"Evidence and Hearsay for the Family Lawyer"

March 19, 2013

PRESENTERS:

The Honorable William Ward
Elizabeth Warner Altman
Hilary Bendik
Roslyn Berger
Barbara Cymerman
Nicole Boyle Kairys
Sibyl McNulty
Barbara Payne
M. Farley Schlass
Michael Steinberg

qubit
a publication on computer forensic and e-discovery issues
August 2011

Defendant's Computer Printout of Facebook Messages Excluded as Evidence: Authentication Requires Corroborating Facts

By Susan A. Ardisson, Esq.

Authenticating electronic evidence such as email, text messages and Facebook postings offer unique challenges for parties and the courts. Recently, in *State v. Eleck*, 2011 WL 3278663 (Conn.App. August 9, 2011), the court held that authentication requires more than simply printing out a copy of the proffered Facebook postings. As impeachment evidence in *Eleck*, defense counsel sought to introduce a printout from the defendant's computer of his Facebook account showing that the state's key witness had "friended" him on Facebook and sent him three messages following the crime he was charged with committing. The witness denied sending the messages to the defendant, claiming her computer had been "hacked." Although skeptical of the witness' veracity, the appellate court affirmed the trial court's exclusion of the Facebook messages holding that the defendant was required "to advance other foundational proof to authenticate" that the messages came from the witness herself and "not simply from her Facebook account."

In this case, the defendant was charged and convicted of aggravated assault involving an altercation at a party which resulted in multiple stabbings of two victims, and was sentenced to five years' imprisonment. At the trial, the state's key witness testified that prior to the party, the defendant told her that if anyone "messed" with him, he was "going to stab them." On cross-examination by defense counsel, the witness testified that she had not communicated by telephone or computer with the defendant since the incident. For purposes of impeachment, the defendant testified that she had both "friended" him on Facebook after the incident, and sent him three messages on Facebook, including the message that "the past is the past," and attempted to offer into evidence a printout from his computer containing the Facebook message. The defendant also subsequently testified the witness had removed him as a Facebook "friend" after his testimony. The witness then testified that she hadn't sent any of the messages to the defendant and that her Facebook account had been "hacked." The court suggested that the witness' claim was "dubious under the particular facts at hand, given that the messages were sent before the alleged hacking of the account took place…" Notwithstanding this skepticism, the court stated that the witnesses' "testimony highlights the general lack of security of the medium and raises an issue as to whether a third party may have sent the messages via [her] account."

"To impeach the witness' testimony, the defendant testified that she had both 'friended' him on Facebook after the incident, and sent him three messages on Facebook, including the message that 'the past is the past.'"

The *Eleck* court began its legal analysis by noting that there were no appellate decisions directly on point in Connecticut, and cited *In Re F.P.*, 878 A.2d 91 (Pa.Super. 2005) a Pennsylvania Superior Court case

This issue of qubit and past issues are available on our website at: www.bit-x-bit.com

Defendant's Printout of Facebook Messages Excluded as Evidence

(from p. 1)

for the principle that electronic communications (in that case instant messages) can be properly authenticated within the existing framework of the rules of evidence. On this point, the *Eleck* court stated:

> We agree that the emergence of social media such as e-mail, text messaging and networking sites like Facebook may not require the creation of new rules of authentication with respect to authorship. An electronic document may continue to be authenticated by traditional means such as the direct testimony of the purported author or circumstantial evidence of "distinctive characteristics" in the document that identify the author.

The *Eleck* court, however, added that "the circumstantial evidence that tends to authenticate a communication is somewhat unique to each medium." See e.g. *People v. Clevenstine*, 891 N.Y.S.2d 511 (2009) [MySpace messages authenticated by police retrieval of conversations from victim's hard drive and testimony that the defendant had created the account sending the messages.]

In this case, because the state's witness testified that she had not sent the Facebook messages to the defendant, the trial court properly ruled that "it was incumbent on the defendant, as the proponent, to advance other foundational proof to authenticate that the proffered messages did, in fact, come from [the witness] and not simply from her Facebook account."

The defendant argued on appeal that the exchange of messages with the witness was "distinctive evidence of the interpersonal conflict between" them, i.e. the witness' statement that "the past is the past." The appellate court, however, rejected this argument stating that more was required, and cited numerous cases where additional "distinctive" evidence was offered including *United States v. Safavia,* 435 F. Supp.2d 36, 40 (D.D.C. 2007) (distinctive content of email messages included discussions of identifiable personal and profession matters) and *Dickens v. State*, 927 A.2d 32 (Md.App. 2007) (threatening text messages on victim's cell phone contained details "few people" would know and were sent from the defendant's cell phone in his possession at the time).

According to the *Eleck* court, the exchange of Facebook messages "could have been generated by any person" using the witness' account and did "not reflect distinctive information that only [the witness] would have possessed regarding the defendant or the character of their relationship." The court also pointed out that distinctive evidence of the author could have been provided by "forensic computer evidence." Accordingly, the appellate court concluded that "the reference...to an acrimonious history, with nothing more" did not sufficiently establish that the witness had "authored the messages such that it would be an abuse of discretion to exclude [them]."

"According to the* Eleck *court, the exchange of Facebook messages 'could have been generated by any person' using the witness' account and did 'not reflect distinctive information that only [the witness] would have possessed regarding the defendant or the character of their relationship.'"

◊ ◊ ◊ ◊ ◊

For questions or comments regarding this issue of qubit, please contact us at info@bit-x-bit.com.

qubit \'kyü -bit\ n. a quantum bit, the counterpart in quantum computing to the binary digit or bit of classical computing. Just as a bit is the basic unit of information in a classical computer, a qubit is the basic unit of information in a quantum computer. *whatis.com*

AN OVERVIEW OF COMMONLY USED SOCIAL MEDIA

FACEBOOK (https://www.Facebook.com)

Facebook is a social networking service co-founded by Mark Zuckerberg that was launched in February 2004. As of September 2012, there were one billion active users, more than half of them using Facebook on a mobile device. The United States accounts for the most users worldwide, with about 168.8 million members or 53.97% of all worldwide users. According to the Nielsen Media Research study released in December 2011, Facebook is the most accessed website in the United States, behind Google.

Users can create profiles with photos, lists of personal interests, contact information, and other personal information. Users can communicate with friends and other users through private or public messages and a chat feature. They can also create and join interest groups and "like pages".

Facebook has affected the social life and activity of people in various ways, including the ability to stay continuously in touch with friends, relatives and other acquaintances wherever a person is in the world, as long as there is internet access. It also unites people with common interests and or beliefs through groups and other pages. Facebook has also had a political impact as when Facebook teamed up with ABC and Saint Anselm College before the 2008 New Hampshire primary. Facebook also allows politicians and campaign organizers to understand the interests and demographics of their Facebook fan bases, as with Wisdom for Facebook, to better target voters. Facebook retains a proprietary interest in the information that has been shared.

To address fears about privacy, Facebook allows users to choose their own privacy settings and choose who can see specific parts of their profile. Facebook requires that users give their true identity, a demand that MySpace does not make; however, a teacher was just arrested for "Catfishing" on Facebook in that he pretended to be a female and young boys sent explicit photos to him.

Facebook requires that users be at least thirteen (13) years old, but a study in the online journal *First Monday* found that parents consistently enable children as young as ten (10) years old to sign up for accounts, directly violating this policy. The 1998 Children's Online Privacy Protection Act (COPPA) requires that a minor aged 13 or younger must obtain parental consent to access commercial websites. In the study 1,000 households were surveyed and 76% of parents reported that their child joined Facebook when he or she was younger than 13. Facebook currently removes 20,000 people a day, including many underage users.

In November 2012, several Facebook users reported that their accounts were hacked and their profile pictures were replaced with pornographic images. For more than a week, users' news feeds were spammed with pornographic, violent and sexual content. It has been reported that more than 200,000 accounts in Bangalore, India were hacked, but Facebook has denied these claims.
In December 2008, the Supreme Court of the Australian Capital Territory ruled that Facebook is a valid protocol to serve court notices to defendants. It is believed that this was the world's first legal judgment that defines a summons posted on Facebook as legally binding. In March 2009, the New Zealand High Court allowed for the serving of legal papers on Craig Axe of the company Axe Market Garden via Facebook.

In *Trail v. Lesko,* No. GD-10-017249, the Honorable R. Stanton Wettick, Jr., in his opinion and order of Court took the opportunity to address the issue of defendants seeking access to Plaintiff's Facebook profiles. Judge Wettick identified and discussed Pennsylvania cases in which parties have requested access to information on Facebook. Judge Wettick's opinion contains a description of how the information placed on Facebook is transmitted and stored (Case included in materials). Judge Wettick denied the discovery requests of both parties asking for access to the other party's Facebook pages.

In Part III of his opinion, Judge Wettick summarizes the following Pennsylvania cases relating to discovery motions and Facebook issues. The disposition of each case is included and comments are included for some of the cases.

