Handling Electronically Stored Information (ESI) from Social Networking Sites (SNS)

By Peter Coons, Senior Vice President, Digital Forensics Expert, D4, LLC

Table of Contents

Part I: Court Opinion On Social Networking Sites (SNS) Discoverability

by Peter Coons

Rule 26(b) of the Federal Rules of Civil Procedure ("FRCP"), entitled "Discovery Scope and Limits", states:

> "(1) Scope in General. Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any non-privileged matter that is relevant to any party's claim or defense – including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter. For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence. All discovery is subject to the limitations imposed by Rule 26(b)(2)(C)."

The above says it all. Facebook and other SNS information are discoverable if it is relevant to the claims or defenses in the case. A claim of privilege may be difficult as well, since the mere posting of information to a SNS means that at least one other person has access to it. The entire purpose of an SNS is sharing with others!

It may not be privileged, but it is somewhat private, so it is usually not appropriate to ask for everything on a person's FB or Twitter account. The request should be similar to that of e-mail or any other ESI. It should include a specific request for postings, communications, photos, etc. related to the claims or defenses of the matter.

You may now say to yourself – "Yes, I see your point but what about the Stored Communication Act, doesn't that protect my or my client's data?"

The SCA

The Stored Communication Act ("SCA") was passed by Congress in 1986 as part of the Electronic Communications Privacy Act. In a nutshell, the SCA's intention is to provide 4th Amendment-like protection for data stored by third-party service providers. Meaning the Government can't come in and force FB to hand over all the information it has on all its users without permission from a Court. Most people familiar with the SCA would agree that it is antiquated and is in serious need of an overhaul. The privacy protections afforded by the Act vary and are determined by whether the service provider is considered an electronic communication service ("ECS") or a remote computer service ("RCS") provider. In the present day these two classifications are difficult to delineate.

In the matter, Crispin v. Audigier (U.S. District Court for the Central District of Calif.), the Defendant sought information from the Plaintiff's MySpace and FB accounts. The Plaintiff sought to quash the subpoena for a number of reasons, including that it violated the SCA. The Court concluded any unopened messages or communications would allow for FB or MySpace to be branded an ECS as per the SCA definition, but once those messages were opened the service provider was acting as an RCS. Therefore, some components of the Plaintiffs pages were protected by the SCA, while others were not.

Confused?

Do you think an Act enacted in 1986, with arcane definitions, should be used to determine whether SNS information is discoverable in a proceeding? What else do we have to assist and guide the Courts? Perhaps after Congress solves the debt crisis they can move on to revamping the SCA.

EEOC v. Simply Storage Mgt. LLC (2010 Southern District of Indiana)

In this sexual harassment matter, the Defendants requested all content posted by the two lead plaintiffs. The EEOC did not protest the fact that information on SNS was discoverable or relevant, rather they took issue with the Defense's request for everything.

The position by the EEOC supports my statement above that SNS information is akin to any other ESI. The same basic discovery principles must be applied. Is it relevant? Is the request overly broad?

FRCP 26(b)(2)(c)

> When Required. On motion or on its own, the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that:
>
> > (i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive;
> >
> > (ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or
> >
> > (iii) the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.

The Court was split down the middle. While it agreed that Plaintiffs needn't hand over everything, it did not agree with the EEOC that their clients should be required to produce only communications that directly reference the matters alleged in the complaint. The Court defined the scope of relevance "any profiles, postings, or messages (including status updates, wall comments, causes joined, groups joined, activity streams, blog entries) and SNS applications for claimants Zupan and Strahl for the period from April 23, 2007, through the present that reveal, refer, or relate to any emotion, feeling, or mental state, as well as communications that reveal, refer, or relate to events that could reasonably be expected to produce a significant emotion, feeling, or mental state."

If it's locked down or marked Private then the Courts can't get it.

Wrong. A personal diary is potentially discoverable as it goes to state of mind and is often used in proceedings. If a person locks his or her account down so it is only viewable to a limited number of individuals that is not protection from discovery. In Leduc v. Roman and Murphy v. Perger, the Courts determined that locking down the accounts did not preclude discovery or requests for information from the SNS accounts. However, that does not mean that the opposing party has the keys to the kingdom. Parties should only produce and receive items that are relevant or that have been ordered for production by the Court.

As the Judge in the Leduc matter observed, "Facebook is not used as a means by which account holders carry on monologues with themselves."

