Thursday, May 31, 2012

THE DAILY RECORD

WESTERN NEW YORK'S SOURCE FOR LAW, REAL ESTATE, FINANCE AND GENERAL INTELLIGENCE SINCE 1908

eDiscovery UPDATE

(Deleted) text messages and eDiscovery

In April, British Petroleum employee Kurt Mix was arrested for deleting over 300 text messages. The deleted messages tracked failing efforts by BP to control the Deepwater Horizon spill, including the fact that the amount of leaking oil exceeded what the company reported.

This is the first criminal charge arising from the April 2010 Deepwater Horizon incident. The Justice Department arrested Mix and charged him with two counts of obstruction of justice for allegedly destroying evidence. If convicted, he could face up to 40 years in prison and a fine of $500,000.

By PETER COONS
Daily Record Columnist

Deleting text messages can get you 40 years in prison? Of equal interest is that it now appears that Mix deleted 200 messages in 2010 and an additional 100 a year later. This says to me that a computer forensic examiner was able to recover those messages long after they were deleted.

What type of phone was the engineer using? A special phone that only high-tech oil engineers have access to? Nope, it was an iPhone, and the indictment states that BP repeatedly told Mix to retain all relevant material, including text messages. Not surprisingly, attorneys for Mix say that there is a plausible explanation for the deleted texts and point to the fact that he did produce other documents.

What I find most interesting about this case is it demonstrates the power of computer forensics in the discovery process. Cell phones — aka "smart" phones — are the new computers that happen to fit in a pocket. In my experience, there can be more data on a smart phone than a computer.

But is a phone a computer, and is it fair game in discovery? The answer is yes to the latter and possibly to the former. One court went so far as to say that a phone is a computer.

In the case *United States v. Neil Scott Kramer*, the U.S. Court of Appeals for the Eighth Circuit affirmed that under the facts of that case, the phone was a computer. This holding was central to the case because the sentencing provision included an enhancement that applied if the defendant used a computer — which in this case happened to be a phone — to commit the crime.

So how do computer forensic examiners get at all those deleted messages? Again, from a technical standpoint, a phone is a computer and stores data just like a computer. It has an operating system (e.g. Windows or Mac) and a file system (e.g. FAT32). The phone has a memory card or internal memory where data like emails and text messages are stored. When that data is "deleted," it can sometimes be recovered — again, just like a computer.

Qualified forensic examiners can use a number of commercially available software and hardware tools to preserve and extract data from cell phones. This includes, but is not limited to, deleted text messages, photos, emails, contacts, calendar appointments, notes and apps. If it can be seen on a phone and deleted, then it can possibly be recovered.

However, as is true with computers, deleted information does not stay around forever, so time is of the essence. Proper handling of a phone is also important. Most phones need to be powered on to have the evidence collected so it is important that they are shielded properly. This means using a device like a Faraday box or bag that will block any outgoing or incoming signals. The phone is placed in this box or bag before it is powered on.

Why is this important? Among other things, iPhones have a remote wipe feature that allows someone to send a signal to your iPhone and wipe it remotely, thus clearing the settings to the factory defaults. As we learned in the BP case, (confirming my own personal experience) it is possible to recover text messages with the proper tools and know-how, but some items may be forever lost if a remote wipe signal is sent.

How can one request data from cell phones or include phones in a preservation letter to ensure the opposition will not delete

Continued ...

Thursday, May 31, 2012

THE DAILY RECORD

WESTERN NEW YORK'S SOURCE FOR LAW, REAL ESTATE, FINANCE AND GENERAL INTELLIGENCE SINCE 1908

Continued ...

potentially relevant material, like text messages? In short, use the same language as a request for a laptop, server or email account. It is electronically stored information and if there is potentially relevant data stored on the phone then it must be preserved. Include smart phones, cell phones and tablets in any preservation or document request, and use examples such as BlackBerrys, iPhones, iPads, Droids, etc. If an opportunity arises to depose a 30(b)(6) witness, plan to discuss how the organization uses smart phones and other remote computing devices.

At the end of the day we all realize that technology is changing faster than we can keep up. At the end of that same day we must also realize that litigation and the obligations of parties to preserve evidence has not changed at all. Where it is stored may be different but the same rules apply. Today's deleted texts from iPhones are yesterday's deleted emails from laptops and are tomorrow's deleted Facebook postings in the cloud!

Peter Coons is a senior vice president at D4, providing eDiscovery consulting services to clients. He is an EnCase Certified Examiner, an Access Data Certified Examiner, a Certified Computer Examiner (computer forensic certificates) and is a member of the High Technology Crime Investigation Association, the professional organization for people involved in computer forensics.