

Uncovering Communications: A Forensic Look at Online Social Networking Communities

SAM LAU

The author explores online sources of evidence of communications, as well as how to approach the new frontier of social networking communities, as they relate to information gathering in litigation and investigations.

Today, the fast-paced evolution of technology has enabled people to communicate using various channels, including everything from blogging to sending messages on social networking sites such as Facebook or MySpace. In the current environment, in which companies face a number of challenges in managing the damaging effects of fraud and misconduct on their organizations, rapidly evolving social networking communities and their impact on gathering information for investigative or litigation purposes only complicate matters. It was not so long ago that investigating a particular communication involved accessing and analyzing phone records to find out who spoke to whom and when. While analyzing those records usually helped develop a time frame around a communication, the laborious process of obtaining access to phone records did not reveal the substance of the actual communication. As computers became more prevalent in companies and homes, not only could records be obtained more easily, but it was also possible to review the communications themselves and determine the parties involved in the communications. This article explores online

sources of evidence of communications, as well as how to approach the new frontier of social networking communities, as they relate to information gathering in litigation and investigations.

THE HISTORY OF ONLINE COMMUNICATIONS

The ARPAnet (Advanced Research Projects Agency Network), the backbone of the Internet, was commissioned by the U.S. Department of Defense in 1969. The network was initially designed for military applications and had only four computers connected to it.¹ It was not until the mid-1990s that two companies, America Online and CompuServe, enabled the Internet to become accessible to the general public. During these formative years, before the widespread use of the Internet, e-mail communications were limited. As with all forms of communication, e-mail relied heavily on “positive network externality,” i.e., the more people using the communication channel, the more valuable it becomes for each individual user. Clearly, times have changed. In 2008, approximately

Sam Lau is a manager with the Litigation and Fraud Investigation Practice of BDO Consulting, a division of BDO Seidman, LLP, in New York. Mr. Lau, who specializes in computer forensics, e-discovery and data analysis, has more than seven years of experience providing litigation support involving forensic identification, preservation, collection, analysis and presentation of electronically stored information. Mr. Lau is an EnCase Certified Examiner (EnCE).

In the current environment, in which companies face a number of challenges in managing the damaging effects of fraud and misconduct on their organizations, rapidly evolving social networking communities and their impact on gathering information for investigative or litigation purposes only complicate matters.

1.6 billion out of 6.7 billion people around the world have Internet access.² With 24 percent worldwide market penetration, the Internet's functionality serves as the foundation for the rapid advancement of sophisticated new ways to create business and social connections.

Today's technologies allow us to communicate with someone within seconds. Gone are the days when the quickest way to reach a person was by landline or pager. Today, we can stay in contact by snail mail, home or office phones, cell phones, voice-over-IP ("VOIP"), corporate e-mail, Web mail, online messaging systems, text messaging, blogs, social networking sites and other methods. With so many easy-to-use options available to make communication faster and more efficient, companies are challenged with issues of managing risk to the security of corporate information, possible inappropriate employee behavior in new online environments with which they may be unfamiliar, and additional avenues to pursue for information gathering in litigation and investigations.

IMPACT OF ONLINE COMMUNICATIONS IN CORPORATIONS

When companies began providing employees with corporate e-mail addresses, considerable effort was needed to maintain and monitor the information flow. While the initial workflow development and rollouts were time consuming, the task was still manageable. As more communication channels have arisen — and will continue to arise — monitoring their use becomes increasingly challenging.

For example, Instant Messaging ("IM"), which was once popular for teenagers and young adults, has found its way into corporations. There have been ongoing debates over the impact of using IM in the corporate workplace. Proponents of IM consider it to increase productivity by enabling employees to communicate with other employees from the same or dif-

ferent office locations in a quicker, easier manner. It is generally accepted that IM is less formal and less permanent than other communication channels and, therefore, can be used as a tool to gather and communicate quick information without needing to follow the conventions of formal sentence structure or professional tone required for e-mail or letters. Companies that see the benefits of IM have taken steps to gain a level of control over its use. Some have implemented secured enterprise level IM, such as IBM/Lotus Sametime, which restricts the communications to a company's employees and logs all IM exchanges. Opponents of online messaging consider IMs to be distracting for employees and to increase the possibility of security leaks. These corporations employ efforts to block the Internet ports used by the most popular IM service providers. Additionally, companies and governmental organizations involved in secured research or dealing with extremely sensitive information severely restrict Web site address access for employees and shut down all external ports and peripherals (e.g., USB/FireWire ports, CD, DVD, etc.) within a computer to prevent employees from transferring potentially sensitive information. As new technologies continue to emerge and become accessible to employees via the Internet, such as Web mail clients and the increasingly popular social networking sites, companies may find themselves falling behind in safeguarding and monitoring the use of such communication channels.