You have no privacy on SNS. So don't think you do! And anything on the Internet will be there forever. Whether these statements are true or not, it is best to err on the side of caution.

How to find information on SNS or the Bebos and Buzznets

Now we can stop with the legal discussions and look at some ways to search for people on SNS.

What are the top sites? We all know about Facebook, MySpace, LinkedIn, YouTube and Twitter but what about Tumblr, Picasa, Flickr and WordPress?

According to Alexa.com the top ten sites (as of August 11, 2001):

So, half of the top ten are SNS. One could argue that Yahoo and Google are SNS as well. Certainly, one can leave messages, post comments, and ask questions on both Google and Yahoo.

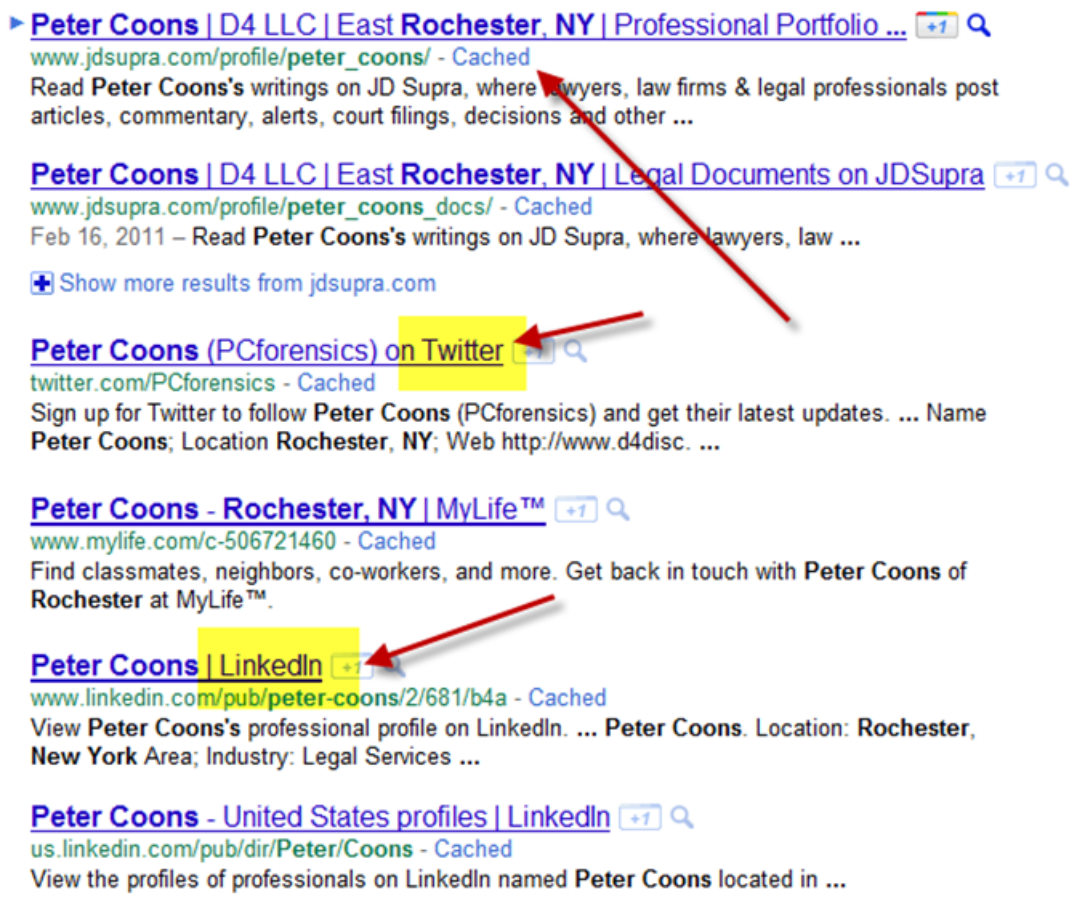
What about eBay? Would it be interesting to find out that a person that claims they are bed-ridden, but they just bought tickets to see Journey and REO Speedwagon and the week prior to that they purchased a treadmill? And then you see on their FB account, a status update that says "getting in shape for a journey." You can now put it all together. Far-fetched? Maybe.