McMillen v. Hummingbird Speedway Inc., 2010 WL4403285, No. 113-2010 CD (Jefferson C.P. Sep.9, 2010) (Foradora, P.J.). Because the public profile on Facebook indicated that there might be relevant information that would impact this personal injury suit, the court directed the plaintiff to provide the defendant's counsel with the login and password information on a read-only basis. No information was to be divulged to any defendants in the case unless pursuant to a further order of court.

Zimmerman v. Weis Markets, Inc., 2011 WL 2065410, No. CV-09-1535 (Northumberland C.P. May 19, 2011) (Saylor, J.). On the basis of information contained in the publicly available information , the court concluded that it was reasonable to infer the existence of additional relevant information within the private portion of the plaintiff's profile. Although the court ordered the plaintiff to provide the defendant with all login and password information, the court did note that the order should not be construed as a blanket entitlement to this type of information.

Largent v. Reed, 2011 WL 5632688, No. 2009-1823 (Franklin C.P. Nov. 8, 2011) (Walsh, J.). The court granted access to Facebook information, making the point that if the party seeking discovery is able to articulate in good faith that further discovery will lead to relevant discovery. The court also said that because

non-public information posted is shared with third parties ("friends"), there is no reasonable privacy expectation. The court reasoned that the since the very purpose of Facebook is to share information with others, that purpose abrogates any claim of privilege.

Arcq v. Fields, No. 2008-2430 (Franklin C.P. Dec. 2011) (Herman, J.). Access denied because the defendant had not articulated some reasonable, good-faith basis for believing the private profile contained relevant information. The mere fact that the plaintiff had an account was categorically insufficient to justify the discovery sought by the defendant.

Martin v. Allstate Fire & Casualty Ins. Co., Case ID 1104022438 (Phila. C.P. Dec. 13, 2001) (Manfredi, J.). Access to Facebook denied because the defendant failed to make any threshold showing that the plaintiff's profile might contain relevant information.

Kennedy v. Norfolk Southern Corp., Case ID 100201473 (Phila. C.P. Jan. 4, 2011) (Tereshko, J.). Motion denied.

Kalinowski v. Kirschenheiter, No. 2010-6779 (Luzerne C.P. 2011) (Van Jura, J.). Motion denied, but the plaintiff was ordered to refrain from deleting any content from his profile.

Piccolo v. Paterson, No. 2009-04979 (Bucks C.P. Marc. 2011) (Cepparulo, J.). Motion denied because the defendant failed to establish a threshold need for the information or articulate any prejudice that could result from nondisclosure.

Gallagher v. Urbanovich, No. 2012-33418 (Montgomery C.P. Feb. 27, 2012) (Carpenter, J.). The defendant was ordered to provide plaintiff's counsel with the requested information for a period of seven days. Judge Wettick considers this to be the outlier as access was granted without any factual basis for an investigation or what an investigation of the account might uncover.

TWITTER (https://twitter.com/)

Twitter is an online social networking service and microblogging service that enables its users to send and read text-based messages of up to 140 characters, known as "tweets". It was created in 2006 and now has over 500 million registered users as of 2012, generating over 340 million tweets daily and handling over 1.6 billion search queries daily. Twitter is one of the ten most visited websites on the Internet, and has been described as the "SMS (Short Message Service) of the Internet". Unregistered users can read tweets, while registered users can post tweets through the website interface SMS, or a range of apps for mobile devices.

Users can group posts together by topic or type by use of hashtags, which are words or phrases prefixed with a "#" sign. Similarly, the "@" sign followed by a username is used for mentioning or replying to other users. To repost a message from another Twitter user, and share it with one's own followers, the retweet function is symbolized by "RT" in the message. A word, phrase or topic that is tagged at a greater rate than other tags is said to be a *trending topic*. Trending topics become popular either through a concerted effort of Twitter users or because of an event that prompts users to discuss that event. The logo of Twitter is a bird that is said to be internationally identifiable. If Twitter experiences an outage, users see the "fail whale" error message. Twitter will censor hashtags that other users find offensive.

Twitter messages are public but users can also send private messages. Twitter collects personally identifiable information about its users and shares it with third parties and Twitter reserves the right to sell this information as an asset if the company changes hands.

Twitter has a verification program, which allows celebrities to get their accounts verified and has been used to verify accounts of businesses and accounts for public figures who do not tweet themselves, but wish to maintain control over their accounts.

Twitter has been used for a variety of purposes, such as, to organize protests ("Twitter Revolutions"), as a form of civil disobedience, as an emergency communication system for breaking news, and as a way of making television more interactive and social.

Twitter has had security breaches on several occasions and The Federal Trade Commission brought charges against Twitter which was settled in 2010. Twitter must maintain a information security program to secure users' private information. The US Department of Justice issued a subpoena in 2010 directing Twitter to provide information for accounts registered to or associated with WikiLeaks. Individual countries can now remove tweets selectively, i.e., anti-Semitic French tweets or neo-Nazi German tweets.

Tweets are publically visible by default, but senders can restrict message delivery to just their followers. Users can tweet via the Twitter website, smart phones, or by SMS in certain countries. Users may subscribe to other users' tweets. This is known as "following" and subscribers are known as "followers" or "tweeps". Users can also check the people who are un-subscribing them on Twitter better known as "unfollowing" in other services. Users also have the ability to block those who have followed them. Users can also update their profiles by using their mobile phones or using apps for certain smart phones and tablets.

The first unassisted off-earth Twitter message was posted from the International Space Station in January 2010. Twitter usage spikes during prominent events, such as sporting events, deaths of prominent celebrities (Twitter crashed after Michael Jackson died), and the Japanese New Year. Japan is more popular in Japan than Facebook. Since 2013, after Twitter acquired a video clip company, users can create and share six second looping video clips.

FOURSQUARE (http://foursquare.com)

Foursquare is a location-based social networking website for mobile devices, such as smartphones. Users "check in" at venues using a mobile website, text messaging or a devise-specific application by selecting from a list of venues the application locates nearby. Each time a user checks in, the user is awarded points and sometimes "badges".

Foursquare has approximately 20 million users and as of April 2012 there have been more than 2 billion check-ins. Users are encouraged to be hyper-local and very specific with their check-ins (i.e., a specific floor or a specific activity) while at a venue. Users can choose to have their check-ins posted on their accounts on Twitter, Facebook, or both. These check-ins can also notify friends of these updates and they are called "pings".

A user can be crowned "mayor" if a user has checked-in at a venue on more days that anyone else in the past 60 days. Foursquare confers "Superuser status" on users who have been selected by the staff for their helpful contributions to the community.

Companies can create pages of tips for users so that a user can follow the company and receive special expert tips when they check in at certain locations. Businesses (in excess of 750,000 of them) also use "Specials" that include discounts and freebies when you check in. Some stores now post the Foursquare sign on their door to attract new customers.

In February 2010, a site known as "Please Rob Me" was launched, which took data from public Twitter messages that had been pushed through Foursquare, to list people who were not at home. The purpose was to raise awareness about the potential thoughtlessness of location sharing.

PINTEREST (http://pinterest.com)

Launched in March 2010, Pinterest is a pinboard-style photo sharing website that allows users to create and manage theme based image collections, such as events, interests, hobbies, recipes and more. Users can upload, save, sort and manage images, known as pins, and other media content (i.e., videos) through

collections known as pinboards. Pinboards are generally themed so that pins can easily be organized, categorized and discovered by other users. Pinterest acts as a personalized media platform, whereby your own content as well as anyone else's uploaded pins can be browsed on the main page. Users can save their favorite pins to one of their own boards using the "Pin It" button and content found outside of Pinterest can also be uploaded to a board via the "Pin It" button.

Despite a slow start, in December 2011, the site became one of the top 10 largest social network services and in January 2012 the site had 11.7 million unique users. Most of the users are female. In March 2012 it was reported that Pinterest became the third largest social network in the United States behind Facebook and Twitter. Both Ann Romney and Michelle Obama created accounts during the 2012 campaign. Businesses create pages aimed at promoting their businesses online and shoppers seem to spend more money when accessing items through the company's pinboard rather than through the company's website.

Scammers have used Pinterest to promote surveys promising free products. Scam images, linked with well-known companies, offer incentives such as gift cards for completing a survey. Once the link in the description is clicked, users are taken to an external site and asked to re-pin the scam image. Victims are phished for their personal information and the free product is never delivered.

INSTAGRAM (http://instagram.com)

Instagram is an online photo-sharing and social networking service that allows its users to take pictures, apply digital filters to it, and share them on a variety of social networking services, including Facebook and Twitter. The photos are confined to a square shape, similar to Kodak Instamatic images.

Instagram has rapidly grown since its launch in 2010 to one hundred million users in January 2013. By May 2012, 58 photographs were being uploaded and a new user was added every second. On September 2012 Facebook bought Instagram for approximately $1 billion in cash and stock.

Instagram has an age requirement of 13 years old or older, restrictions against posting violent, nude/partially nude, or sexually suggestive photographs, and users must be responsible for their account and all activity conducted with it. Instagram does not claim any ownership rights to the content that users post on or through Instagram Services.

PLEASE NOTE: The above material has been condensed from information found on Wikipedia, the free encyclopedia. Each article contains extensive references, which have been omitted here.