Traditionally, it has been a battle between those who "build the better mouse" versus those who "build the better mousetrap." For instance, when a company blocks an IM site like AIM, employees may turn to MSN; when a company blocks MSN, employees can shift to Trillian, and the cycle continues. In an effort to be proactive, companies today are continually looking for new ways to address this counter-productive cycle.

Rich Mason, Chief Information Security Officer

at Honeywell International, states, “Heuristically, people have chosen to implement Web site content filtering via a ‘black list.’ This is a never-ending and highly reactive effort to stay on top of new threats and vulnerabilities, define signatures for them and block them. Conversely, a ‘white list’ approach allows only known-good content and the system ‘fails-safe’ by denying content that is either unknown or ‘untrusted.’ As a result of the increasing prevalence of malicious software and Web content, a paradigm shift toward the more preventative ‘white list’ is being witnessed in the industry. By combining this approach with a trusted provider to manage the reputation of software and Web sites and the roles of individuals, IT organizations can get out of the business of managing lists, whether black or white, and get focused on the bottom line: enabling the corporations to conduct their business ... securely.”³ Employees will continue to strive to “build the better mouse” and search for new corporate security work-arounds. However, all is not lost. According to a Vodafone survey, 50 percent of employees use their corporate laptops for personal use.⁴ As long as employees are using corporate laptops from either their offices or in the comfort of their own homes, there are methods available for corporations to potentially uncover “personal” communications, if it is deemed necessary.⁵

ONLINE COMMUNICATIONS IN INVESTIGATIONS OR LITIGATION

One of the fastest-growing types of communities over the past few years is online social networking, including commonly known sites such as Classmates.com, Friendster.com, MySpace.com, LinkedIn.com, YouTube.com, Twitter.com, and Facebook.com. These social networks are designed to help individuals reconnect with old friends and colleagues, network with others of similar career backgrounds or interests and keep friends and families up-to-date on their lives. One of the more popular social networking communities is Facebook, which has over 200 million members worldwide.⁶ Facebook alone provides registered members with an array of communication possibilities, including, but not limited to, the ability to share photos, post thoughts or activities on a personal wall, instant message with friends online

and exchange online messages with other registered members. Many companies today have corporate communication and monitoring policies, which state that corporate e-mails or other forms of electronic communications may be read, examined or scrutinized, if deemed necessary. Some employees may be cautious about their personal communications and may try to exploit the member-to-member e-mail features offered through social networking sites, operating under the false notion that such messages can go undetected by corporate communication monitoring practices. However, communications can often be uncovered and possibly supplied as evidence used in an investigation or in litigation.

As more communication channels have arisen — and will continue to arise — monitoring their use becomes increasingly challenging.

Similarly, it is not uncommon for employees to access personal e-mail accounts online through corporate laptops, thinking that such communications are secure and irretrievable because user names and passwords are required to log in to their online accounts. While such communications are secured to an extent, they are not necessarily irretrievable. These communications can be cached in various areas of a computer’s hard drive that may not be visible to a user. Most users are only concerned with the information contained on the hard-drive areas that they can see (i.e., displayed by the operating system, known as allocated space). However, forensic examiners are equally, if not more, interested in the hard-drive areas that are not displayed by the operating system (i.e., unallocated space). Forensic examiners employ specialized applications that allow access to hard drives on a disk level, enabling examiners to view every single bit contained on a hard drive. This capability becomes critically important in the context of an investigation or pursuant to litigation. Specifically, when responding to an inquiry or a discovery request, a company can retain forensic examiners to

uncover *all* potentially relevant communications, including those that can be seen by a user and those that cannot. Internet communications that employees may think are “secure” can often be uncovered.

Computer forensic examiners often advise companies of the option to look beyond corporate e-mail traffic pertaining to employees of interest during an investigation or in response to litigation. This allows a company to make a more informed decision and determine whether to expand the scope of its review to include other available communication channels and corresponding information not typically considered.

IDENTIFYING ONLINE COMMUNICATIONS

Although the actual procedures vary on a case-by-case basis, typically a forensic examiner will analyze computer hard drives to find a pattern in an employee of interest’s Web-browsing history, determining whether they have any external e-mail addresses, instant messaging accounts or social networking accounts. If any are identified, the forensic examiner can attempt to retrieve related communication histories. While computer forensic experts portrayed on television or in the movies seem to click a magical “find evidence” button to locate hidden communications and display them in a coherent manner just minutes before the bad guy gets away, much of what forensic examiners do requires manual processing and training to review data that exists in fragmented format, which would seem abstract or unintelligible to an untrained eye. These communications typically do not resemble the structure of an e-mail or document with which most people are familiar. Instead, a simple, multiple-line communication between two parties can span across tens of pages before it can be deciphered to reveal the actual context of the message. For instance, a computer forensic examiner encountering a hard drive with Facebook activity might find coding such as <http://www.facebook.com/profile.php?id=983453298>.⁷ This type of coding would indicate that the user is a registered Facebook member, with the unique identification of “983453298” having logged into Facebook. Typically, when a user searches for friends using Facebook, they must enter information about the person of interest, such as first and last name, e-mail address, city and state or country, schools and universities at-