What about new social networking sites? They are popping up all the time. Expect some big buzz around Google+ and FourSquare.
According to Wikipedia, foursquare is "a location-based social networking website based on hardware for mobile devices." The service is available to users with GPS-enabled mobile devices such as smartphones. Users "check-in" at venues using a mobile website, text messaging, or a device-specific application by running the application and selecting from a list of venues that the application locates nearby. Each check-in awards the user points and sometimes "badges." If you have not heard of foursquare that will likely change in the coming months. President Obama just signed up!
Google+, not yet fully available to the public, is a social networking service that was launched on 1/28/11. The New York Times have declared it Google's attempt to compete with Facebook.

The fact is that the SNS market will only grow. There will be the Facebooks and YouTubes of the world, but don't neglect the Bebos and the Buzznets.

The Usual Suspects
Use Google, Yahoo, and Bing. Search for full names of people. If you know someone's e-mail address or their username for a website, even better, Google it! Do not get this information illegally!

If I Google my name, Peter Coons, along with Rochester NY, I get the following:



You can quickly see I have articles on JD Supra, an account on Twitter, and a LinkedIn profile.

The next thing you can do is go to the sites themselves and run a search. Go to Facebook and see if you can locate the person. A quicker solution is to use a service like Spokeo. Spokeo.com is a paid service that allows one to put in a person's name, e-mail, username, or phone number to find out if they have any SNS accounts. Again, this is a paid service but it is very cool and scary! I put in my name and it told me when I was born, my phone number and it even had a picture of my house and knew how long I have lived there!

If you happen to identify someone's FB profile, feel free to browse anything that is open to the public. However, do not try to become that person's friend under false pretenses in an attempt to find out more about that person.

Pipl.com is another great (scary) site. Great because it provides a one-stop shop for searching SNS info about a person, in addition to other personal information.

I went to pipl.com and typed in my name and current city. It returned the name of my Dad, brother, my age, middle name, the fact that I used to live in Miami, Larchmont and New York City. Understand the scary part now?

In addition to Spokeo and Pipl, one can use the following sites to find out more about an individual:

1. Snitch.name
2. Yoname.com
3. Socialmention.com
4. Folowen.com
5. Samepoint.com
6. Google Social Search

All are decent sites. If you have the time and some patience, the amount of "personal" information available on the Internet is astounding. Try it for yourself using some of the sites above.

Conclusion

In this first part we discussed some legal issues, as well as, ways to find people on SNS.

Social networking is now an undisputable part of our everyday lives. We should be cautious about what we say, do, or place on social networking sites. It's not only for our eyes or for the eyes of the intended recipients. It could end up as evidence in a legal proceeding.

Now that we know SNS information is potentially discoverable and where to find it, how do we go about preserving it? That's part two.

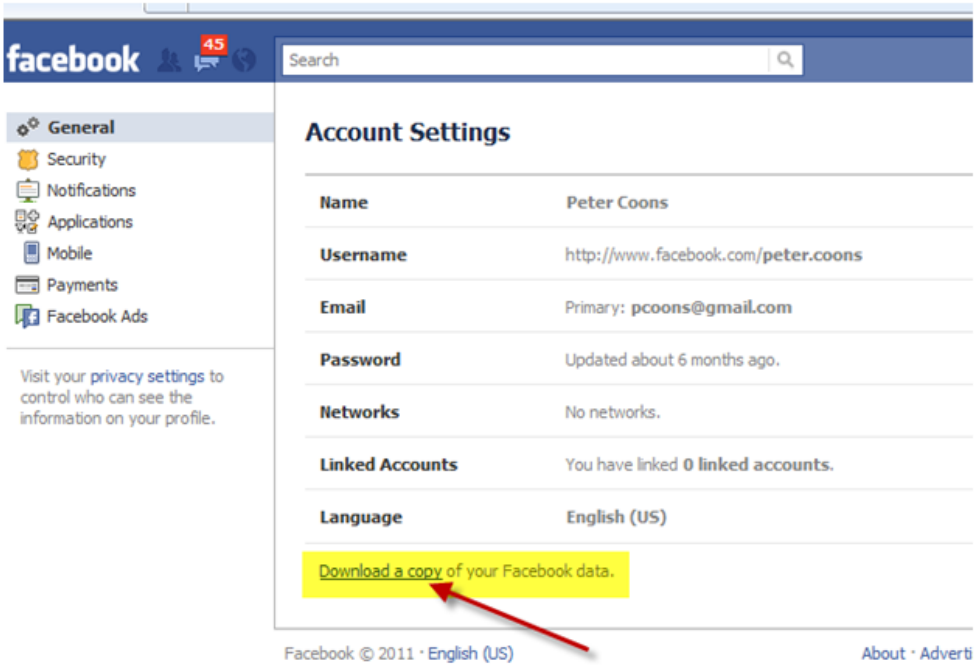
Now that we know SNS information is potentially discoverable and where to find it, how do we go about preserving it?

