eDiscovery in Social Media – Controversial Facebook Photo Sparks Debate

by Peter Coons, SVP, Computer Forensics and Collections

Ethics 101

'I <3 Hot Moms!' This was the phrase on a t-shirt of a widower, Mr. Lester. He was wearing it in a picture he had posted on his Facebook page. Lester was the plaintiff in the case *Lester v. Allied Concrete Company*. His lawyer, Mr. Murray, didn't think this was an appropriate picture and he instructed the paralegal on the case to have Lester clean up his Facebook page. It was found that Lester deleted a total of 16 photos prior to producing material to defense counsel.

As you may know, this case ended up costing the lawyer his career and the judge in the case reduced the damages awarded to the plaintiff. The judge in the case also fined the lawyer to the tune of $522,000.

Based on the facts of the case that I reviewed, the lawyer in this case was clearly in the wrong and engaged in unethical behavior. **Evidence on ones Facebook page and other social media is fair game in litigation** and attorneys need to appropriately advise their clients on steps to preserve and produce relevant material.

How did experts in the case find that Lester deleted these photos?

Plaintiffs subpoenaed Facebook and asked for the IP logs. I looked into this a bit further and found some interesting information about what IP logs from Facebook reveal.

IP logs can be produced for a given user ID or IP address. A request should specify that they are requesting the "IP log of user Id XXXXXX" or "IP log of IP address xxx.xxx.xxx.xxx".

The log contains the following information:

- Script – script executed. For instance, a profile view of the URL *http://www.facebook.com/profile.php?id=29445421*, would populate script with "profile.php"
- Scriptget – additional information passed to the script. In the above example, scriptget would contain "id=29445421"
- Userid – The Facebook user id of the account active for the request
- View time – date of execution in Pacific Time
- IP – source IP address

From the information above I came to the conclusion that the log files provided the "script" that was executed when the user was logged in. I assume that if someone deleted photoXYZ, it would state that in a corresponding line item along with the date, time, and the userid that executed the command. If my assumption is correct, someone analyzing this information would be able to identify every action taken

by a user. I am making this assumption because I do not have an actual IP log. I did attempt to e-mail Facebook to request my own IP log. I e-mailed records@facebook and received an auto-response that stated my request would not be responded to unless the request was from law enforcement or I was an attorney issuing a subpoena. I guess IP logs for my account do not belong to me.

On Facebooks' terms!

In the terms of service for Facebook, it clearly states that all data uploaded to a Facebook page belongs to the owner of that page.

> "You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings."

I guess that statement does not apply to information about my information.

But what about information I delete on my Facebook page? What about that hot moms' photo? If Lester deleted it, could Facebook retrieve it? In the Lester case the experts determined 16 photos were deleted but they did not state in the court papers I read which 16 photos were deleted.

In the Facebook terms of service it also states the following:

> "When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others)."

In the world of computer forensics this says to me that Facebook has the ability to retrieve this information, assuming it has permission from the owner of the account. Whether Facebook would undertake this effort is another question and I wonder why they even put this in their TOS. It seems like a potential nightmare for them. However, as stated above, you would need to have authorization from the user as Facebook will hide behind the Stored Communication Act if you try to subpoena them without the users' permission. This is what happened in*Crispin v. Audigier* when the defendants served a subpoena on Facebook and it was successfully quashed by plaintiff. It is also clearly stated on Facebook:

> "Federal law prohibits Facebook from disclosing user content (such as messages, Wall (timeline) posts, photos, etc.) in response to a civil subpoena. Specifically, the Stored Communications Act, 18 U.S.C. § 2701 et seq., prohibits Facebook from disclosing the contents of an account to any non-governmental entity pursuant to a subpoena or court order.
>
> Parties to civil litigation may satisfy discovery requirements relating to their Facebook accounts by producing and authenticating contents of their accounts and by using Facebook's "Download Your Information" tool, which is accessible through the "Account Settings" drop down menu."

DIY or DYI

I have discussed the "Download Your Information" tool in another post and there is a great post about it on a blog by X1discovery.

Based on the research by X1, the "Download Your Information" tool from Facebook does not capture potentially important metadata for the pages being downloaded and it fails to capture all the information from a users' site. As I stated in my earlier post, no matter what option one chooses to capture ESI, the method should be vetted and the resulting information should be validated to ensure all potentially responsive information is being captured. **Do not rely on the statement by Facebook that their tool is to be used for electronic discovery purposes.**

Let's get back to deleted information. Once a user deletes information, can it be retrieved by the user? According to Facebook, the answer is:

> "You cannot retrieve deleted messages, but you can go back and find messages you archived. Archiving a message hides it from your messages view, while deleting a message permanently removes the entire conversation and its history."

I tested this out on my own Facebook page and deleted an e-mail thread. Once deleted I could not find a way to get it back. However, when I asked my friend to respond to the deleted thread, the entire thread once again appeared in my message area in Facebook. This makes sense since this is how I would expect it to work in an application like Outlook.