July 2012

Preserving and Authenticating Social Media: Why Hitting "Download" Isn't a Defensible Process and May Result in the Exclusion of Valuable Electronic Evidence

By Joseph Decker, Esq. and Susan A. Ardisson, Esq.

The Problem with Printouts of Electronic Social Media Evidence

Consider the following scenario: Henry, the owner of a very successful three star restaurant, was sued for sexual harassment and age discrimination by Grace, a 42 year old sommelier, who was terminated for poor performance. Henry replaced Grace with Jane, who is 29 years old. At the initial client meeting, Henry informed his counsel that he had not harassed Grace, but in fact had rejected Grace's overtures, and had proof. According to Henry, Grace "friended" him on Facebook under the name "gracyluscious" and sent him at least three very suggestive posts six months earlier, to which he did not respond. Having clicked "download" Henry gave his lawyer a printout of his Facebook account which included the three posts from "gracyluscious." No electronic discovery was conducted by the parties, including any discovery regarding Facebook. At trial one year later, as impeachment evidence while cross-examining Grace, Henry's counsel attempted to introduce the suggestive Facebook posts from "gracyluscious." Grace denied having a Facebook account and denied having sent the posts to Henry. The Court rejected counsel's efforts to authenticate Henry's Facebook printout, and excluded the three "gracyluscious" Facebook posts. That evening, Henry checked his Facebook account, and found that there were no longer any posts from "gracyluscious." Henry couldn't recall the last time that he had viewed the "gracyluscious" posts on his Facebook account.

How the Courts See It - The Rules of Evidence

This all too common set of facts raises the pitfalls associated with the failure to properly preserve and authenticate electronic evidence from social media. As pointedly stated by the court in *Griffin v. State of Maryland*, 19 A.3d 415 (2011), "[t]he concern arises because anyone can create a fictitious account and masquerade under another person's name or can gain access to another's account by obtaining the user's username and password." A party's reliance on a download or printout of the electronic information from a particular type of social media may not provide an adequate foundation for the admission into evidence.

In *Griffin*, the Maryland Court of Appeals reversed a murder conviction because the trial court admitted evidence of a MySpace posting - "snitches get stitches"- allegedly made by Griffin's girlfriend, Jessica Barber. The prosecutor did not attempt to authenticate the MySpace posting through Ms. Barber, and instead offered the posting "snitches get stitches" through the police officer who had "downloaded" the MySpace page and provided a printout for the court. Outside the presence of the jury, the trial court accepted the testimony of the police officer's authentication of the "snitches get stitches" posting based on his viewing of the MySpace account which included the evidence that Ms. Barber's MySpace profile contained her photograph, references to her children and birthdate. The appellate court, however, found that the evidence did not amount to "sufficient distinctive characteristics" of a MySpace profile to authenticate the printout. The *Griffin* court concluded that:

> The potential for abuse and manipulation of a social networking site by someone other than its purported creator and/or user leads to our conclusion that a printout of an image from such a site requires a greater degree of authentication than merely identifying the date of birth of the creator and her visage in a photograph on the site in order to reflect hat Ms. Barber was its creator and the author of the "snitches get stitches" language.

Similar results have been reached by the courts in Connecticut and Massachusetts. See, e.g., *State of Connecticut v. Eleck*, 23 A3d 818 (Conn. 2011) [Facebook download and printout obtained by the defendant of key witness' Facebook messages purportedly sent to the defendant, which appeared to contain statements that would impeach witness's testimony, were properly excluded as evidence due to improper authentication] and *Commonwealth v. Williams*, 926 N.E.2d 1162 (Mass. 2010) [trial court properly excluded download of MySpace messages regarding a pending criminal case because there was no authenticating evidence regarding the security of the MySpace page or purported author's exclusive access].

In federal cases, authentication is addressed by Rules 901(a) and 901(b)(4) of the Federal Rules of Evidence. Rule 901(a) provides that at trial, the proponent of the evidence must offer "evidence sufficient to support a finding that the matter in question is what its proponent claims." Electronically stored information, such as evidence from Facebook, MySpace, Twitter and text messages, may be authenticated by offering evidence that would establish the "contents, substance, internal patterns or other distinctive characteristics."

Similarly, Pennsylvania Rule of Evidence 901(a) provides that "authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." Like the federal rule, Pennsylvania Rule of Evidence 901(b)(4) provides for evidence of "distinctive characteristics and the like." Notably in *In re F.P.*, 878 A.2d 91 (Pa.Super.Ct. 2005), the appellate court stressed that there is:

> no justification for constructing unique rules for admissibility of electronic communication such as instant messages; they are to be evaluated on a case-by-case basis as

any other document to determine whether or not there has been an adequate foundational showing of their relevance and authenticity.

[The *F.P* court affirmed the trial court's admission of threatening instant messages where circumstantial evidence included purported author's accusations, threats against the recipient of instant messages, reference to theft of DVD, and calling the recipient "vile" names.]

The Solution: Proper Collection and Preservation of Social Media

What should our fictitious counsel in the Henry- Grace case have done to avoid the exclusion of valuable impeachment evidence at trial, and how can these evidentiary issues be avoided in the future?

1. Proper Collection of Social Media Evidence: Instead of relying on Henry's paper printout, which he tucked away in a file, Henry's counsel should have arranged for collection of his Facebook account in electronic form at the outset of the litigation, and requested in discovery that Grace also preserve her Facebook account in electronic form in a forensically sound manner. With the use of proper forensic collection tools, all available Facebook metadata is preserved, validating "hash values" are generated, and a defensible chain of custody is maintained throughout the capture and export, thereby providing evidence of "distinctive characteristics" for authentication purposes. Additionally, Harry could have established that the alleged posts were sent to him during a time period important to the events in question, thereby providing further evidence of "distinctive characteristics" for authentication of Grace's posts.

2. Preservation of Metadata Fields: When Facebook and other social media are properly collected and preserved, multiple potentially relevant metadata fields are preserved. The metadata fields may be searched for relevant evidence and also serve to authenticate the electronic evidence to be offered at trial. See, e.g. *Lorraine v. Markel American Insurance Company*, 241 F.R.D. 534, 547 (D.Md. 2007). The available metadata fields for Facebook include: user account ID; URL (the web address) of where the user profile image is located; the created date of a message or post; when a post or message was revised or updated; all the recipients of a message identified by name; all the recipients of a message identified by user ID; unique numeric identifier for posted photographs or videos; and unique numeric identifier for each wall post and more.

3. Addressing "Hacking" Claims and Other Denials: Failing to properly preserve and seek discovery of social media like Facebook, allows witnesses like our fictional Grace, and the witnesses in *Griffin* and *Eleck*, to claim that either they did not create the Facebook account or did not post or send the message(s) at issue. Such arguments can, however, be easily countered by (1) proper collection and preservation of the accounts through pre-trial discovery; and/or (2) a forensic examination of the author's computer. For example, a forensic examination of Grace's computer, including a review of information in the unallocated areas of her computer where deleted items and evidence of web pages resides and web browser cache, would likely reveal information establishing the creation of her "gracyluscious"

Facebook account, as well as fragments of web pages containing drafts of the three posts sent to Henry. Such additional electronic evidence offered by a computer forensic expert should serve as evidence of "distinctive characteristics" sufficient to authenticate the proffered Facebook posts.

4. Disappearing Facebook Posts or Messages: If the parties fail to properly preserve the electronic data contained in their Facebook accounts at the outset of the litigation, or as soon as litigation is reasonably likely, then recovery of deleted posts can raise challenging issues for the parties. In the case of deleted wall posts, once the account user deletes a post on a wall, then that the post is deleted from all of the Facebook accounts/users that originally received it, and cannot be recovered from the recipients' Facebook accounts. However, as noted above, a forensic examination of the unallocated space on the computer, which was used to create or view the account and postings, may well reveal additional corroborating evidence of the creation and sending of the posts. Email messages sent via Facebook, and subsequently deleted by the sender/account holder, however do not "disappear" from recipients' accounts. Like all web based email and domain based accounts, the email messages are retained by the recipients until deleted by the recipients or automated email deletion process.

5. Searching for Relevant Evidence: Had Grace and Henry preserved their respective Facebook accounts at the commencement of litigation, as potential repositories of electronically stored information, both accounts could have been searched for other potentially relevant metadata which would establish when Grace created and posted the suggestive dates, and when Henry received the suggestive posts. Additionally, Grace's Facebook could have been searched for other potentially relevant evidence such as email and postings sent to "friends" regarding Henry or his restaurant. With the proper tools, the search and review and can be restricted to certain dates, acceptable to the parties, and a protocol established to protect privacy interests and other concerns.

Social media is an important source of evidence. It cannot be overlooked in discovery. However, admissibility at trial should not be assumed simply because a paper copy was printed. A paper printout of social media postings may not contain the corroborating evidence of "distinctive characteristics" necessary to clear the initial hurdle of admissibility – authentication. A properly preserved and captured electronic version of the social media posting provides much more information than a paper copy, and could be crucial in satisfying the requirements of authentication at trial.