Preserving SNS

Preservation is a critical phase of discovery. It is important to ensure that it is done in a timely and proper fashion. Since the SNS Facebook never deletes your information (as of this writing), even if you disable the account, one may choose to preserve in place. But when it comes time to gather the information from a site like FB, there are a few options.

Capturing Facebook

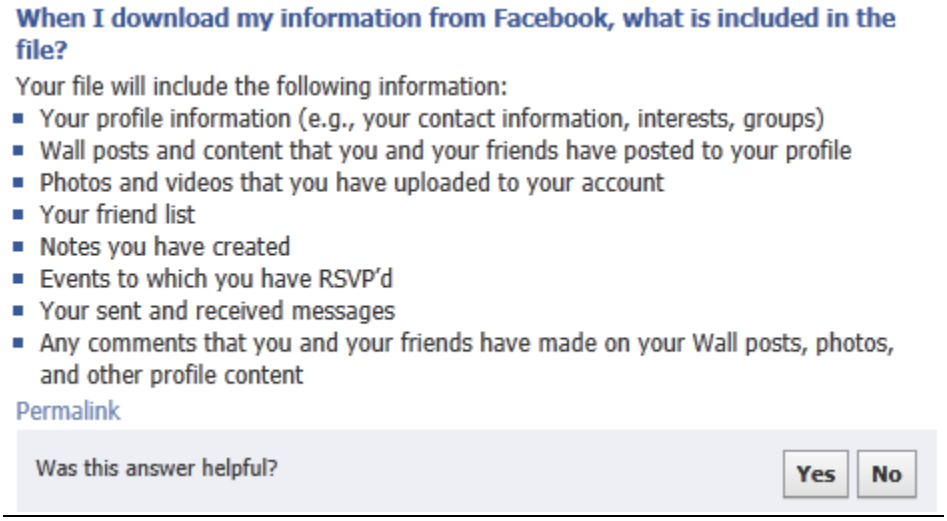
I went in and reactivated my account on FB to check out the "Download a copy" feature.



This feature was added in 2010. It's a nice-to-have feature in the eDiscovery world.

Once I clicked on the "Download a copy" link, it took me to another screen where it prompted me to start the archive. I said OK and then a message popped up and told me I would receive an email once the archive was completed. This is a nice security feature.

So what does the archive actually archive?



When I download my information from Facebook, what is included in the file?

Your file will include the following information:

- Your profile information (e.g., your contact information, interests, groups)
- Wall posts and content that you and your friends have posted to your profile
- Photos and videos that you have uploaded to your account
- Your friend list
- Notes you have created
- Events to which you have RSVP'd
- Your sent and received messages
- Any comments that you and your friends have made on your Wall posts, photos, and other profile content

Permalink

Was this answer helpful? Yes No

That is a lot of information that is potentially responsive or discoverable in a litigation or investigation.

A few minutes later…

I checked my Gmail account for the FB e-mail. I waited a few minutes more…ahhh, there it is.

The e-mail had a link where I was prompted to download a zip file that contained all my private FB information.

So now I guess I am done if I was ordered to hand over all my FB material. Right? Maybe. It would be a good practice to review the contents and ensure that everything that may be discoverable or potentially responsive was delivered in the zip file. Ask your legal counsel.

Of course to get all this great information you must own the account or have the owner's permission.

It would be nice if all SNS had such a feature. They don't. So then what? A couple simple methods may be to use screenshots or manually download photos or other material from the site in question.

Just GrabIt

Let's use Linkedin as an example next. If I wanted to capture information about John Smith on LinkedIn (make sure it is the right John Smith), I may choose to use Windows print screen function to snap a screenshot and then document the date and time. One could also use a nifty tool like SnagIt. SnagIt is a screen capture tool that allows for one to add text, comments, arrows, etc.

Since I don't know this John Smith, I redacted all his information. I don't want to give him free press. Regardless, all of his information and more are freely viewable to anyone with a LinkedIn account. LinkedIn even provides a PDF or Print function for this page. I could now take this screenshot, along with a detailed log that includes the date and time of the screenshot, the exact web address, the username that I was logged in as, etc. I could also create an MD5 hash of the file.

