St. John's University School of Law

St. John's Law Scholarship Repository

Faculty Publications

2015

Social Media: Children's Lawyer's Friend and Foe

Jennifer Baum

Sarah N. Fox

Follow this and additional works at: https://scholarship.law.stjohns.edu/faculty_publications



Part of the Family Law Commons, Juvenile Law Commons, and the Litigation Commons

Social Media: Children's Lawyer's Friend and Foe

By Jennifer Baum and Sarah N. Fox – January 12, 2015

Social media is taking over the globe. The Pew Research Internet Project states that in the United States, 95 percent of 12- to 17-year-old children are online. Teenagers are also sharing more and more information online: 91 percent of teenagers post a photo of themselves, 92 percent post their real name, and 71 percent post the city or town where they live. "Teens Fact Sheet," *Pew Res. Internet Project* (Sept. 2012). This information, in the wrong hands, can be harmful to a child. The Children's Online Privacy Protection Rule, designed to safeguard children's information and access online, is a start, but it defines a child as someone under age 13, thus excluding the majority of underage Internet users: kids ages 13–18.

As attorneys for children, therefore, it is important that we talk to our clients about the use—and misuse—of social media. Children need to be aware that what they share on social media is never completely private and can be used against them, or against people they care about. One New York attorney notes that her office always advises kids to take down their social media sites completely once a case has begun, especially where the parties in the case are known to each other, but kids seldom comply (or they report they have complied when they haven't). This is because the draw of social media, especially on teens, is extremely powerful. The key point for attorneys to remember about electronic communication is that privacy is never guaranteed. As the child's lawyer, you will want to protect your client's electronic privacy, while exploiting gaps in the electronic privacy of others.

The first, and most secure, form of defense is to not use social media at all. Many children's lawyers give out this advice at the first client meeting. But for those who insist on maintaining their social media accounts, there are some options. The first level of protection is to use privacy controls. These controls restrict who can see what you have submitted to the site. Unfortunately, many people choose not to use these controls and then everything they do becomes public information, which can spell litigation disaster.

For starters, many people find it convenient to leave their computers, phones, and other devices logged in to different websites. The obvious risk, however, is that anyone using that device will have automatic access to the logged in accounts. Not only does this mean the account holder's privacy is compromised, it also means that the account holder's identity is compromised, because unauthorized users can access the account and take actions, make purchases, or even post something incriminating or harassing under the veil of anonymity. But even without staying logged in to a site, the information submitted still is not shielded from the public: Once something is shared on social media, anyone who sees it can take a screenshot from any computer or phone, and retain it forever. This is true even if the original post is later deleted. If someone saw it before it was deleted and took a screenshot, they have it as long as they choose to retain it. Moreover, deleted items can often still be discovered through websites that search cached (old) pages. A cached page is a version of a website saved at a previous time and stored. "Delete" does not always mean "delete."

^{© 2015} by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

Children and teenagers do not always understand this and often will post things they later regret, or that are harmful to them. For those doing investigations (defense lawyers, prosecutors, police), social media can often provide substantial background into what is going on. For this reason, police now routinely ask about social media accounts at the earliest stages of an investigation, capturing data before privacy settings are changed or information is deleted. For defense lawyers, finding a public profile means getting an opportunity to look through all of a person's posts and photos. This may provide a gold mine of free discovery: who various people associate with, their physical locations at particular points in time, what activities people were engaged in and when, what their thoughts and feeling are about various circumstances or events, or what their future plans might be.

Another, less obvious, aspect of online privacy includes location trackers. Many social media sites allow (or default to) programs that can identify the location of the user, down to a few feet. According to one juvenile defense attorney:

If I had one piece of advice to give to everyone in high school it would be not to steal an iPhone. 'Find my iPhone' is not your friend. The police can find you on the subway with it: the kid comes up out of the subway, the police are waiting for him, the kid matches the complainant's description, [and that's probable cause].

Location trackers can also be used to blow up alibis, or as circumstantial evidence. Many people do not realize they are being tracked in this manner, or that location trackers can be managed (turned on and off).

A tech-savvy attorney can use social media to supplement factual investigations in creative ways. In one child welfare case, a young client had uploaded videos of herself singing in her shelter apartment prior to the allegations, and the attorney who found the videos online got to "turn back time" to see the conditions in the home prior to the date the petition had been filed.

Most sites have at least a couple of different levels of public and private settings. While anyone at all can view a public setting or page, absent a search warrant, membership in a particular form of social media is required in order to view others' pages. Some pages or items can be restricted to approved users, while others allow varying degrees of access. This can create an issue for attorneys seeking out private information, as ethical considerations come into play for attorneys initiating a "friend" request (access request) to another user. For this reason, the better practice is for an attorney not to use his or her own social media account to explore the accounts or pages of others, but for the client to do so. One attorney noted, "I don't impersonate anyone. When I want to see my client's page I have them bring it up in my office, and I ask them to navigate around and show me." In cases where the parties are already known to each other, there is a good chance that friend requests or other links have already be established, and much information can be obtained. Prosecutors can have the complaining witness log in, because if a complainant is "online friends" with a respondent, each can see the other's pages.

