Sponsored Content

Litigation Goldmine: Employee Internet History – More than just Facebook

When it comes to data breach activity, companies should be examining the Internet activity of their own employees—it is more than just Facebook and ESPN News. In two of our most recent cases, based on the Internet history alone, we discovered one employee was logging into the webmail accounts of the CEO and CFO (and using the financial information contained therein to negotiate a bigger raise for himself), and another, an IT administrator, had copied thousands of files to a thumb drive before he resigned and then ran Google searches on how to destroy key operating system files on his company laptop to hide the activity.

MARAGELL Corporate Investigations

Contact: Jeffrey Brenner, Esq., NJLPI

Address: 2 Coleman Ave, Suite 201, Cherry Hill, NJ 08034

Phone: 856.429.0325 x223

Fax: 856.429.0539

Email: jbrenner@maragell.com

Website: www.maragell.com

In both cases, the employees thought they had hidden their tracks by deleting their recent browsing history. But because a computer's operating system maintains the URL addresses of the websites visited in separate files, and other operating system files record images of those sites, through the use of forensic tools, these disparate files were extracted, combined, displayed visually, and the story of their activity revealed. One ended with the employee being terminated, the other with the IT administrator haled into federal court after he surfaced at a competing firm.

While most forensic experts identify the information as the computer's "Internet history" it is much more than just a compendium of web addresses. Because a number of Windows Explorer system files act in the same fashion as the Internet browser system files, when the "history" is extracted, information such as what files were viewed on a thumb drive or where the user went on the company server can often be determined. This user activity is betrayed by the formation of link files, which are created when a user inserts a USB device into the computer and opens a document from it or uses Windows Explorer to navigate to a location on the server. If an employee is suspected of stealing a customer list or other confidential or proprietary information, but the USB device is not available for inspection, the Internet history might seal his/her fate.

The history will also provide evidence of online document storage sites like Dropbox and Google Drive, and data backup sites such as Carbonite and Mozy. Whenever company file access activity on the employee's computer matches that of visits to these categories of websites, it is best practice for counsel to issue preservation letters and/or subpoenas to prevent the information from becoming lost.

More sophisticated forensic software can also rebuild cached images of webpages and webmail messages just as the user saw them. Because webmail does not reside on the local hard drive, the only evidence that an employee was communicating with others about potentially unlawful activity or sending company documents to a personal email account might come from an examination of email fragments recovered from the Internet history.

Practice Point: The immediate preservation of a suspect computer should be the top priority for any In-House Counsel, Litigation Counsel, Human Resources Professional or IT Administrator. Electronic evidence is ephemeral and can be destroyed through the normal use of the computer. Permitting even the weekly updates by Microsoft to be installed can destroy essential evidence needed to prove a case. In short, to maximize the amount of available evidence in cases like those described above, the computer should be turned off and secured in a location where it cannot be accessed until a forensic bit-by-bit mirror image of its hard drive is created. If the subject of the investigation is suspected of downloading or actively running malware in an effort to harm the company (such as Cryptowall or other ransomware), the computer should be left running, but its power cord or battery removed (to keep its RAM intact for analysis).