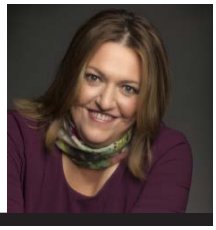
THE DARK SIDE OF SOCIAL SHARING

About a year ago, a news headline caught my attention: "Prominent Seattle Attorney Arrested and Thought To Be Serial Rapist." After reading the article, I thought: Why was the attorney's name so familiar? Then I remembered: he'd recently sent me an invitation to connect on LinkedIn! While this was coincidental, it made me ponder how well I knew the people I'd randomly clicked "yes" to when they requested that we connect.

We live in a society where we are lulled into believing that sharing is good. We've all heard "sharing is caring." But with headlines of celebrity photos leaked, stalking, online abuse and the like, it's time to take a closer look at the dark side of social media.

About the Author

Donna Payne, CEO of PayneGroup Inc., is a recognized expert in IT, with specialization in legal software and technology. She conducts roadshows on privacy and delivered a keynote on the subject at LegalTech New York in 2014. She and PayneGroup are the author of 13 books on Microsoft Office. Donna was awarded the ILTA 2013 Vendor Thought Leader of the Year award, the first-ever Lex Proficio award for lifetime achievement (ABA) and LTN's innagural Consultant of the Year award. PayneGroup created the products Metadata, Redact, Numbering, Forms and Outlook Send Assistants. Contact her at donnapayne@thepaynegroup.com.



SHARING IN THE SHADOWS

I spoke about the dark side of social media with Cullen Hoback, a director and producer well-known for his 2013 documentary "Terms and Conditions May Apply." He succinctly summed up the problem: "Social media companies prey on our desire to connect with each other. Companies like Google and Facebook are actually in the business of getting to know us better than we know ourselves. While this may help them advertise more effectively, being able to predict someone's actions through the intimate knowledge of their desires comes at a frightening cost."

When we talk about sharing, there are two things to consider:

1. What are we sharing by choice (*e.g.*, what we had for dinner)?

2. What information is captured and shared for us?

LINGERING LOCATIONS

Do you use an iPhone? If so, you might be surprised to learn about the Frequent Locations setting quietly deployed in the release of iOS 7. Turned on by default, this feature tracks almost every location you go to regularly (*e.g.*, home, work, the park near your home). Not only does it track locations, it provides a map, a list of dates you visited a location, and arrival and departure times.

Apple states this information is stored on your device only; however, when a device or its information is stolen, hacked and compromised, this is exactly the information you do not want to share.

To control this setting on your iPhone, go to Settings, Location Services, System Services, then Frequent Locations. In that same place, you can enable a Status Bar icon that shows when information is being tracked and added to the list.

If you have a propensity for taking selfies or pictures of your kids (or dog), you'll also want to make sure the Location Services setting for your cellphone camera is disabled. By default, when you take a picture, most portable devices embed the longitude, latitude and altitude as properties with the picture. When these pictures are shared or posted, exact address and location information can be exposed. This information entered into mapping software will provide a startlingly accurate location.

In a recent TED Talk, privacy expert James Lyne discussed the risk of GPS data being embedded in pictures. Lyne commented that 60 percent of dating site photos contain GPS location coordinates.

Make sure geotracking and Location Services are not enabled, whether on your phone, in the software you use or in social programs such as Twitter.

DATA MINING DOOM

LinkedIn allows you to send invitations to up to 3,000 friends before having to request that LinkedIn grant additional friends in monthly allotments. Clicking "connect" is easy; clicking "accept" is just as easy. We do both without thinking sometimes.

The downside to random connectedness is that people can mine your data when you don't implement controls. And, of course, the default option in LinkedIn is to leave your profile settings unprotected. Just view the profile of someone you are connected to, click "Connections" in the box that contains their name and picture. If you see the words "Shared" and "All," then you are free to look at and connect to any of the people in their network. If you only see the word "Shared," good for them — they have locked down their profile to prevent people from mining their hard-earned connections.

Individual data mining — someone viewing and piggybacking on your connections — can be controlled. Just go into your privacy settings and change the options for who can see your connections. While you're there, consider turning off data-sharing with third-party applications, and manage settings for LinkedIn plugins on third-party sites as well.

Cullen Hoback noted, "The terms and conditions of most social media sites are designed to take as much from you as possible. You have no meaningful choice to [make], because you don't own your data, they do."

POSTED (AND BUSTED)

Free speech and self-expression are rights granted under the U.S. Constitution; however, if you plan to apply for a new job or apply to a select school, you'll want to think twice about allowing unrestricted access to your Facebook or other social media pages. It's

Lyne commented that 60 percent of dating site photos contain GPS location coordinates.

also prudent to think first before randomly posting pictures or engaging in negative behavior online.

A few years back, my organization posted a job ad on Craigslist — to which we received hundreds of responses. We narrowed down the field quickly by doing a simple browser search about candidates. Some of the results were shocking. There were profanity-laced profiles, naughty pictures and a profile full of insults directed at a current employer. Needless to say, those individuals did not get a call back.

A good rule of thumb is: If you don't want your mom to see it, don't post it.

And while we're talking about posting, it's not a good idea to post information about going on, or currently being on, vacation. Letting a would-be robber know that your house is empty is never a good idea.

A good rule of thumb is: If you don't want your mom to see it, don't post it.

CORPORATE SOCIAL BLUNDERS

Many corporations are using social media to monitor feedback from customers. I recently posted a comment about Alaska Airlines. Within a minute, I received a response.

Companies respond to social media because they know posts will be seen by many people and have the potential to go viral if not addressed promptly and adequately. But sometimes it's the customer service posts that go viral. Take, for instance, this unfortunate exchange between US Airways and an unhappy passenger.

Passenger: @USAirways Unhappy that 1787 sat for an hour on tarmac in CLT because overweight, resulting in over hour late arrival in PDX.

Airline: We truly dislike delays too and are very sorry your flight was affected.

Passenger: @USAirways yeah, you seem so very sorry. So sorry, in fact, that you couldn't be bothered to address my other tweets.

Airline: We welcome feedback, (name). If your travel is complete, you can detail it here for review and follow-up (followed by a link to a sexually explicit photo).

The airline later stated the mistake occurred when a picture flagged as inappropriate was pasted into the contents of the response for a different message. US Airways issued an apology. The exchange, however, had already gone viral.

Other corporate social media mishaps include one from @KitchenAidUSA who made a negative comment about President Obama's grandmother's death, and Chrysler, whose social media manager posted an f-bomb rant about drivers in Detroit. The list of corporate blunders is too long to list.

OPT OUT OF THE DARK

There is a proliferation of information being captured about each and every one of us, and much of it we have little control over. Candidly, I'm not sure anyone knows the true extent of how much information is being captured about us.

As Hoback noted: "Good surveillance happens invisibly. It's only when someone messes up that we find out about it. The profiles social media companies build on you could lead to something like a tax audit, or even your arrest, and you may never know the cause."

Fortunately, there are things we can do to limit our exposure. We can choose better software browsers. We can set privacy options. We can opt out of sharing information with third parties. We can use more robust passwords. We can avoid taking and sharing compromising pictures of ourselves (or others). We must think before we post, connect and like. Above all, we must realize that everything we post will outlast us all. You can click delete, but it's already been indexed and stored.

Beware of the dark side of social media, and think twice before your next post. P2P