Other tools on the market purport to create screenshots of web pages (including SNS) and automatically create hashes of the pictures, with a date and time stamp. It's only a matter of time before there are more tools in the market space that make it easier to "snap" a shot of a person's SNS and use it as part of the authentication process.

Subpoena

Is it possible to subpoena records from an SNS? Yes, but you may only receive limited information unless you are the government. The below is right from FB's website:

> *"We may disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required by law. This may include respecting requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law under the local laws in that jurisdiction, apply to users from that jurisdiction, and are consistent with generally accepted international standards. We may also share information when we have a good faith belief it is necessary to prevent fraud or other illegal activity, to prevent imminent bodily harm, or to protect ourselves and you from people violating our Statement of Rights and Responsibilities. This may include sharing information with other companies, lawyers, courts or other government entities."*

What you need for a FB subpoena in a civil matter: **A valid California or Federal subpoena**

What you get: **Usually basic subscriber information (not content)**

What does FB say?

> *"Federal law prohibits Facebook from disclosing user content (such as messages, Wall 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.*
>
> *If a user cannot access content because he or she disables or deleted his or her account, Facebook will, to the extent possible, restore access to allow the user to collect and produce the account's content. Facebook preserves user content only in response to a valid law enforcement request."*

Nice Fish or "doveryai no proveryai"…

You can tell a lot from a picture. This is my FB profile picture.

What you can tell from this picture:

1. I am a Buffalo Bills fan…sad, but true
2. I have a silver salmon in my hand (if you know your fish)
3. I am on a boat
4. There are mountains behind me

What you can't tell from this picture:

1. Where this picture was taken (It was Alaska)
2. Who caught the fish (I did)
3. The year this picture was taken (2006)

My point is that you shouldn't jump to conclusions. Let's say I was suing someone for an injury suffered in an accident in 2010 and I was claiming that I couldn't fish anymore. Well, someone may jump on my FB account and see this picture and use it as evidence that I am lying. See where I am going with this? As Ronald Reagan famously stated, "doveryai no proveryai"…Trust, but Verify!

How do we even know this is a picture of Pete Coons? Or that Peter Coons setup this account?

In the past year I assisted a client with a matter that involved someone creating a fake Facebook page using my client's name, photos of her, etc. The fake profile had her hometown identified correctly, her place of work, and her birthdate. There was no reason to think it was not her account. The perpetrator made false and inflammatory statements on the fake page in attempt to deface my client. In the end, I referred my client to the local authorities. So yes, this does happen!

In the matter Griffin v. State, 2011 Maryland, the defendant Antoine "Boozy" Griffin was charged with murder. In the second trial (first was a mistrial) a witness claimed he was threatened by the Boozy's girlfriend. As evidence, the State submitted the girlfriend's My Space page as evidence. The girlfriend's alleged page gave her hometown, her birthday, etc. In testimony, an officer that stated that he believed it to be the girlfriend's legitimate account because of the information and pictures on the account. In addition there was a posting that said "FREE BOOZY!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!"

The trial judge admitted the evidence.

On appeal, the Maryland Court of Appeals reversed Boozy's conviction. Some of the commentary of the higher court included…"anyone can create a fictitious account and masquerade under another person's name or gain access to another's account by obtaining the user's username and password."

The Court chastised the State for not:

1. Questioning the girlfriend about the post
2. Examining the girlfriend's computer
3. Contacting MySpace for more information about the account

Trust, but verify! Where's the Gipper when you need him?

In Closing

No matter what method you choose for persevering SNS info, remember these 8 key tips:

1. Document your process (dates, times, who captured the info) – this is true of any preservation and collection endeavor
2. The person that preserves may be the person that testifies about the process
3. Know the tool or method being used and its shortcomings
4. Know what you get and don't get by using the FB "download a copy" method
5. Don't gain access to an account illegally or through nefarious means
6. Don't assume an account belongs to someone just because it says it does – verify it, if necessary and possible!
7. Don't assume anything about pictures since you don't know when they were taken! Verify it, if necessary and possible!
8. I am not a lawyer so none of this is legal advice. Only nerd advice.

In Part III of this series I will discuss the final part of the discovery process; hosting, review and production of SNS ESI.

Part III: Reviewing Electronically Stored Information (ESI) on Social Networking Sites (SNS)

by Peter Coons

In the first two parts of this series on SNS and eDiscovery we discussed the Why, What and How. The third part will address the "OK, we identified and collected it, now what?" part.