^{© 2015} by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

Clients also need to be aware that no-contact orders now routinely include social media. If there are privacy settings in place, it is likely that no one will know the contact is taking place other than the two parties—until one of the parties complains, that is.

Because of all the different ways social media can play into a legal case, it is important for attorneys to understand at least the basics of social media, so they can properly advise their clients about it. So even if you don't use it, your clients do, and those clients need to understand how their social media use (or misuse) can impact their rights and remedies.

Facebook

Facebook is one of the original forms of social media. While you may have heard that Facebook's popularity is down, it is still very much in use, and needs to be understood. Members (users) create a profile and have a "wall." This is a digital page where you can post text, links, and pictures. Sharing is done through "friend" lists: when a user adds a friend, the friend can see what the user has posted. They can also share it with their other friends. Messages can be left on the wall, or sent privately. Upon logging in to the site, a user sees a feed, which is a list of activity by friends. The feed allows a user to see at a glance what is happening on friends' sites, and also to respond to that activity with comments or "likes."

Facebook has different levels of privacy, and while the default privacy setting is currently "friends only," this is a recent change. Previously, the default setting was public. That meant that anyone at all could see what was posted, unless the user affirmatively changed the privacy settings. Users can choose the level of privacy for each post and each picture taken, and it is always a good idea to check the privacy setting prior to each posting.

In addition to providing a wall and a feed, Facebook also allows users to "message" each other. Private conversations may be had among members, but entire conversations can be forwarded to nonparticipants, and new users can be added to group conversations, allowing pretty much anyone to view all prior messages in that conversation. This means that private conversations are never really private, as they depend on the voluntary compliance of other users.

Facebook provides a treasure trove of useful information for law enforcement and defense attorneys alike. One example of the usefulness of finding inner thoughts made public through Facebook is discussed in *In re D.T.J.*, 956 F. Supp. 2d 523, 543 (S.D.N.Y. 2013), in which voluminous Facebook diatribes by a father toward his daughter were admitted into evidence in a Hague Convention child abduction trial. Another example includes the use of a child's public Facebook posts as identity evidence in a series of burglaries. *See In re D.O.*, 840 N.W.2d 641 (N.D. Sup. Ct. 2013). Minutes after robberies, another defendant posted Facebook photos and messages of himself holding cash and attempting to fence stolen goods. *See State v. Phipps*, 2014-Ohio-2905 (Ct. App.). A juvenile once posted his profile to the page of a known graffiti crew. *See In re Isaac C.*, No B250475, 2014 WL 931033 (Cal. Ct. App. Mar. 10, 2014). Facebook has also been used to violate no-contact orders, *see In re A.H.*, No. HO39967, 2014

^{© 2015} by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

WL 2932601 (Cal. Ct. App. June 30, 2014) (mother sent Facebook messages to children in violation of restraining order), and to commit new crimes, *see <u>In re P.T.</u>*, 995 N.E.2d 279 (Ohio Ct. App. 2013) (child made Facebook posts mocking Sandy Hook shootings and making similar threats).

Facebook posts, like other electronic documents, can be authenticated in any admissible way, including through circumstantial evidence. *In re L.P.*, 749 S.E.2d 389, 393 (Ga. Ct. App. 2013). In sum, Facebook posters should beware that anything they post or message can be used against them.

Instagram

Instagram is a newcomer to the social media world. Launched in 2010, it is an online photo- and video-sharing social network that allows users to upload pictures or short videos with descriptions, and share them publicly or privately with "followers." According to Instagram's *Parents' Guide*, the minimum age for use is 13. As with all other forms of social media, Instagram notes that the safest and most appropriate way for kids to participate in photo file sharing is with appropriate adult supervision—and as with all other forms of social media, that does not always happen.

Photos posted to Instagram can easily be shared with a variety of other social media platforms, including Facebook, Twitter, Tumblr, and Flickr. Even if an item is not cross-posted to another platform, it will appear on the user's web profile page and on friends' feeds. Instagram users can place a description, their thoughts, or anything else online with their photo. Often, people will use a description with a hashtag in front of it, for example, #selfie. There is also a section of Instagram called Explore. This provides a place to search for specific people or hashtags. A search for #selfie will result in photos from people with public profiles who put #selfie in the description section of their photo.

