursue her legal rights.

In addition to hiring me as her lawyer, my client also employed an attorney who is also a computer expert to serve subpoenas on the Internet service providers that Mr. Bernadin used to access the Internet. The subpoenas revealed that my client's computer was accessed from a computer that Mr. Bernardin's wife, Tara, used to assess the Internet. So we started the case by suing Tara Bernardin. The suit quickly settled after Ms. Bernardin revealed that it was actually her husband who had been using the computer, not herself. We then sued Mr. Bernardin. As soon as he was served with the suit, Mr. Bernardin moved to dismiss it on the ground that it was not timely. The U.S. District Court of the Eastern District of New York agreed and dismissed the suit on the ground that it had not been filed within two years of the date that my client could not access her AOL account. The court held that once her AOL account had been hacked, she was on notice that other accounts could have been hacked as well. So I appealed to the Second Circuit.

PHOTO: PASHA IGNATOV VIA ISTOCKPHOTO.COM

In a decision that was reported on the front page of the New York Law Journal on Aug. 6, 2015, the Second Circuit upheld the dismissal with regard to the plaintiff's AOL account. *Sewell v. Bernardin, ---- F. 3d ---- (2nd Cir., August 4, 2015)*. However, it reversed the lower court's decision with regard to Mr. Bernardin's trespass of my client's Facebook account, which occurred in February 2012, well within the two year statute of limitations. The court held that unauthorized access of the AOL and Facebook accounts were separate violations because, as the court said:

It is not uncommon for one person to hold several or many Internet accounts, possibly with several or many different user names and passwords, less than all of which may be compromised at any one time. At least on the facts as alleged by the plaintiff, it does not follow from the fact that the plaintiff discovered that one such account – AOL e-mail – had been compromised that she thereby had a reasonable opportunity to discover, or should be expected to have discovered, that another of her accounts – Facebook – might similarly have become compromised.

The court also noted that a flexible approach was warranted because of the brevity of the statute of limitations and the difficulty many litigants will have in discovering who hacked their computer.

As it stands, this case demonstrates just how the Internet can be used for pernicious purposes. One must always be on guard to ensure that passwords are stored safely and are not easy to infiltrate. The importance of this lesson cannot be stressed better than a recent hilarious conversation between the famous whistleblower Edward Snowden and the British comedian and political commentator John Oliver. Go to YouTube and search for "Last Week Tonight with John Oliver: Edward Snowden on Passwords." Besides being funny, it is instructive to anyone who uses computer passwords – which is pretty much everyone.