Social Networking Sites (SNS) data is just like any other ESI. That is not such a bold statement since the data that results from an SNS collection may include e-mail messages, documents, photos, blogs, web pages, etc. These are all items we in the eDiscovery world have been dealing with for years. However, there are some differences that may make it difficult to review the information in a meaningful context, if not collected properly.

For example, in Part II of this series I mentioned one could request data from Facebook through the "Download a copy" feature. If you recall, FB made a zip file available with the contents of my FB account. Part of those contents included comments that others made about photos that I had uploaded to my account. Here is an example:

August 1, 2008 at 10:20 am
Looks very familiar. Were they trying to get you to roll down the hill Like Jacob and Molly were doing to me?? LOL!
August 2, 2008 at 12:16 am

That's it? What photo is my friend discussing?

Here is that same comment with a meaningful picture.

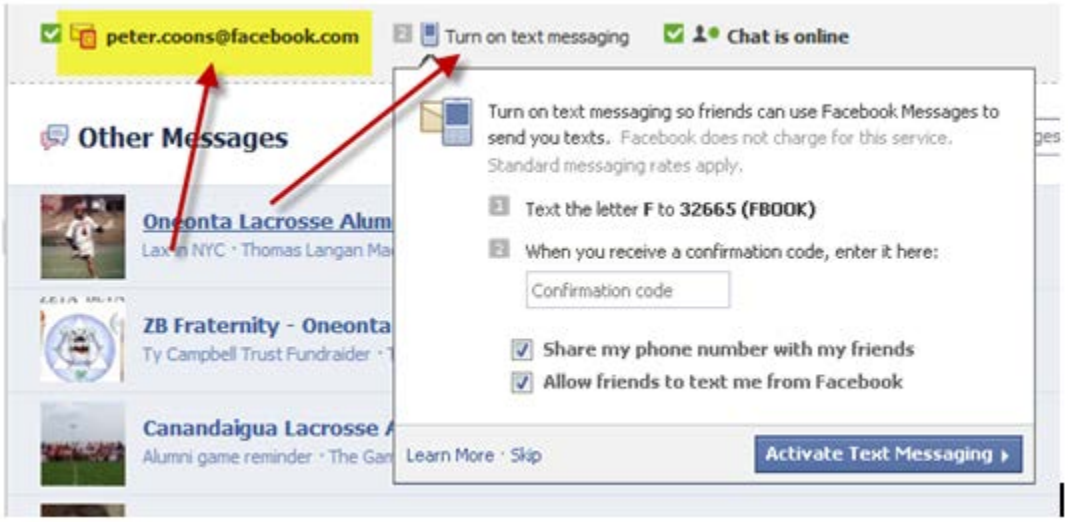
This pertains to my point in Part II of this series, that one must ensure all the important parts of the FB account are included in the zip file.

Sort of off topic, since this section is about reviewing SNS data, but also related…

Review Starts at Collection

Prior to the collection, one must be thinking about the review process and what items need to be reviewed:

1. Is it only photos? What about comments re: the photos?
2. Do instant messages need to be captured and reviewed? Make sure the texting parties involved can be identified.
3. Do e-mails need to be scooped up and reviewed? FB now lets a user receive his or her e-mail through the @facebook domain. Same with TEXTS from phones!



FB users can be contacted through texts and @facebook domain.

Take the example above where there is a comment and no photo attached. Think about a case where an insurance company is investigating a person claiming to be incapacitated, yet that person has photos on his/her FB page with daring exploits of skydiving or snowboarding. Just seeing a comment that says, "Wow, amazing", means little if one cannot see that the comment is referring to someone doing a "triple lindy" off a diving board.

"Click" – Simple Method for Capture and Review

One way to review SNS data is by reviewing screenshots that have been properly collected and documented.