IN THE COURT OF COMMON PLEAS OF ALLEGHENY COUNTY, PENNSYLVANIA

HOWARD TRAIL, individually and as Administrator of the ESTATE OF JESSICA TRAIL, deceased, SUE TRAIL, TAMMIE GRICE, individually and as Administratrix of the ESTATE OF WILLIAM GRICE, deceased, MICHAEL TRAIL, and AMANDA DELVAL,

Plaintiffs

vs.

TIMOTHY LESKO and PITTSBURGH LODGE NO. 11 BENEVOLENT AND PROTECTIVE ORDER OF ELKS, a Pennsylvania Corporation, t/d/b/a B.P.O.E. PITTSBURGH LODGE 11,

Defendants

CIVIL DIVISION

NO. GD-10-017249

OPINION AND ORDER OF COURT

HONORABLE R. STANTON WETTICK, JR.

Counsel for Plaintiffs:

Matthew D. Racunas, Esquire
Law Offices of Patricia L. McGrail, LLC
1714 Lincoln Way
White Oak, PA 15131

Counsel for Defendant, Timothy Lesko:

Joseph A. Hudock, Jr., Esquire
Suite 2400 Gulf Tower
707 Grant Street
Pittsburgh, PA 15219

Counsel for Defendants, Pittsburgh Lodge No. 11 Benevolent and Protective Order of Elks, t/d/b/a B.P.O.E. Pittsburgh Lodge 11:

James W. Young, Jr., Esquire
Terrance R. Henne, Esquire
Suite 150
5500 Corporate Drive
Pittsburgh, PA 15237

OPINION AND ORDER OF COURT

WETTICK, J.

I.

The subjects of this Opinion and Order of Court are the motion of Michael Trail seeking access to defendant Timothy Lesko's *Facebook* profile and defendant's motion seeking access to plaintiff Michael Trail's *Facebook* profile.

I am responsible for discovery disputes in General Docket cases that are not on a trial list. Within the past year, defendants are far more frequently presenting motions seeking access to the plaintiffs' *Facebook* profiles.[1]

Usually, I have disposed of these motions through rulings from the Bench (frequently acceptable to both parties).

In order that I may provide a context for the arguments presented by counsel and the implications of my rulings involving the discovery of *Facebook* content, I have included, at Part II of this Opinion, a brief discussion of what *Facebook* is, how it is used, and what information is available to its users.

In Part III of this Opinion I identify and discuss the Pennsylvania cases in which parties have requested access to information on *Facebook*.[2]

---

[1]There are other social networking sites. However, *Facebook* has been the subject of the discovery requests presented to me.

[2]To date, no Pennsylvania appellate court has addressed discovery requests for information contained within an individual's *Facebook* profile.

In Part IV of this Opinion I discuss selected opinions of other state courts and federal courts pertaining to the discovery of *Facebook* content.

In Part V of this Opinion I deny plaintiff's and defendant's motions, which are the subject of this Opinion and Order of Court, because of the protections that Pa.R.C.P. No. 4011(b) affords *Facebook* content.

II.

Social networking sites[3] are web-based services that allow individuals to construct a public or semi-public profile within a bounded system, choose from a list of other service users with whom they intend to share a connection, and navigate among those connections and those made by others within the system. Users create a unique user identity, establish relationships with others who have done the same, join communities of users who share connections, and exchange information among one another.[4]

Social networking sites like *Facebook* utilize "Web 2.0" technology, which allows users to create and edit content on a web page while interacting with other users simultaneously in real time.[5] With respect to *Facebook*, an individual initially creates a

---

[3]Although there are numerous sites that fit this classification, this discussion is limited to *Facebook*, which is the largest and most heavily trafficked on the web.

[4]Evan E. North, Comment, *Facebook Isn't Your Space Anymore: Discovery of Social Networking Websites*, 58 U. KAN. L. REV. 1279, 1284 (June 2010). Among the law review articles on the subject, student authors tend to offer the more detailed accounts of the functioning of social networking platforms.

[5]This participatory platform is in contrast to antecedent, Web 1.0, which is produced, edited, and maintained by a single publishing entity. Consider, for example, any run-of-the-mill website, which unilaterally publishes information online for their users' passive perusal. Megan Uncel, Comment, *Facebook Is Now Friends with the Court: Current Federal Rules & Social Media Evidence*, 52 JURIMETRICS J. 43, 46 (Fall 2011).

"profile," which functions as a personal web page and may include, at the user's discretion, numerous photos and a vast array of personal information including age, employment, education, religious and political views and various recreational interests. Once a profile is established, the user is encouraged to connect with other *Facebook* users - so-called "Friends" - with whom they exchange limited access to their respective profile pages and the ability to post pictures, comments and other content thereon.[6] Each time content is posted directly to a user's profile page, the recipient user has the administrative capability to delete the offered content from his or her own profile.

In a departure from the control generally afforded a user over the content of his or her own profile page, *Facebook* employs a system whereby users may "tag" others in photographs and other content, thereby establishing a link from that content to the tagged user's profile page.[7] For example, User A uploads a photo to his or her own profile page of several individuals including User B. User A "tags" User B in the photo. Once tagged, the photo on User A's profile page will contain a link directing individuals to User B's profile.[8] While User B's profile will indicate that he or she has been tagged in User A's photo, and the tagged photo will unwittingly appear among the pictures that User B has selected for publication on his or her own profile page.[9]

---

[6]In this Opinion, I briefly discuss some of the more relevant aspects of the *Facebook* user interface; for a more detailed description see Megan Uncel's comment, *supra* n. 5 at 46-50.

[7]See Daniel Findlay, Comment, *Tag! Now You're Really "It" What Photographs On Social Networking Sites Mean For the Fourth Amendment*, 10 N.C.J.L. & TECH. 171 (Fall 2008).

[8]Access to User B's profile will be governed by User B, who can opt to restrict access to his or her page to only Friends, Friends of Friends or, at the least restrictive level, the public at large. Self-regulated privacy settings are discussed briefly, *infra*.

[9]A user who has been tagged has the ability to "untag" the photo and, by altering *Facebook*'s default privacy settings, may restrict the class of individuals who are authorized to view tagged content. However, even if untagged or if otherwise restricted by our tagged user,

Finally, any time any user posts content to their own or their Friends' profile pages, this information appears in the user's and user's Friends' "news feeds." The news feed provides a constantly updating display of activity among the user and the user's Friends. From this page, the user will be notified any time a Friend is tagged in an item, posts a status update or a news story, or comments on another's content.[10]

The sheer volume of potentially relevant information is staggering.[11] In the aggregate, users collectively update their "statuses" (a short indication of what's on a user's mind at a given moment, posted to the their own profile page) more than 60 million times each day. Individual users create on average 90 pieces of content every month (photos, status updates, comments or other posts) with fully half of all *Facebook* users accessing their individual profiles on a given day.[12] Facebook users collectively upload 300 million photos to the site each day.[13]

---

the photo will be available for viewing on the page of the user who initially posted it. Only the user who posted the photo is able to remove it from the website altogether. Once a Friend posts a photo of our user, any Friends of the posting user, including our user (or opposing counsel armed with our user's login information), may peruse Friends' photos to locate any material, including unauthorized material.

[10]The purpose of the news feed feature is to facilitate a user's awareness of Friends' online activities without necessitating their constantly visiting each Friend's profile page sequentially. The average *Facebook* user has 130 Friends, and may even have Friends numbering in the thousands. See North, *supra* n. 4, at 1285.

[11]Although not relevant to the current question and, therefore, not addressed herein, sites like *Facebook* collect and store "metadata" about their users, which might reveal more about an individual's use of the site, their Friends' identities, what a user saw on another user's profile, and may track a user's general Internet activity. All of this data is potentially discoverable under the proper circumstances. See Derek S. Witte, *Your Opponent Does Not Need A Friend Request to See Your Page: Social Networking Sites & Electronic Discovery*, 41 MCGEORGE L. REV. 891 (2010).

[12]Uncel, *supra* n. 5 at 49.

[13]*Facebook* has gone public, and in the April 23, 2012 amendments to its S-1 SEC filings, the company disclosed that monthly active users now number 901 million; daily active

Not all information posted on *Facebook* by a user is universally public, viewable by anyone with an Internet connection or even all other *Facebook* subscribers. By adjusting *Facebook*'s default privacy settings, each user is empowered to limit the classification of persons (and, in some cases, specific individuals) who are permitted access to a user's profile page and the content contained therein. Although some information is always considered public and accessible to everyone,[14] other information is accessible only by those people to whom the user grants access, usually limited to the user's Friends or Friends of those Friends. Finally, users can exchange messages not unlike traditional email, which, like email, are only accessible to the sender and recipients.

III. PENNSYLVANIA CASES[15]

McMillen v. Hummingbird Speedway Inc., 2010 WL 4403285, No. 113-2010 CD (Jefferson C.P. Sep. 9, 2010) (Foradora, P.J.). The defendant collided with the plaintiff during the final "cool down lap" in a stock car race The plaintiff sought damages from Hummingbird, Inc., the corporate owner of the racetrack where the alleged injuries occurred. The plaintiff claimed substantial injuries including possible permanent

---

users 526 million; monthly mobile users 500 million; users post 300 million photos per day; 3.2 billion likes and comments are recorded each day, and; 125 billion "Friendships" have been forged.

