OBER | KALER
Attorneys at Law

Social Media Technology – A Basic Resource

Today's presentation will provide a wide view of the privacy, security, and employment law issues that are raised by "Social Media." Social Media, however, is a poorly defined term. While it is used frequently, it is also used loosely. Speakers using the term are referring broadly to a large group of services, websites, and applications that allow individual users to rapidly communicate, share images, links, or other data, and "connect" with large groups.

From a compliance perspective, it is insufficient to state that a loss of protected health information ("PHI") occurred through "Social Media." Privacy and compliance officers tasked with preventing, investigating, mitigating and reporting data breaches need to do so in a concise and effective manner that takes into account the different technological structures of the many applications and services known broadly as "Social Media."

Collected in this Resource is basic information regarding the structure, operational parameters, vulnerabilities, and potential risks posed by several popular social networking services, websites, and communication modalities. This is by no means an exhaustive list, as communication technology is evolving rapidly and continuously. But it provides basic technological information necessary to ensure that prevention, investigation, and mitigation efforts are being directed accurately.

Facebook

Basics

- Ubiquitous photo, messaging, and mail service – 750 million users and growing. Famously began as a social network for college students but has spread into a virtually world wide utility that has played roles in everything from the sharing of new baby pictures to allowing communications between protesters in the Arab Spring protests of the summer of 2011. The President of the United States has a Facebook account, but so does the author's grandmother.

- Supplanted other, similar services, such as MySpace.com, but shares a technological structure with many similar sites, including MySpace, LinkedIn and more specific applications, such as SalesForce's "Chatter". Each service is slightly different, but all are designed to allow multi-media communication from a single individual to a large audience in real-time.

- Users create accounts that can include much or little personal information and then can connect to other users. In common usage, user's "friend" one another. User connections are by mutual consent only – no one can "friend" you without your explicit permission. Users can then organize their friends into "groups" (though they are not required to do so).

- In its most basic format, Facebook allows users to post pictures and "status updates" (short textual descriptions of how a user is feeling, what they're doing, etc.) Updates may also include embedded movies, or links to other internet sites. These updates are then published to the user's connections ("friends"). Users may also send one another private messages, post messages on one another's public main page ("wall") chat via facebook's live chat functionality, and "tag" or identify friends in other friend's photos.

- Additional applications and add ons – games, surveys, groups that can be joined are constantly in flux and complicate any in-depth analysis of risk. Add-ons often seek user permission to collect personal data, including friend lists, locations, employment, and other data.

- Facebook is not passive. Photos, status updates, and changes in personal information are sent automatically to all of a user's "friends." In other words, once a photo is posted, its distribution occurs automatically and instantly – users do not need to invite friends to come see their photos.

- Users have a wide variety of privacy functionalities to limit distributions of photos, tags, and status updates. Privacy functions are also available to limit information visible to the public, conceal a user altogether, or limit display to certain friends or groups of friends. Privacy functions are constantly evolving and can be complicated to both use and track.

- While Facebook functions much like a personal website, where people may come to learn about you, see your pictures, see what is going on in your life, properly managed privacy settings and thoughtful "friend" selections can maintain a relatively high degree of privacy.

Facebook Risks and Complications

- Privacy functionalities are constantly in flux – new protections are added regularly, and procedures for setting or maintaining old settings may be changed administratively without much warning.

- Newer or more technologically naïve users may not be aware of privacy functions or the risks inherent in providing a constant stream of information. In a classic example of an unforeseen risk – posting both your address and the fact that you're "having a great time on vacation!" can let someone know that your house is empty. Similarly, a picture or message that was meant for an individual could be accidentally made "public" or sent to an entire friend list.

- Friend lists are not always actively managed, and the total number of "friends" can become a competitive number. It is not unusual for an individual to have 1,000 or more "friends" some of whom they barely know, if at all.

- Employees are frequently inclined to "friend" one another and may not realize that their conversations about work related events, problems, struggles, or even successes can be viewed and shared by a potentially wide audience, depending on their personal privacy settings.