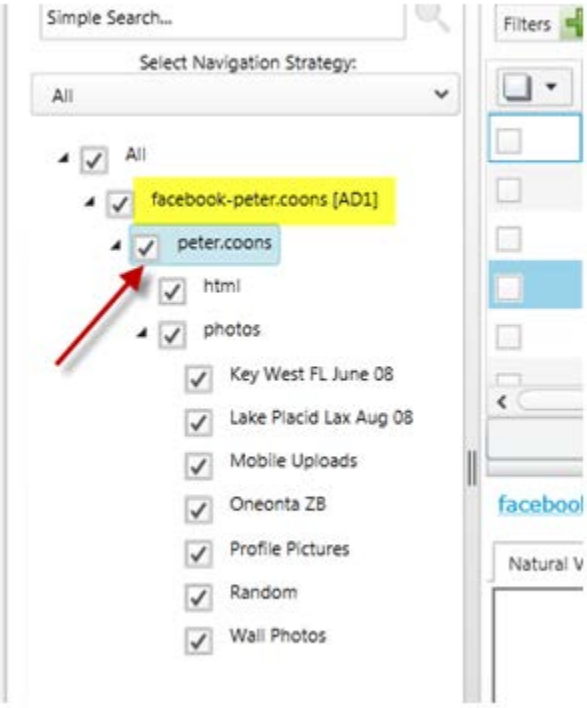
Screenshot of Peter Coons FB group page "Oneonta Lacrosse Alumni" taken 9/2/11 at 3:40 PM Eastern. Viewed through IE 8 browser. – snagit screenshot capture tool used. MD5 Hash 123456EFA546879

The above may be one way to document the date, time, and other stats about the screenshot.

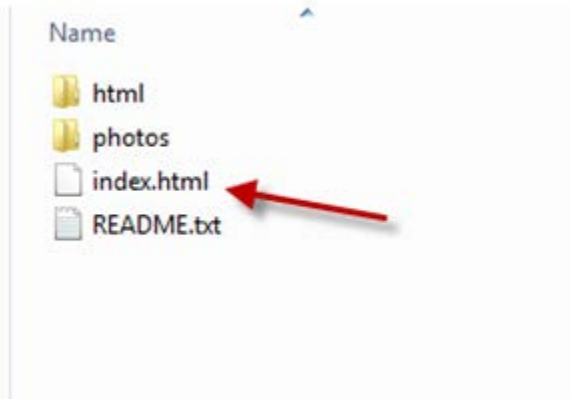
Screenshots are a great way to see what a page looked like on a given day through a given browser.

What's better is that those screenshots (saved as picture files) can be organized by custodian and site, prior to being loaded into a review tool, such as Summation or Relativity. They become just like any other ESI waiting for review, tagging, and possible production.

Below is a screenshot of my FB data in AccessData's Lab web review tool.

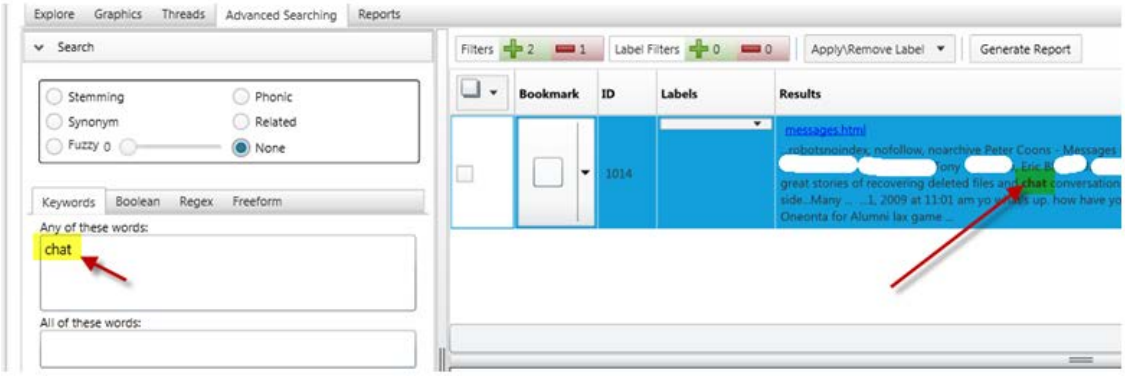


ABOVE: Facebook data organized by custodian.