tended, companies employed, etc. Computer forensic examiners can also use Facebook’s search feature to perform a reverse lookup. In other words, examiners can find the individual to whom the ID “983453298” belongs. Once the forensic examiner determines that the unique identifier belongs to one person, he or she can begin to recover communications between the employee and other registered Facebook members. If the communications contain evidentiary values, the forensic examiner may need to determine the exact date and time when the communication took place. Facebook encodes the date and time in UNIX format, which makes it easy for the computer to determine the precise time when the communication occurred. The UNIX time (aka POSIX [Portable Operating System Interface for UNIX] time) is a system that calculates the number of seconds elapsed since January 1, 1970. Therefore, when a forensic examiner uncovers a string of text such as “1244581078_ ... Facebook | Message: Did you cash the check?_...,” it indicates that the message took place 1,244,581,078 seconds from January 1, 1970, which directly translates to March 15, 2009, 08:33:00 GMT time. Since Facebook messages are contained within the unallocated areas of the hard drive, it may not be possible to restore the date and time for every message. When the UNIX time is not available, forensic examiners can potentially calculate the best estimate of when the communication took place by applying outside-of-the-box logic. For instance, the example below expands on the coding of the previous example:

```
<html>
...
1244581078_ ... Facebook | Message: Did you
cash the check?_...,
...<img src = “http://static.ak.fbcdn.net/images/
advertise.gif” > ...
...
</html>
```

In the above example, the message is accompanied by an advertising.gif logo from Facebook. This is common since Facebook, as well as other social network sites, generate their revenues from marketing and advertising. Forensic examiners could attempt to

locate the advertising.gif file on the employee of interest's hard drive and determine the date and time when this file was introduced to the employee's computer system. In addition, the examiners can also analyze the employee's Internet history to see when the Web site from which the advertising.gif file originated, <http://static.ak.fbcdn.net/>, was last accessed. Using these dates and times, forensic examiners can make a reasonable assumption that a communication took place at or around an identified time period. While not an exact science, it provides forensic examiners with a starting point. The ability to connect various parties to communications becomes instrumental during an interview of an employee of interest in order to help establish time frames around computer usage to test the veracity of an employee's responses. Responses such as "I do not know how that data got there" or "someone must have hacked into my account" can be refuted, and forensic examiners can conduct further analysis of an employee of interest's computer systems to potentially eliminate plausible deniability.

To mitigate risk to corporate information, and to use as a valuable source of information about employee or corporate conduct pursuant to an investigation or to litigation, companies are well-advised to be aware of how current social networking channels are employed within their organizations.

CONCLUSION

While we explored Facebook as an example of a well-known social networking channel available today, other sites have similar methods for storing communications between registered members. Coupled with standard corporate e-mails, instant messaging, text messaging, Web mails and numerous others com-

munication channels, there are multiple avenues that companies can use today to uncover communications for purposes of investigation or litigation. To mitigate risk to corporate information, and to use as a valuable source of information about employee or corporate conduct pursuant to an investigation or to litigation, companies are well-advised to be aware of how current social networking channels are employed within their organizations.

NOTES

¹ Wendy Boswell, "History of the Internet," About.com, <http://websearch.about.com/od/whatistheinternet/a/historyinternet.htm>.

² Miniwatts Marketing Group, "Internet Usage Statistics," Internet World Stats, <http://www.internetworldstats.com/stats.htm>.

³ Rich Mason, Chief Information Security Officer at Honeywell International, in an interview with the author, June 10, 2009.

⁴ David Masters, "Employees See Work Laptops as Personal Property," *Security Watch*, March 24, 2009, <http://www.securitywatch.co.uk/2009/03/24/employees-see-work-laptops-as-personal-property/>.

⁵ Monitoring and/or recovering employees' computer system(s) that may contain personal documents or communications is subject to local privacy laws. Please consult with counsel to determine whether your corporation adheres to the laws prior to engaging in any computer forensics processes.

⁶ Lee Bains, "Facebook Overtakes MySpace as Most Popular Social Network Site," Switched.com, January, 27, 2009, <http://www.switched.com/2009/01/27/facebook-overtakes-myspace-as-most-popular-social-networking-sit/>.

⁷ The user ID presented is a fictitious ID and, at the time of publication, does not pertain to any member of Facebook. This may or may not change in the future. However, if this user ID does tie at any point to any Facebook member, it is only through sheer coincidence, and the member is not associated with the author(s) and/or the company responsible for editing or publishing this article.