[14]In addition to information the user chooses to make public, *Facebook* considers publicly available the user's name, profile picture, username or user ID and network. See *Facebook* Data-Use Policy, http://www.facebook.com/about/privacy/your-info.

[15]Because these cases are unpublished, because many are simply court orders absent any accompanying rationale, and because most Pennsylvania counties do not maintain electronic dockets, I was compelled to rely on other traditional media outlets including the PITTSBURGH POST-GAZETTE and the PENNSYLVANIA LAW WEEKLY. As a result, the citations, in places, are incomplete.

impairment, loss and impairment of general health, strength and vitality and an ongoing inability to enjoy certain pleasures in life. Upon review of the publicly accessible portion of the plaintiff's *Facebook* profile, the defendant discovered the plaintiff's comments about a fishing trip and his attendance, as a spectator, at another race in Florida. Thereafter, the defendant sought to compel the production of the plaintiff's user name and password to gain access to the private portions of the plaintiff's profile under the assumption that more relevant information might be contained within.

Because the public profile indicated that relevant information might be contained in the private portion showing that the plaintiff's injuries were exaggerated, and because no privilege exists between mere Friends (and even if it did, any privilege was waived once the information was shared with others), the court directed the plaintiff to provide the defendant's counsel with the login and password information on a read-only basis. No information was to be divulged to any defendants in the case unless pursuant to further order of court.

•

Zimmerman v. Weis Markets, Inc., 2011 WL 2065410, No. CV-09-1535 (Northumberland C.P. May 19, 2011) (Saylor, J.). The plaintiff injured his leg while operating a forklift and sought damages including lost wages, lost future earning capacity, pain and suffering, scarring and embarrassment. He claimed to have sustained permanent diminution in the ability to enjoy life's pleasures and permanent impairment to his general health. The plaintiff's public *Facebook* profile indicated that he enjoyed "bike stunts" and contained photographs of the plaintiff posing with a black eye and his motorcycle taken both before and after the accident. Furthermore, despite

allegations that the plaintiff was embarrassed to wear shorts due to the scar which resulted from his injury, the plaintiff's public profile contained a photograph of the plaintiff in shorts, his scar clearly visible.

On the basis of the foregoing, publicly-available information, the court concluded that it was reasonable to infer the existence of additional relevant information within the private portions of the plaintiff's profile. Although the plaintiff contended that he had a reasonable expectation of privacy in this information, the court ruled that the plaintiff consented to share the information when he created the account and voluntarily posted information. Moreover, the plaintiff placed his physical condition at issue in the case, and, as a result, the defendant was entitled to conduct discovery thereon.

Although the court ordered the plaintiff to provide the defendant with all login and password information without further limitation, the court did note that the order should not be construed as a blanket entitlement to this type of information in all personal injury cases. Rather, the court limited its holding to requests based on some factual predicate gleaned from the publicly available pages, requiring some threshold showing that the public portions contain information that suggest additional relevant postings are likely to be found within the non-public portions. Fishing expeditions, the court noted, would not be authorized.

•

Largent v. Reed, 2011 WL 5632688, No. 2009-1823 (Franklin C.P. Nov. 8, 2011) (Walsh, J.). The plaintiff was injured when the motorcycle on which she was a passenger collided with the defendant's van. As a result of the accident, the plaintiff claimed serious and permanent physical and mental injuries, pain and suffering. During

her deposition, the plaintiff testified that she had an active *Facebook* profile and had accessed it as recently as the previous evening, but refused to provide defense counsel with her login and password information. In the defendant's motion to compel, the defendant argued that the plaintiff's profile was recently public and that certain posts contradicted the plaintiff's severe injury claims. Specifically, the defendant claimed that the plaintiff had posted "several photographs that show her enjoying life with her family and a status update about going to the gym."

As a threshold matter, the court found the information sought clearly relevant and discoverable in light of the plaintiff's testimony that she suffers from depression and uses a cane to walk as such information might prove that the plaintiff's injuries were exaggerated. Furthermore, because non-public information posted on *Facebook* is shared with third parties, there is no reasonable privacy expectation. Indeed, the court reasoned, the very purpose of *Facebook* is to share information with others, which purpose abrogates any claim of privilege.[16]

Like the court in *Zimmerman*, *supra*, the *Largent* court limited its holding to those instances whereby the party seeking discovery is able to articulate in good faith that further discovery will lead to relevant information. On the foregoing bases, the court ordered the plaintiff to provide the defendant with her login and password for a period of 21 days, after which time the plaintiff would be permitted to change her password to preclude any further access to her account by defense counsel.

---

[16]The plaintiff also argued the Stored Communications Act ("SCA"), Pub. L. No. 99-508, 100 Stat. 1848 (1986), codified at 18 U.S.C. §§ 2701 *et seq*, prohibited the disclosures sought by the defendant. The SCA regulates service providers, not individuals. Therefore, although the Act might preclude *Facebook* from disclosing information directly to the defendant in response to a civil subpoena (citing *Crispin v. Christian Audigier, Inc.*, 717 F.Supp.2d 965 (C.D. Cal. 2010)), the plaintiff could not claim the protection of the SCA because that Act does not apply to individuals.

•

Arcq v. Fields, No. 2008-2430 (Franklin C.P. Dec. 2011) (Herman, J.). The plaintiff was injured in an automobile accident and sought damages for, *inter alia*, continuing medical care, disfigurement and infertility. The defendant, upon learning that the plaintiff had a *Facebook* account, requested the plaintiff's login and password information.

The court, noting the paucity of Pennsylvania authority, reviewed the few instances whereby the courts had granted similar requests and determined that each was predicated on a showing that the public portions of the subject profile contained some relevant information that established a gateway to the non-public pages. Thus, the court denied the defendant's discovery request because the defendant had not articulated some reasonable, good-faith basis for believing the private profile contained relevant information. The mere fact that the plaintiff had an account was categorically insufficient to justify the discovery sought by the defendant.

•

Martin v. Allstate Fire & Casualty Ins. Co., Case ID 1104022438 (Phila. C.P. Dec. 13, 2011) (Manfredi, J.). The plaintiff suffered serious injuries as a pedestrian when she was struck by a passing car and sought damages for physical injury, pain, trauma, humiliation, anxiety, and mental anguish. At her deposition, the plaintiff was asked whether she had a *Facebook* account and, upon affirmation, for her password. The defendant moved to compel the login and password information, citing the plaintiff's lack of privilege and the absence of any reasonable expectation of privacy. The plaintiff opposed the defendant's motion to compel on the ground that the defendant never

asked how the plaintiff used the site or whether she commented on or posted photographs of her injuries. Thus, the defendant failed to make any threshold showing that the plaintiff's *Facebook* profile might contain relevant information. The court denied the defendant's request without amplification.

•

Kennedy v. Norfolk Southern Corp., Case ID 100201473 (Phila. C.P. Jan. 4, 2011) (Tereshko, J.). The plaintiff sought damages for personal injuries including loss of life's pleasures in connection with a vehicle collision with a train. At his deposition, the plaintiff indicated that he enjoyed shooting skeet with his children prior to the accident but was no longer able to do so. On the public portion of his *Facebook* profile, his interests included "shooting" (among others such as "Starbucks" and "Breast Cancer Awareness"). Although the defendant argued that the inclusion of "shooting" among his interests on his public profile was inconsistent with his deposition testimony, the court denied the defendant's motion without further explanation.

•

Kalinowski v. Kirschenheiter, No. 2010-6779 (Luzerne C.P. 2011) (Van Jura, J.). The plaintiff was injured in a car accident. He alleged that his injuries limited his ability to perform his job and other daily activities, and, because he could no longer drive long distances, his ability to travel was similarly limited. The defendant learned at the plaintiff's deposition that the plaintiff had a *Facebook* page and requested his login and password information. In support of its motion to compel, the defendant claimed that one picture available on the plaintiff's public page depicted the plaintiff "lounging comfortably, on a bar stool with one foot up on another barstool." Presumably because

the public content was not sufficient to impeach the plaintiff's claims, the court denied the defendant's request without prejudice (or explanation) but ordered the plaintiff to refrain from deleting any content from his profile.

•

Piccolo v. Paterson, No. 2009-04979 (Bucks C.P. Mar. 2011) (Cepparulo, J.). The plaintiff was injured while a passenger in the defendant's vehicle, sustaining severe lacerations to her face which required at least two surgeries and multiple subsequent laser treatments to repair the scarring. At her deposition, defense counsel asked if the plaintiff would accept his "Friend request," thereby allowing him access to the photographs on the plaintiff's non-public profile on the same footing as her other "Friends." After the plaintiff denied this request, the defendant moved for an order requesting only access to photographs. The plaintiff had already provided numerous photographs taken both before and after the accident. Furthermore, the defendant apparently failed to establish a threshold need for the information or articulate any prejudice that could result from nondisclosure. The court denied the request without an accompanying opinion.