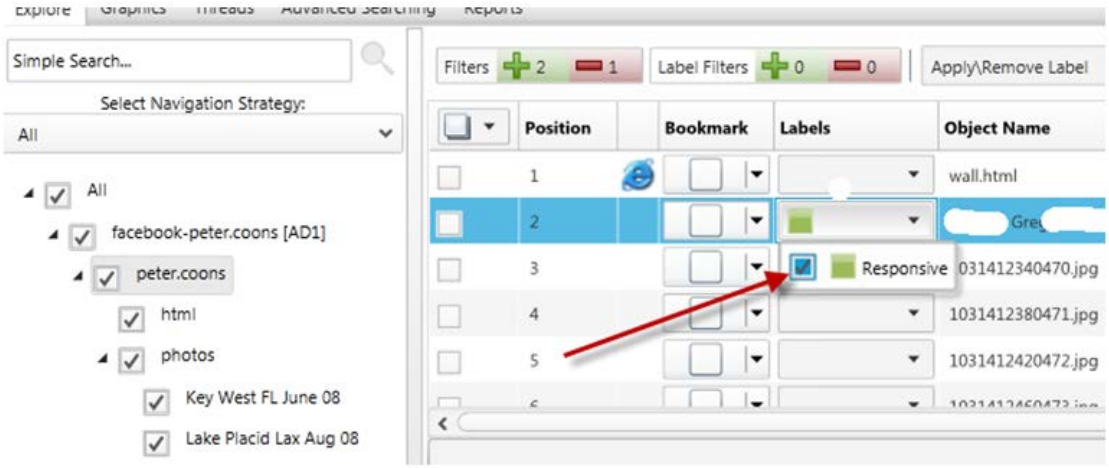


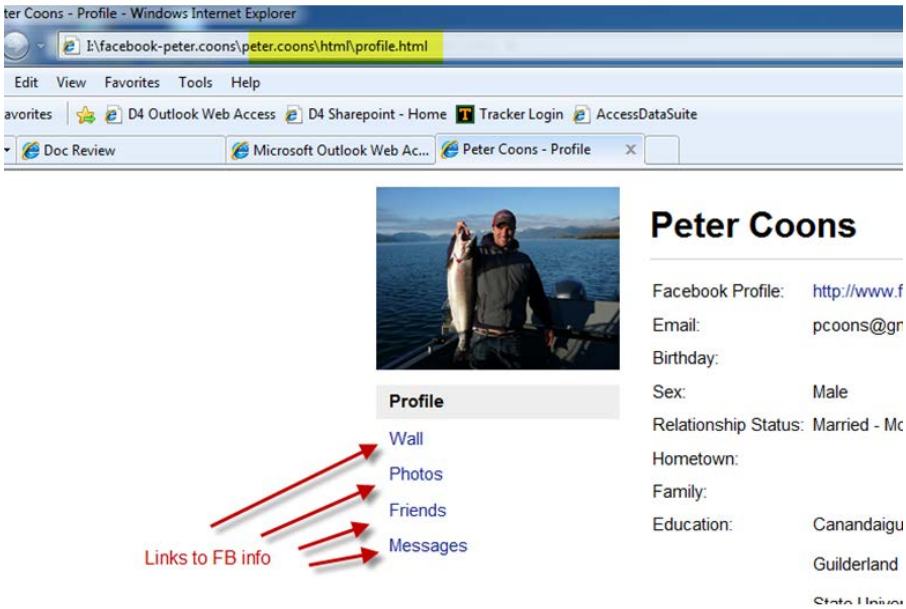
To be fair to FB and its download feature – when the file is downloaded it is a nice, mini FB website. If one clicks on the index.html file it should launch the archived FB site.

The screenshot below depicts how that same FB data can be indexed and searched like any other ESI. However, this may not be true of data captured via screenshot. Since screenshots are pictures, they may not be text searchable without converting the picture to text (if possible).



The screenshot below shows how one can tag a FB photo responsive just as any other ESI.





If one clicked on the links noted above with red arrows, one would see a graphically stripped down version of my FB site. However, it would have the comments next to the appropriate photos.

If one were to simply load this data into a review tool without knowing it was a mini FB site then the links would be essentially broken and one may not get a clear view of the FB site. This goes back to my point of knowing what you are collecting, how it is being collected, and how it will be reviewed.

In Conclusion

Here are some tips to remember when thinking about reviewing SNS data:

1. **Think about the review stage at the time of collection.** Ask yourself what is important to retrieve from the person's SNS and how do I…
    a. …want to review it
    b. …want to have it tagged?
    c. …want to produce it?
    d. …redact it if necessary?
    e. …ensure I can authenticate the evidence?
1. **Think about the site that is being collected from and find out if they have any auto-download functionality for the content.** If they do, what is the output? Will the output fit nicely into my review tool?
2. **What review tool am I going to use** and do they have any built-in support for SNS?
3. **Have I verified the vendor or individual collecting the data** will maintain a base level of organization by custodian and site?
4. **Have I verified the individual or vendor preserving the ESI** has experience with SNS collections?
5. **Have I discussed the form of production for SNS with opposing counsel?** What is acceptable?
6. **Do I even need a review tool** because I am only reviewing FB data for one custodian and the "Download a copy" feature provided me with a sufficient mini FB site?