A computer record could save, or ruin, a trade secret case

By Brandon J. Vogel

That confidential document saved to a smartphone could be powerful evidence against an employee who leaves to work for a competitor.

In an age in which confidential documents are emailed from work computers to home, and work email can be accessed on cell phones, sensitive information can be found…anywhere.

This poses significant legal risks for both employees who start new jobs and for their past employers.

Panelists at "Obtaining Computer Evidence in Trade Secret Litigation" cleared up several employee misconceptions about privacy on company-owned computers and how the actions of all the involved parties can impact e-discovery if there is litigation. The program was the final panel of the Intellectual Property Section's daylong Annual Meeting discussions.

Steps to take

Lance J. Gotko of New York (Friedman Kaplan Seiler & Adelman LLP) discussed important pre-litigation steps for employer-plaintiffs in trade secret cases.

Gotko said that the forum for trade secret cases—litigation, arbitration or criminal court—will impact what kinds of discovery, including e-discovery, will be available. Civil litigation generally offers the most methods of discovery. Arbitration might offer limited discovery, but could be the best forum for companies to guard the confidentiality of trade secrets.

"Getting forensic and trade experts involved early to identify where discovery is located is very important," said Gotko.

Bryan J. Rose of New York (Stroz Friedberg) agreed. "You want to be sure that you do due diligence immediately," he said. "There is often good evidence on computers and other fragile sources that can be lost."

Gotko advised attendees to identify key sources of e-documents. Employees may have many electronic documents on their home computers or have sent sensitive work emails to or from their personal accounts, which are sometimes stored on a server or copied to a hard drive.

"On the flip side, employee defendants may want to use emails to show that they were good employees and remained so," said Gotko. "In keeping with their confidentiality obligations to their employers, exiting employees should carefully delete work documents from their personal devices when they leave."

Computers will record Internet activity that can be "very valuable," said Rose. "They record a tremendous amount of history. It can be tremendously powerful evidence."

Employees who chat via instant messenging thinking it's a safe way to communicate are mistaken. After closing a window, instant messages do not disappear, but are archived instead on the device's hard drive.

Delete after reading—Lance J. Gotko of New York (Friedman Kaplan Seiler & Adelman LLP) and Bryan J. Rose of New York (Stroz Friedberg), right, examine pre-litigation steps in trade secret cases. *[Photo by Jacques Cornell/Happening Photos]*

"Instant messages can be a very fertile and damaging piece of evidence," said Rose.

Gotko noted that, "employees often are at their frankest when communicating with co-workers via instant messenger."

Work computers that may have been used to create files of trade secrets that were uploaded to the Internet are a "goldmine" for employer-plaintiffs and a "critical piece of evidence that needs to be secured right away."

In the December 2010 case, *United States v. Aleynikov*, Sergey Aleynikov was sentenced to 97 months in prison followed by three years of supervised release, for using the Internet to transfer source code files from Goldman Sachs to a computer in Germany. It was the first use of the Economic Espionage Act to control the misuse of source code in high frequency trading.

Other sources of evidence include unusual activity on print job logs and company-issued laptops, where data is stored until new data overwrites it.

"You have to be aware of other potential sources of discovery, such as Facebook, Twitter and LinkedIn and other cloud storage sites," Gotko said.

Andrea Sharrin of Washington D.C., deputy chief of the Computer Crime and Intellectual Property Section, U.S. Department of Justice, also spoke at the program. ◆

Vogel is NYSBA's Media Writer.