•

Gallagher v. Urbanovich, No. 2010-33418 (Montgomery C.P. Feb. 27, 2012) (Carpenter, J.). The plaintiff, who was assaulted during a recreational soccer game, moved to compel the defendant's *Facebook* login and password information. Although the plaintiff did not point to anything in the defendant's public profile to trigger access to the non-public pages, and did not appear to have any articulable expectation of what a search of the defendant's *Facebook* profile might reveal, the court, without discussion,

ordered the defendant to provide the plaintiff's counsel with the requested information for a period of seven days after which time the plaintiff would be denied further access to the defendant's profile.

•

As the foregoing cases suggest, the Courts of Common Pleas that have considered discovery requests for *Facebook* information appear to follow a consistent train of reasoning. The courts recognize the need for a threshold showing of relevance prior to discovery of any kind, and have nearly all required a party seeking discovery in these cases to articulate some facts that suggest relevant information may be contained within the non-public portions of the profile.[17] To this end, the courts have relied on information contained in the publicly available portions of a user's profile to form a basis for further discovery.

IV. OTHER JURISDICTIONS

The decisions of other state and federal courts are largely in line with the Pennsylvania case law. As in Pennsylvania, courts elsewhere agree that content posted by the plaintiff on *Facebook* is not privileged, either because communications with Friends are not privileged or because, if the communications were privileged, such privilege was waived by sharing the content with others. Also like the Pennsylvania courts, other jurisdictions disfavor "fishing expeditions" and tend to require some factual

[17] *Gallagher v. Urbanovich*, *supra*, is the outlier. In that case, the court granted a plaintiff's request for the defendant's *Facebook* username and password without the plaintiff's identifying any factual basis for an investigation or representing any expectation of what that investigation might uncover.

predicate suggesting the existence of relevant information prior to ordering access to the sought-after information. See e.g. *Tompkins v. Detroit Metropolitan Airport*, 278 F.R.D. 387 (E.D.Mich. 2012) (because the publicly available information was not inconsistent with the plaintiff's claims, further discovery was denied as overly broad); *Mackelprang v. Fidelity Nat'l Title Agency of Nevada, Inc.*, 2007 WL 119149, No. 06-cv-00788 (D.Nev. Jan. 9, 2007) (regarding email-type communications on a social networking site, because the defendant based its request for production on nothing more than suspicion or speculation as to what information might be contained within, the request was denied).

Unlike our Common Pleas Court cases, however, other jurisdictions have wrestled to establish a middle ground between the wholesale denial of the request on the one hand and the granting of unlimited access to the user's profile on the other. Thus, some jurisdictions, when faced with these questions, fashion more narrowly tailored discovery orders and are more likely to rely on counsel to peruse the client's profile for relevant information in the first instance.

One federal district court, faced with a request for production from a plaintiff who was claiming certain emotional damages in an employment discrimination case, defined the issue as follows:

> ...the main challenge in this case is not one unique to electronically stored information generally or to social networking sites in particular. Rather the challenge is to define appropriately broad limits - but limits nevertheless - on the discoverability of social communications in light of a subject as amorphous as emotional and mental health, and to do so in a way that provides meaningful direction to the parties.

EEOC v. Simply Storage Mgmt., 270 F.R.D. 430, 434 (S.D. Ind. 2010). After concluding that the content was not shielded from discovery simply because the plaintiff had made such content private, and that such information must be produced when relevant to a claim or defense, the court ordered production on the basis that the plaintiff's allegations of severe emotional distress rendered some *Facebook* content relevant, and discovery of this magnitude is the inevitable result of alleging these sorts of injuries.[18]

Rather than ordering complete access to the plaintiff's *Facebook* profile, however, the court defined a relevant period, from the time of the alleged harassment to the present, and ordered the plaintiff to provide all verbal communications (comments, status updates, group memberships, *et cetera*) that reveal, refer or relate to any emotion, mental state or feeling or to events that could reasonably be expected to produce significant emotion, feeling or mental state. The plaintiff was then ordered to produce only those photos depicting the plaintiff during the relevant time period, which the plaintiff posted on the plaintiff's profile. The court concluded that photos of the plaintiff in which she was "tagged" after being uploaded by a third-party, were not sufficiently relevant to warrant disclosure. Similarly, photos depicting someone other than the plaintiff would generally be considered outside the scope of the order.

Pursuant to the court's order, the plaintiff's counsel would make the initial determination of relevance in producing the information, and further inquiry into what was and was not produced would be permitted at the plaintiff's deposition. See also *Held v. Ferrellgas, Inc.*, 2011 WL 3896513 (D.Kan. Aug. 31, 2011) (Slip Op.) (postings

[18]The court explicitly limited its decision to cases involving severe emotional distress, stating that the proper scope of discovery might be different in "garden variety emotional distress claims."

from the period of alleged harassment are relevant, and privacy concerns are mitigated by the fact that the defendant only wants the information, not access to the account).

Finally, a small minority of courts have reviewed *Facebook* content *in camera* so the reviewing court may assess its relevance. See, e.g., *Loporcaro v. City of New York*, 2012 WL 1231021, No. 100406/10 (Richmond Cnty. N.Y. April 9, 2012) (Slip Op.), where the court concluded that the plaintiff had no reasonable expectation of privacy in the content posted on her *Facebook* profile and ordered the information be provided for the court's review.

Also see *Offenback v. L.M. Bowman Inc.*, 2011 WL 2491371, No. 10-cv-1789 (M.D.Pa. Jun. 22, 2011), where, after *in camera* review in which the court found some of the information relevant and other information not relevant, the court admonished the parties to conduct their own reviews in the future, given that the plaintiff is in a better position to determine what content is responsive and, if necessary, to object to the disclosure of other, potentially relevant information. See also *Zimmerman*, *supra*, where the Pennsylvania court declined an invitation for *in camera* review as an "unfair burden to place on the Court" and which would require "the Court to guess as to what is germane to defenses which may be raised at trial."

V. PLAINTIFF TRAIL'S AND DEFENDANT LESKO'S DISCOVERY REQUESTS

This case arises from an accident which occurred on September 26, 2009 after defendant, Timothy Lesko, attended a "Gun Bash" event at the Pittsburgh Elks Lodge No. 11. Plaintiff, Michael Trail, is claiming serious injuries from the accident, and defendant has claimed he was not the driver and does not know who may have driven

the vehicle. Plaintiff and defendant have filed cross motions to compel access to each other's *Facebook* accounts.

A. Plaintiff's Motion to Compel

Because defendant in his most recent Answer and New Matter (Feb. 22, 2012) asserted the defense that he was not the driver of the vehicle and does not recall who drove the vehicle, plaintiff urges that any postings surrounding the time period at issue are relevant in determining defendant's whereabouts or in uncovering any potential witnesses who could shed light on the events in question. Some of these posts may have been deleted and are, therefore, in *Facebook*'s sole possession.

In support of plaintiff's assertion that such information may be contained within defendant's non-public profile or among the content deleted from that profile, plaintiff offers the following: (1) after receiving plaintiff's interrogatories seeking information contained on defendant's social networking sites, plaintiff avers that defendant removed, deleted and/or altered significant portions thereof; (2) at approximately 12:01 P.M. on the day of the accident defendant purportedly posted "gun bash today now where is randy at" on his publicly accessible profile page; (3) another status update on defendant's profile, time-stamped 1:38 P.M. on the day of the accident, reads "Gun bash time" followed by a brief dialogue from which it may be inferred that defendant planned to attend the event with someone referred to as "dp," and; (4) a status update posted on defendant's page at 6:33 P.M. two days after the accident, which reads:

> to everyone who left me a line i thank you and your support means everything to me i just came home today and I am hurtin but like i said before thankyou everyone it means alot

> to me to all of you guys you never know just be careful i wouldnt wish this on anyone

(Errors in the original).

As a result of defendant's foregoing verbal representations and plaintiff's (apparently unsubstantiated) belief that defendant may have altered or deleted significant portions of other relevant information, plaintiff seeks access to defendant's profile and the authorizations necessary to compel *Facebook* to provide any deleted content.

However, in Defendant's Response to Plaintiff's First Request for Admissions (Apr. 27, 2012), defendant admitted that he was driving the car, was intoxicated, crossed the center line and that plaintiffs were both seriously injured and not themselves at fault, which admissions render the sought-after information seemingly irrelevant. Indeed, within a month of filing his Answer disclaiming liability, defendant explicitly conceded liability in his Brief in Opposition to Plaintiff's Motion to Compel at 4 (Mar. 21, 2012) wherein he stated, "there is no issue as to defendant's liability." Thus, none of the information which plaintiff seeks would be relevant to the only issue that remains in this case - damages.

Plaintiff does not argue that the information which he seeks is relevant to a punitive damages claim.[19] Furthermore, it is unclear why any information on defendant's *Facebook* profile would be relevant to a punitive damages claim as to this defendant who has admitted that he was driving while intoxicated with a .226% blood alcohol level.