Privacy on this site is also varied. The "friends only" setting limits views to approved contacts, but any contact can be approved, even contact by strangers. Public settings are just that, and can be viewed by anyone. Users should know that despite privacy settings that limit access to account activity, an Instagram user's profile is always public. Also, there is a "locations" button that uses a phone's GPS to identify the location the photo was taken, and once set it remains set such that locations are updated automatically.

Instagram has been used by parents to post photos of themselves violating no-contact orders with children, by children to post pictures of themselves using illicit substances or engaging in other inappropriate activities, and by law enforcement to aid in criminal investigations.

Twitter

Twitter is a social networking site that is meant to be public. "Twitter does not guarantee any of its users complete privacy. Additionally, Twitter notifies its users that their Tweets, on default account settings, will be available for the whole world to see. . . . Tweets [are], by definition

^{© 2015} by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

public. . . . Indeed, that is the very nature and purpose of Twitter." <u>People v. Harris</u>, 945 N.Y.S.2d 505, 509–10 (Crim. Ct. 2012).

Tweets are messages sent through Twitter that contain 140 or fewer characters. Tweets can be sent by SMS text, from a Twitter app, or through Twitter's website. Users "follow" one another, and tweets appear in a feed on the user's account page.

Privacy on this site can be managed, but the site is essentially public, and that is the default setting for new accounts. Users follow other users to view what they are saying; followers subscribe to the account holder's Twitter feed. Caution is advised because, as with all other forms of social media, information can be forwarded with the click of a button; in the Twittersphere, this is known as "re-tweeting," and is a common practice and one of the most popular ways of sharing information by Twitter.

Snapchat

Snapchat allows people to send exploding (self-destructing) photos and videos to one or more people at a time. The content is referred to as a "snap." Users also have the ability to add text or draw on the photos before sending them. What makes Snapchat different from other forms of social media is that the user sets a time limit for how long the photo or video can be seen by the recipient of between one and 10 seconds. Once the time limit is up, the snap is hidden from whatever device the recipient is using and deleted from Snapchat's servers.

Privacy is a huge problem on this site. For starters, the site appallingly advises users who are under age 13 that they can get around the site's safety limitations if they "just delete [their account] and start over with a fictitious birth date." <u>A Parent's Guide to Snapchat</u> (2013). The site also advises:

Snapchat lets you know when your message has been opened and—usually—if it has been captured and saved by the recipient. We say "usually" because it doesn't work 100% of the time and there are workarounds, including some "hacks" and the ability to take a picture of the screen with a camera, including a friend's cell phone camera.

Users, including kids, sometimes send sexually explicit snaps (a practice known as "sexting") under the mistaken belief that the content really will disappear when the time limit expires. But as noted above, this is not always true. Attorneys should be aware that in some states, sexting laws apply equally to children and adults, meaning that in addition to criminalizing sexting between an adult and a child, kids can be prosecuted for sexting with one another.

Another concern is that Snapchat associates phone numbers with user names. That information has been hacked in the past. It provided the hackers with phone numbers and matching names. After the hack, many people received spam snaps. Some of those were pornographic ads. There is also a grave concern that teenagers continue to use this medium for sexting, something Snapchat addresses in its parent guide.

^{© 2015} by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

In short, Snapchat offers all of the lure of privacy and safety, with none of the guarantees. Be careful with Snapchat.

PVP Servers

PVP servers are online gaming sites that allow messaging and information exchange. "Moderators" are supposed to monitor the ages and messages of users, but conversations scroll by quickly and disappear. As with all other forms of social media, content can be captured by screenshot or users' cameras, and nothing is really ever private. Nothing prevents users from exchanging information about more intrusive ways to communicate, such as email and Skype.

Video Conferencing Services (Skype, FaceTime)

Video conferencing services such as Skype and FaceTime provide a way to make video and voice calls, send instant messages, and participate in file sharing. Two or more users with a video conference account can call each other using their device's built-in camera and have a face-to-face conversation. The conversations are not recorded, but third-party software has been developed that does allow one user to record another. And screenshots can still be made of any instant messaging sent through video conferencing. There are privacy controls, but kids often do not understand the implications of accepting a request for a video call from a stranger (or complainant, or other person with whom a child should not have contact). Unwanted live (real-time) video contact with others is possible without carefully managing privacy settings.

Skype has been used to maintain parental or sibling bonds in child welfare cases, and witnesses have testified via Skype.

Conclusion

Given the prevalence of social media use by children and youth, it is essential that children's lawyers have at least a basic understanding of these platforms in order to advise their clients. One of the most critical things to convey to child clients is that there is no privacy online—everything they post should be considered public and can be used against them.

Keywords: litigation, children's rights, social media, privacy settings, public information, identity, location trackers, sexting

<u>Jennifer Baum</u> is a professor at the St. John's University School of Law in Queens, New York. <u>Sarah N. Fox</u> is a solo practitioner in Cincinnati, Ohio.

^{© 2015} by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.