- User uploaded information is stored and controlled centrally on Facebook servers. A user may close their account, but that in and of itself does not ensure that posted information has been destroyed or even rendered entirely inaccessible.

- User controls cannot override corporate decisions – posted information is "out there" forever. Similarly, posted information can be stored or saved by other users – especially pictures, for example.

- Technology is mobile, ubiquitous, and free – anyone with a smart phone can access Facebook, post photos, and communicate in real time. Preventing an employee from accessing Facebook on company computers, for example, means little when they can access it just as conveniently from their phone.

- Accounts can be faked or hacked. A "hacked" account is a genuine account that is being used and accessed by someone other than the authorized user. There are viruses and other malware programs designed specifically to facilitate this sort of Facebook "hacking." A faked account is just that – an account which has been set up as though it belonged to a particular person or company (often a celebrity or well-known company) when that person or company in fact has nothing to do with its contents. Famously, the Facebook page of a female Syrian protestor was entirely fictional and operated by a male living in Germany.

- Even with Facebook's industry leading privacy controls, there is no guarantee that posted information will remain private.

- Both Facebook and third party application providers collect immense amount of personal information which is shared with advertisers and other third parties.

Questions Following a Breach on Facebook

- What is the information posted?

- Is it clear that it is both private medical information and personally identifiable?

- Was the information posted by the user, or was the account hacked or otherwise tampered with?

- Was the PHI sent specifically to a single person, or broadcast?

- How many "friends" received the update?

- Was the information copied or downloaded by any other user? (This information will generally not be available at a user level. In the absence of clear data, it will have to be assumed that the information was broadly disseminated.)

- Why was the information posted? (a picture posted for innocent reasons that contains PHI should be handled differently, for example, than a picture posted specifically because of the PHI it contains, such as, for instance, pictures of trauma victims in an Emergency Room).

- When the information is "taken down" can the covered entity be certain that it has ended the breach, or is it reasonably possible that the information was copied and stored elsewhere?

Twitter

Basics

- Though it is a separate service, Twitter in essence reproduces Facebook's ability to post short bursts of text to thousands, if not millions of "followers."

- Messages are limited to 140 characters ("Tweets"). They may include links to other media or pictures through the use of separate, add-on applications (such as "TwitPic" which allows users to "tweet" photos).

- Content is limited to "tweeted" materials – users do not maintain a separate storehouse of photos or other personal information as they do in Facebook.

- Though tweets may be sent to a single individual, Twitter's default setting is to allow public access to all messages.

- Tweets are sent through the internet, but may originate from mobile phone applications or even text messaging services (SMS services). Like Facebook, access to the technology is free and ubiquitous.

- Twitter is not passive. Tweets are distributed automatically and instantly to all of a user's "followers."

Twitter Risks and Complications

- Data is centrally stored and is not user controlled. As in the case of other centrally stored and controlled information, a user may close their account, but that will not destroy or render inaccessible existing data.

- Information that users tweet is forever "out there" and may not be effectively recalled. A popular tweet can be "re-tweeted" by hundreds or thousands of other users almost instantaneously, making recall or destruction entirely impossible. Representative Anthony Wiener's recent, and devastating, embarrassments all came as the result of a single "private" tweet which most certainly did not remain private.

- Information that is posted may, depending on the application used, actually become available to other companies or individuals for their own use. Famously, the use agreement for the most commonly used picture sharing software (TwitPic) grants the company a license to use and/or sell all photos uploaded by users, without the users consent or knowledge.

Again – once it is "out there" it has effectively permanently left a user's sphere of control.

- Accounts may be faked or hacked. It was only recently that Twitter began to offer an identity verification service. Previously, for instance, there may have been hundreds of different users who identified themselves as "Brad Pitt." Similarly, accounts can be hacked – though in the most famous incident of "hacking" (Representative Anthony Wiener) it later became clear that the photos posted were posted as a result of bad judgment, not bad security.