---

[19]Plaintiff does not contend that information on Mr. Lesko's *Facebook* profile is relevant to his claim against the Pittsburgh Elks Lodge No. 11.

B. Defendant's Motion to Compel

Defendant asserts that because plaintiff avers in his complaint that "he may suffer great physical pain," "be disabled or limited in his normal activities," and "his general health, strength, and vitality have been seriously impaired and this impairment is possibly permanent," defendant is entitled to access plaintiff's *Facebook* profile, because of the possibility that defendant will find relevant information concerning the extent and severity of plaintiff's injuries.

In support of this request, defendant has attached two photographs obtained from the public portion of plaintiff's profile, which depict plaintiff (1) "at a bar socializing" and (2) "drinking at a party." These photographs do not contain any information as to when they were taken or uploaded. Furthermore, plaintiff has not alleged he is bedridden or that he is otherwise unable to leave the home, and the attached photographs are not inconsistent with plaintiff's alleged injuries.

SUMMARY

I base my rulings on Pa.R.C.P. No. 4011(b) which bars discovery that would cause "unreasonable annoyance, embarrassment, oppression . . . ." This Rule will reach intrusions that are not covered by any constitutional right to privacy or any common law or statutory privileges.

A court order which gives an opposing party access to *Facebook* postings that were intended to be available only to persons designated as "Friends" is intrusive because the opposing party is likely to gain access to a great deal of information that has nothing to do with the litigation and may cause embarrassment if viewed by persons who are not "Friends."

Because such discovery is intrusive, it is protected by Rule 4011 where the party seeking discovery has not shown a sufficient likelihood that such discovery will provide relevant evidence, not otherwise available, that will support the case of the party seeking discovery. However, on a scale of 1 (the lowest) to 10 (the greatest), the intrusion from most *Facebook* discovery is probably at a level of 2. This is so because the party resisting the discovery has voluntarily made this information available, in most instances, to numerous other persons, none of whom has any legal obligation to keep the information confidential, and Rule 4011 bars only discovery that is unreasonably intrusive.[20]

In determining whether an intrusion is unreasonable, a court shall consider the level of the intrusion and the potential value of the discovery to the party seeking discovery. For a level 2 intrusion, the party seeking the discovery needs to show only that the discovery is reasonably likely to furnish relevant evidence, not available elsewhere, that will have an impact on the outcome of the case.

Almost all discovery causes some annoyance, embarrassment, oppression, burden, or expense. However, Rule 4011 bars only discovery which causes "unreasonable" annoyance, embarrassment, oppression, burden, or expense. The use of the term "unreasonable" requires a court to balance the need for discovery and the extent of the annoyance, embarrassment, oppression, burden, or expense. In this case, I denied the discovery requests of both parties because the intrusions that such discovery would cause were not offset by any showing that the discovery would assist the requesting party in presenting its case.

---

[20]The intrusion would be greater if, for example, a party's only Friends were a spouse and a daughter.

By way of comparison, a discovery motion that I previously considered arose out of a plaintiff's suit against her doctor who performed breast implant surgery. The plaintiff's case was based solely on a lack of informed consent. Through discovery, the plaintiff sought the names and addresses of the other twenty-six women who received implants during the same month that she received her implant. She sought such discovery because of the possibility that these other women might support the plaintiff's version of what the physician communicated and did not communicate. I regarded this intrusion as reaching a level 9 or 10. I found that these witnesses were not essential because the case could be decided on the basis of the testimony of the plaintiff and the physician. Thus, I denied the discovery request based on Rule 4011.

For these reasons, I enter the following Order of Court:

IN THE COURT OF COMMON PLEAS OF ALLEGHENY COUNTY, PENNSYLVANIA
CIVIL DIVISION

HOWARD TRAIL, individually and as Administrator of the ESTATE OF JESSICA TRAIL, deceased, SUE TRAIL, TAMMIE GRICE, individually and as Administratrix of the ESTATE OF WILLIAM GRICE, deceased, MICHAEL TRAIL, and AMANDA DELVAL,

Plaintiffs

vs.

TIMOTHY LESKO and PITTSBURGH LODGE NO. 11 BENEVOLENT AND PROTECTIVE ORDER OF ELKS, a Pennsylvania Corporation, t/d/b/a B.P.O.E. PITTSBURGH LODGE 11,

Defendants

NO. GD-10-017249

ORDER OF COURT

On this 3 day of July, 2012, it is hereby ORDERED that the discovery motions of plaintiff Michael Trail and defendant Timothy Lesko are denied.

BY THE COURT:

WETTICK, J.

Copies mailed. (CL) 7/3/12

WHAT THEY KNOW | October 6, 2012

A Spy-Gear Arms Race Transforms Modern Divorce

By STEVE EDER and JENNIFER VALENTINO-DEVRIES

Danny Lee Hormann suspected his wife was having an affair. So the 46-year-old Minnesota man installed spying software on his wife's cellphone and the family computer, and stuck a GPS device to her car, letting him follow her to a lakeside cabin one night.

"It was awful," says Michele Mathias, his 51-year-old ex-wife, who denies cheating on him. She says she was so worried about her husband's spying that she and her children searched their garage for cameras and held whispered conversations on the lawn in case he was recording indoors. "It wasn't just invasion of my privacy. It was an invasion of the privacy of everyone who ever texted me or anyone who was ever on my computer."

Scott Lewis for The Wall Street Journal

Jay Ciccarone pleaded not guilty to criminal charges on claims he put spyware on his family?s PC.

The sleuthing got Mr. Hormann thrown in jail for 30 days, convicted of stalking his wife. "Whenever I tell people about this," Mr. Hormann said, "They say, 'I'd have done the same damn thing.' " He adds: "The technology just amazes me."

Mr. Hormann's tactics reflect a new reality for suspicious spouses. Supplied by a tech industry that is making James Bond-like gadgets more affordable and easier to use, they are taking investigations into their own hands.

Techniques once accessible only to governments or corporations are now trickling down to daily use. It's part of a broader transformation of modern privacy in which even the most personal spheres of people's lives—home, friendships, intimacy—can be exposed for examination without knowledge or consent.

Lawyers say the technology is turning divorces into an arms race. Gerry Lane, a marriage counselor in Atlanta, says almost every infidelity case he sees started with a spying spouse. "If someone begins to have thoughts that they are being betrayed, they become obsessed with finding out the truth," Mr. Lane said. "Privacy does not exist in 2012."

More From What They Know

Websites Vary Prices Based on Location

U.S. Terror Agency to Tap Citizen Files

They Know What You're Shopping For

What They Know Video

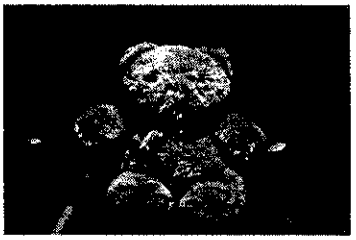
Three companies that sell GPS trackers said sales are soaring. A BrickHouse Security executive said sales of tiny devices that can be placed in a bag or clothing have been "almost doubling" each of the past three years. Another maker, LandAirSea Systems Inc., said that so far this year it has sold about 15,000 of the devices, some of which magnetically attach to cars, already surpassing 2011's full-year sales. SpygearGadgets.com said sales of nannycams and hidden cameras are up 40% this year, and GPS tracking devices almost 80%.

More than three dozen people interviewed, including family lawyers, prosecutors, private investigators, gadget retailers and marriage counselors, as well as individuals who have gone through divorces themselves, said that spouses are embracing snooping technology. A February report by the American Academy of Matrimonial Lawyers found that 92% of lawyers surveyed had seen an increase in evidence from smartphones the past three years, citing in particular text messages, emails, call histories and GPS location information.

The legality of spousal spying is complicated. Not all courts agree on what constitutes a "reasonable expectation of privacy" in a marriage.

In one 2011 Nebraska case, a mother who embedded a listening device in her daughter's teddy bear to record the girl's father was found guilty of violating the Federal Wiretap Act. And in a 2008 Iowa ruling, a court found that a man had violated his wife's privacy by taping her with a camera surreptitiously installed in an alarm clock in her bedroom in their home.

All together, at least five of the 13 U.S. circuit courts have found that the Federal Wiretap Act does prohibit surveillance within marriages. But at least two have ruled that the law doesn't prohibit recording your spouse.



Philip Montgomery for The Wall Street Journal

A hidden-camera bear in a spy shop

In October 2010, for instance, a federal judge in Texas ruled against Rhea Bagley, who, while divorcing her husband, sued him over allegations that he had put spyware on a computer she used and placed a recording device in the family home before he moved out. District Court Judge Lee Rosenthal cited a 1974 circuit court precedent that the Federal Wiretap Act didn't apply to "interspousal wiretaps."

Ms. Bagley, in an interview, said that when someone knows that everything they are doing on their computer or that their private conversations have been recorded, "You feel like your privacy has been violated."

For his part, her ex-husband, Larry Bagley, said he felt he had a right to know what was going on in his home, particularly because, among other things, he was paying the bills. "I feel that if you are married to somebody, you should know everything," said Mr. Bagley, 41 years old.

