Chicago Daily Law Bulletin®

Volume 163, No. 203 Serving Chicago's legal community for 162 years

# Nasty divorce litigation opens doors to threat of cyber exposure

It is virtually impossible to watch the news or open a modern mainstream mobile news app without seeing a headline concerning cybersecurity.

Recognizing the importance of cybersecurity, October is the Department of Homeland Security's National Cybersecurity Awareness Month.

The growth of modern society's reliance on technology and connectivity is undeniable. This growth perpetuates increased risk for cyberattack, electronic monitoring and surveillance and data breach. A notable recent example is the Equifax data breach, which, according to Federal Trade Commission, affected more than 143 million American consumers with credit reports.

Not surprisingly, the abuse of varying forms of technology is becoming more common in divorce litigation.

With access to genuine information a click or two away, with little cost, effort and technical skill, a spouse in contested divorce litigation can uncover e-mails, text and video messages, transcribed voicemails, photographs, videos, audio-recordings and financial and other information.

The following is a typical example of potentially illicit information gathering: Spouse A suspects Spouse B of extramarital infidelity and financial impropriety. Acting on that suspicion, Spouse A accesses Spouse B's computer and e-mail accounts with a password found written in Spouse B's daily planner, which is typically kept in Spouse B's briefcase.

Along the way, Spouse A installs spyware on Spouse B's computer. Next, Spouse A, having previously seen Spouse B enter the six-digit password, "borrows without permission" and accesses Spouse B's iPhone to obtain text and other messages.

Armed with the spoils of espionage, Spouse A schedules an appointment with a divorce lawyer.

Many divorce litigators have seen this situation become reality and thus know the corresponding legal implications on both federal and state levels.

**Federal law**

The Electronic Communications Privacy Act, 18 U.S.C. Section 2510, et seq., is a federal statute with three components dealing with electronic communications, two of which are relevant here.

First, the Wiretap Act (Sections 2510 to 2522), prohibits, in summary, the intentional or attempted interception or disclosure of any wire, oral or electronic information.

Second, the Stored Communications Act (Sections 2701 to 2712) prohibits intentional and unauthorized access of a facility providing electric communication services.

Also of note is the Computer Fraud and Abuse Act, 18 U.S.C. Section 1030, which, in summary, prohibits a party from accessing another's computer without (or by exceeding) authorization. The act applies to computers utilized in interstate or foreign commerce, which includes any computer connected to the internet.

**Illinois law**

In response to the Illinois Supreme Court's ruling in *People v. Clark*, 2014, IL 115776, and *People v. Melongo*, 2014 IL 114852, the legislature recently amended the Illinois Eavesdropping Act (720 ILCS 5/14, et seq.), which provides that a person commits eavesdropping when they knowingly and intentionally use an eavesdropping device in a surreptitious manner to overhear, transmit, record or transcribe any private conversation or private electronic communication to which he or she is not a party without the consent of all other parties to the private conversation.

The Eavesdropping Act defines a "private conversation" as any oral communication between two or more persons, whether in person or transmitted by wire, where there exists a reasonable expectation of privacy and a "private electronic communication" as any transfer of signs, writing, images or sounds where the communication is intended to be private under circumstances reasonably justifying that expectation. (720 ILCS 5/14-1(d)(e)).

In the hypothetical, Spouse A's accessing Spouse B's computer, intercepting e-mails and installation of spyware may be a violation of all three federal acts to varying degrees depending on the level of access and subsequent transmittal.

Likewise, Spouse A's accessing Spouse B's cellphone for text and other messages may violate the Wiretap Act, and if Spouse A intercepted telephone conversations through the use of spyware, arguably the Eavesdropping Act.

Additionally, assume for example that Spouse A used the family's smart-home audio-video recording devices to record private telephone conversations of Spouse B in a bedroom or office. The Eavesdropping Act may be invoked to render the recordings illegal and thus excluded from litigation.

The takeaway for divorce litigators and clients is threefold:

First, given the increasing risk of exposure to cyber breach in varying forms, it is good practice to advise clients at the outset of a divorce case to take defensive measures, such as changing passwords to cellphones, personal computers, e-mail and other online accounts.

Where families operate on a shared cell and data plan, clients should be advised to either restrict or disable account access so as to avoid one spouse's unauthorized access to messaging features through multiple platforms (e.g. iMessage access on an iPad linked to the same account as a spouse's iPhone).

In certain cases, clients should be advised to set up credit monitoring alerts aimed at notifying the registrant of any alterations to existing accounts or opening of new accounts.

Second, cognizant of the legal authority referenced herein, practitioners must be cautious in the retention or transmittal of illegally obtained information from clients through mechanisms like those employed by Spouse A.

Third, clients in divorce litigation may not be the only people perpetrating a cyberattack. In representing certain high-net worth or high-profile clients with confidentiality at an ultra-premium, a divorce litigator and their law firm should be proactive in cyber defense, through for example, installation and maintenance of protective software and hardware encryption as well as firmwide cybersecurity training, to avoid both general and targeted cyberattack.

MODERN FAMILY

**BRETT M. BUCKLEY**

*An associate attorney with Schiller DuCanto & Fleck LLP, Brett M. Buckley represents business owners, executives, professionals, celebrities, professional athletes, people with multigenerational wealth and their spouses in divorce and custody disputes. He can be reached at bbuckley@sdflaw.com.*

*... take defensive measures, such as changing passwords to cellphones, personal computers, e-mail and other online accounts.*