- Twitter encourages bad judgment. It takes only seconds to type a 140 character rant, insult, secret, or libelous comment and disperse it forever to hundreds if not thousands of people. Representative Weiner's example is telling in this regard.

- Twitter openly shares user information with third parties.

- FTC took the unusual step of bringing an action to force Twitter to improve its security after multiple celebrity accounts (including President Obama's) were hacked. The case settled in 2010 and resulted in several new privacy features for users. Recent news, however, has indicated that Twitter may again be under FTC investigation. The FTC, of course, operates its own Twitter account at "@FTCGov."

Questions Following a Breach on Twitter

- What is the information posted?

- Is it clear that it is both private medical information and personally identifiable?

- Was the information posted by the user, or was the account hacked or otherwise tampered with?

- Was the PHI sent specifically to a single person, or broadcast?

- How many "followers" received the update?

- Was the information copied or downloaded by any other user? Has it been "re-tweeted?" (This information will generally not be available at a user level. In the absence of clear data, it will have to be assumed that the information was broadly disseminated.)

- Why was the information posted?

- When the information is "taken down" can the covered entity be certain that it has ended the breach, or is it reasonably possible that the information was copied and stored elsewhere?

Websites (Including Photo-Sharing Sites)

Basics

- People may maintain their own websites, or they may post to common photo sharing sites (Flickr and Snapfish are two common examples, but there are many others).

- Personal websites are typically not operated physically by the administrator (in that individuals rarely maintain their own servers) it is more common that a personal website is maintained on server space provided by an internet service provider ("ISP") such as Comcast, AOL, Verizon, and others.

- Personal website administrators, however, have administrative authority over their own content – they can shut the site down and remove material from the remote servers.

- Personal websites may include uploaded text, movies, pictures, etc. Content is controlled by the administrator but generally is publicly available. It is possible to include password protected content on a personal site, but not typical.

- Commercially operated photo sharing sites are operated by corporate entities, not individuals. As in the case of Facebook and similar sites, users maintain accounts and can post and delete content from their section of the site, but have no true administrative authority. Each commercial site will have different privacy controls and settings, but they generally default to public availability.

Photo Sharing Risks and Complications

- Sharing photos through a commercial site subjects the user to the vagaries of that website's privacy policies and its privacy controls (or its lack thereof).

- Popular sites such as Flickr offer some privacy controls, but naïve users may not be aware that they exist or may not use them properly.

- Photo sharing sites and personally operated websites both may allow the collection of data on "views" – how many people, for instance, viewed a particular picture.

- Both photo-sharing accounts and personal websites may be shut down by the user/administrator, but information that is made available on the internet may always be copied and may be stored.

Questions Following a Breach on a Website

- What is the information posted?

- Is it clear that it is both private medical information and personally identifiable?

- Was the information posted by the user, or was the account hacked or otherwise tampered with?

- Was the photo viewed by anyone? A photo that hasn't been viewed may not cross the existing "harm threshold" and qualify as a breach.

- Why was the information posted?

- When the information is "taken down" can the covered entity be certain that it has ended the breach, or is it reasonably possible that the information was copied and stored elsewhere?

Web Logs, or "BLOGS"

Basics

- Blogs allow users to post an online multi-media journal on a specific topic or topics of general interest.

- Blogs may be operated on a personal website, but, more typically, are made available through websites that specialize in hosting blogs, such as Blogspot.com or Blogger.com.

- Content is almost always available to the general public, though it may be industry specific in nature. One need not work in the pharmaceutical industry, for instance, to follow or receive updates from Pharmacomplianceblog.com.

- Updates may be pushed to followers, or they may receive email or other notifications of a new entry after they "subscribe" to the Blog. Availability and terms of features such as these can vary. More typically, blogs are passive forms of publication and readers must visit to read new content.

- A Blog is best understood as an online article that is updated periodically, creating a running history of a person, topic, or event.