Some of the most common forms of tech snooping are the simplest, divorce lawyers say. When someone leaves a smartphone or computer unattended, a curious spouse might quickly thumb through emails.

Occasionally, both husband and wife are spying on each other. In Oakland County, Mich., prosecutors charged Leon Walker under the state's antihacking statute after he read his wife's emails in a password-protected account on a shared computer. Then, this past July, they dropped the charge, claiming that his wife was snooping, too, by reading his text messages.

"If you arrest a spouse for something as trivial as this, then you are going to have to arrest the entire world," said Mr. Walker, 34 years old, in an interview. His wife declined to comment through her lawyer.

Your Car is Being Watched 5:53

How Google Side-Stepped Safari's Privacy Settings 5:55

Can Your Credit Score Predict Your Behavior? 6:14

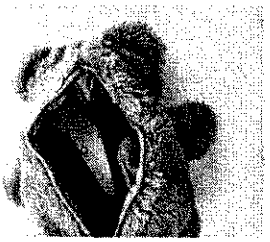
Most Popular

Read | Emailed | Video | Commented

1. GOP Budget Establishes Contrast With Democrats
2. Do the Fitness Math: Gym vs. Stairs
3. Opinion: Paul Ryan: The GOP Plan to Balance the Budget by 2023
4. Opinion: Mark Siedner: About That Baby Who Was 'Cured' of HIV
5. Conclave to Elect New Pope Begins

Divorce and privacy laws vary nationwide, and it is far from settled whether evidence discovered this way would be admissible in a divorce proceeding. However, if the information is used to harass or intimidate someone, a person can face prosecution for stalking or related offenses.

"Stalking laws differ by state, but usually the main element is that there is fear" felt by the victim, said Cindy Southworth of the National Network to End Domestic Violence. Spouses using spying tools could also run afoul of wiretap, cybercrime or trespass laws, or they may expose themselves to civil suits.



Phillip Montgomery for The Wall Street Journal

The hidden-camera bear

Amateur spies have widening options. LandAirSea sells a GPS Tracking Key—a matchbox-size, magnetized gizmo that can stick to cars—for $179 online, far cheaper and more powerful than primitive GPS devices that 20 years ago cost thousands of dollars. Software can be purchased for many smartphones that can track their location. Computer software that copies instant messages and emails can cost less than $100 and be installed without any special know-how. An array of tiny recorders makes eavesdropping easy.

Regulators have a tough time policing the sale of these kinds of devices, since they have legitimate uses by employers or parents. In 2008, the Federal Trade Commission filed a lawsuit against a spyware seller that claimed its software, called RemoteSpy, was a "100% undetectable" way to "Spy on Anyone. From Anywhere."

> *You feel like your privacy has been violated*
>
> Rhea Bagley, whose husband used spyware and a recording device in their home

> *If you are married to somebody, you should know everything*
>
> Larry Bagley

The agency charged the company, CyberSpy Software LLC, with unfair and deceptive practices. In a 2010 settlement, the FTC prevented the company from advertising that the software could be used to spy on people without their knowledge, and it required the software to obtain consent from a computer owner before installation.

CyberSpy didn't admit wrongdoing in the settlement and denied it had violated any laws or regulations. The company still sells the $89.95 software but has changed its marketing pitch. Now the website says: "Especially perfect for those who want to monitor their employees or children, while away from home or work!"

CyberSpy's chief executive, Tracer Spence, said the company's practices met industry norms at the time. He said U.S. companies like his have since changed their products and advertising "to avert a possible run-in with the FTC."

With spyware so affordable, divorce lawyers say they advise clients to buy new computers to avoid the chance that any computers they previously used, or shared with a spouse, are bugged. Some lawyers also say they have begun pre-emptively warning clients that they could run afoul of state or federal laws if they snoop themselves.

"People are dying to know if their spouses are cheating," said Randall Kessler, past head of the American Bar Association's family-law section. "You can have all the laws you want, but I think this is going to go on."

In suburban Atlanta, private investigator T.J. Ward said that his firm, which is handling roughly 80 spousal investigations, is currently tracking about five cars using GPS. It is a standard service he has offered for several years, he said, adding that he has seen the technology improve significantly.

Beyond using tracking gadgets to try to catch cheaters or trace assets, Mr. Ward said his firm also offers clients counter-surveillance options to see if a spouse is spying on them. Sweeping a home for bugs costs roughly $5,000. A cellphone scan runs about $500.

"There is so much technology out there," Mr. Ward said. "You've got to be able to counter."

In 2009, Georgia State Rep. Kevin Levitas sponsored legislation to outlaw the electronic tracking of a person's location or movements without consent. "You know in your gut that that violates some reasonable expectation of privacy," said Mr. Levitas, who retired in 2010.

The bill, which eventually stalled, included exceptions for private investigators, employers tracking company cars, and parents keeping tabs on their kids. It likely wouldn't have applied to spousal tracking, because a car typically would be considered marital property, Mr. Levitas said. In other words, either spouse could make a case for tracking the car under the premise that they own it.

Near Philadelphia, Jay Ciccarone, a father of two young boys, is facing criminal charges stemming from allegations he installed a $97 spyware program on his family's computer.

Three Years of WSJ Privacy Insights»

The Wall Street Journal is conducting a long-running investigation into the profound transformation of personal privacy in America.

Selected findings:

Americans' license plates are now being tracked **not only by the government, but also by repo men** who hope to profit from the information. (10-2-2012)

Google bypassed the privacy settings on millions of Web browsers on Apple iPhones and computers—**tracking the online activities** of people who intended that kind of monitoring to be blocked. (2/17/12)

The government follows the movements of thousands of Americans a year by **secretly monitoring their cellphone records**. (9/9/11)

iPhone and Android apps **secretly shared data** about their users, a Journal investigation found. (12/10/10)

Top apps on Facebook **transmit personal identifying details** to tracking companies, a Journal investigation found. (10/18/10)

One of the **fastest growing online businesses** is that of spying on Americans as they browse the Web. (6/30/10)

Plus, the global **surveillance bazaar**, a secretive **phone-tracking "stingray"** and RapLeaf's clever way of figuring out Web surfers' **real names**.

See full privacy coverage

In September 2010, about six months after Mr. Ciccarone filed to divorce his now ex-wife, she went to police claiming he had been monitoring her, according to court records. According to the records, Mr. Ciccarone's ex-wife told police she discovered his alleged spying when he left his personal email account logged in on the family computer, and she read an email he had written to his lawyer.

She didn't respond to requests for comment.

Nearly a year later, police arrested Mr. Ciccarone and charged him with unlawfully using a computer, intercepting electronic and oral communications, and unlawfully accessing stored communications. Mr. Ciccarone is accused of using a program called Web Watcher, which is designed to record all activity on a computer—capturing email, logging keystrokes and monitoring Internet activity. He has pleaded not guilty and is seeking to have his case dismissed.

Mr. Ciccarone, in an interview, questioned why he was charged when his ex-wife didn't face consequences for reading his email. "I think the case should have been ended right there," Mr. Ciccarone said. "Where is the right to my privacy?"

Tom Hogan, the district attorney in Chester County, Pa., declined to comment specifics of the case. Speaking in general terms, he said, simply looking at an email from an account left open on a family computer probably wouldn't be viewed in the same light as using spyware to intercept messages.

Mr. Hormann, who lives about two hours outside Minneapolis, said he got the idea of sticking a GPS tracker on his wife's car in 2009 from an ad. The one he bought let him observe in real time where his wife drove her Mitsubishi Eclipse. It cost him $500 to buy, plus a monthly fee.

"Pretty amazing stuff," said Mr. Hormann, a former investment salesman and now a truck driver. At least four times in late 2009 and early 2010, he used it to locate his then-wife, Ms. Mathias, court records say.

Ms. Mathias said she and her three children suspected for some time that Mr. Hormann was spying. "He knew where I was constantly," Ms. Mathias said. She said she never cheated. "If you have a device on your phone, your computer, your car," she said, "how the hell are you supposed to have any affairs?"

In March 2010, the month she filed for divorce, Ms. Mathias had a mechanic look for a tracking device. One was found magnetically attached to the car's underside. She contacted police and the county prosecutor charged Mr. Hormann with stalking and using a mobile tracking device on her car.

"She couldn't leave the house without him knowing exactly what she was doing," said prosecutor Tim Hochsprung.

In July, 2010, a jury convicted Mr. Hormann of two charges, stalking and tracking the car. He spent 30 days in jail. On appeal, a judge reversed the tracking charge, saying he had "sufficient ownership interest" of the car and thus could legally track its whereabouts.

Write to Steve Eder at steve.eder@wsj.com and Jennifer Valentino-DeVries at Jennifer.Valentino-DeVries@wsj.com

Related Reading

New Tracking Frontier: Your License Plate
Is Your License Plate Being Tracked?
The Economics of Surveillance
WSJ Privacy Reporting: Full Coverage

MORE IN TECH

Email Print Order Reprints

Email Printer Friendly Order Reprints

Share:

Like Send 350 people like this.

Add a Comment JOURNAL COMMUNITY
View All Comments (120) Community rules

To add a comment please