Also remember that Facebook now allows users to send messages using the e-mail address USERNAME@facebook.com. This means that Facebook messaging is like any other e-mail application. A user without a Facebook account can send and receive messages to/from a Facebook user and vice-versa. This opens up a whole new source of ESI for discovery.

Europe v. Facebook

What about the claim on a post I read recently about all of the information Facebook knows about its users?

Here, an individual requested Facebook to send him all his content: (please note that this is an account based in Europe and there are different rules Facebook must abide by for European based accounts. Meaning, fat chance getting Facebook to do this for a U.S. based account…)

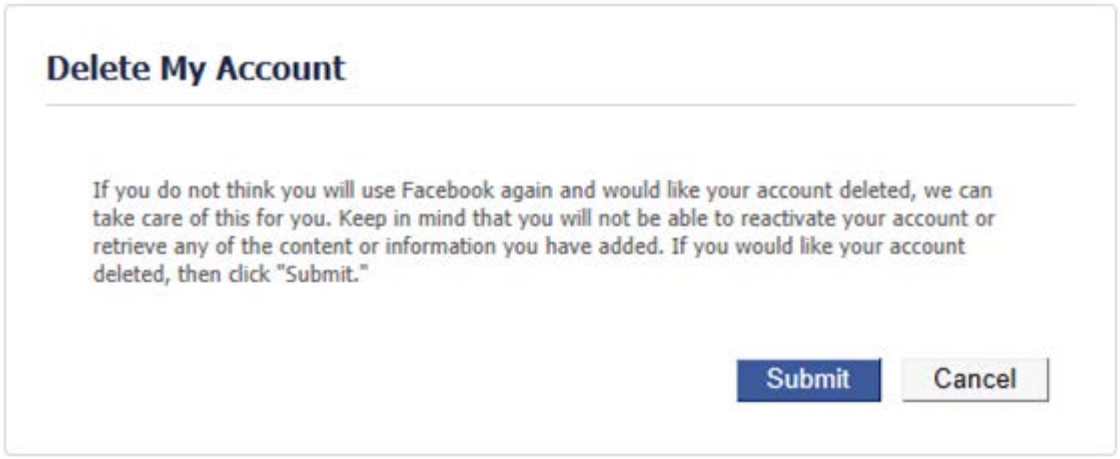
> "A couple of months ago, 24-year-old Austrian law student, Max Schrems, requested Facebook for all his personal data. The European arm of Facebook, based in Dublin, Ireland, was obliged to turn over this information, as they had to follow a European law that requires any entity to provide full access to data about an individual, should this individual personally request for it. Accordingly, Max received a CD containing about 1,222 pages (PDF files), **including chats he had deleted more than a year ago**, "pokes" dating back to 2008, invitations, and hundreds of other details."

I underlined the important part. Chats deleted over a year ago? So where is this information being stored? This says to me that Facebook is retaining this information somehow, somewhere. Certainly not as Facebook claims – "it is deleted in a manner similar to emptying the recycle bin on a computer." If that was the case, I would find it difficult to believe that Facebook would still be able to associate

deleted information with an account. In Facebook's defense, that statement above is prefaced by the words "When you delete IP content", so that may only refer to photos, videos, etc. Maybe Facebook doesn't consider messages, wall posts, and other communications as IP content. So it certainly may be possible to get this information back after it is deleted and it is relevant to a criminal or civil matter.

Is there no escaping Facebook?

Is there no way to permanently delete your account and messages? Even "deleting" your account on Facebook is merely marking it inactive. I have tested this many times and was even the case in the Lester v. Allied matter. Lester, on advice from his counsel, deactivated his account but was able to re-enable it allowing him to delete the 16 photos. I was able to find on Facebook, a way to permanently delete your account.



This seems like a dire warning but do you believe it? I am not sure I do.

Even if you do delete your account, what about the messages you sent to others? What lies in their e-mail accounts and Facebook pages?

Another area to find deleted Facebook information is the good ole' PC or smart phone. Facebook is typically accessed through a browser (or an app on a smart phone) and there may be remnants of deleted ESI on the device used to access the Facebook account.

Deactivation = Preservation?

One of my friends is getting a divorce and he deactivated his Facebook account. He did this after discussing it with his attorney because he did not want his wife or others poking around on his site. Currently, neither party is requesting information from Facebook, but deactivating ones account may be prudent in some situations. It is the ultimate form of preservation, like locking your FB account in a cement box. There are other benefits. It stops YOU from posting or messaging and creating new evidence. It stops "friends" from posting pictures or other items that may not be flattering to you and may damage your case.

Conclusion

If you or your client is in a situation where social media may be responsive or damaging it is best to preserve it; you have to. It may even be in your best interest to have an independent third party, like D4, assist with the preservation. We are currently utilizing some commercial tools and proprietary processes to capture social media sites in a read-only manner. We can then testify to the collection and preservation efforts, if necessary.

As social media continues to become a major part of our everyday lives and lines continue to blur between PC, smart phones, and the cloud, one must look to all sources of ESI to retrieve potentially responsive data whether it be active or deleted.