- Readership or "page views" will almost certainly be tracked as a means of tracking the blog's popularity, but this information may or may not provide enough detail (or certainty) to be of use during a breach investigation.

- Bloggers often link to one another's posts as a way to increase readership.

Blog Risks and Complications

- Hosted content is subject to hosting companies terms of use, may not be entirely controlled by the blogger.

- Hosting companies often refuse to exercise any sort of editorial control over their bloggers, leaving them free, if not encouraged to, engage in hyperbole, defamation, and outright fiction.

- Self-hosted content may be under greater control of user, but it is still subject to copying and storage once published on the web.

- Blogs may be hacked or faked.

Questions Following a Breach on a Blog

- What is the information posted?

- Is it clear that it is both private medical information and personally identifiable?

- Was the information posted by the user, or was the account hacked or otherwise tampered with?

- Was the post viewed by anyone? Is that information available to the blogger, and is it sufficiently reliable?

- Why was the information posted?

- When the information is "taken down" can the covered entity be certain that it has ended the breach, or is it reasonably possible that the information was copied and stored elsewhere? Did another blogger link to the offending post?

Instant Messaging (Chat)

Basics

- Generally limited to person-to-person communication, not typically used for broadcast communications. "Chat" rooms are an exception, where many people may all simultaneously talk to one another. Different providers offer chat rooms in various formats and following various procedures.

- Permits two users to communicate in real-time via short typed messages. Users so engaged are "chatting."

- Messages are sent over the internet through servers owned and operated by the Chat host. Common Chat hosts include Google, AOL, Microsoft, and Facebook.

- Chat may be part of a larger service (such as Facebook) or may be hosted as a stand alone program (such as "MSN Instant Messenger").

- Various chat services are available for free on smart phones and similar web enabled devices.

Chat Risks and Complications

- Security can vary widely based on devices and hosting providers used. Internal chat programs (intracompany) may be very secure, external hosts may not.

- Chat transcripts are typically saved on behalf of both parties, and company servers may store chat information for various periods of time based on their terms of use.

- Chat accounts may be hacked or faked – it can be extremely difficult to be certain that you are talking to who you think you are talking to (or even that you are chatting with a human – several automated robotic chat programs have been developed).

Questions Following a Breach on a Chat

- What is the information chatted?

- Is it clear that it is both private medical information and personally identifiable?

- Was the information posted by the user, or was the account hacked or otherwise tampered with?

- Who else had access to the Chat? Are we certain that person was identified correctly?

- Why was the information posted?

- What are the terms of use of the Chat provider? Are transcripts automatically retained? Is it possible that the other party saved a transcript including the PHI at issue?

Texting (SMS)

Basics

- Short Message Service or SMS is typically known as "texting."

- Permits users to send short messages over a dedicated data channel available to all cellular devices.

- Data channel is typically reserved for location and call messages between handset and nearest tower – provides for phone location and informs phone of available channels for calls.

- Inherently insecure – texts are, by their nature, open communications with the local cell tower. They may be intercepted in transit by any properly configured (and located) device. A recent engineering / hacking experiment posted to the internet involved building a small plane which could, using miniature on board computers, fly to a certain area and intercept all text traffic sent to and from that area's cell towers.

- Texts are also generally stored on a central server of the cellular provider (or more than one) as well as on both the sending and receiving devices. They are stored both to provide a record to users and so that messages sent to a disabled or out-of-service-area device may be delivered later, after the device alerts the tower that it is again able to receive messages.

Text Messaging Risks and Complications

- Texting has become a primary mode of communication for many.

- The temptation to text, rather than call, is extremely high based on the medium's speed and convenience.

- SMS Technology is inherently non-secure. Messages may be intercepted and are stored on both sender's and receiver's handsets, which may be lost or stolen.

- Messages are also stored on a central server – though they are not typically publicly accessible, the messages are no longer under the control of the sender or recipient.

Questions Following a Breach in a Text Message

- What is the information sent?

- Is it clear that it is both private medical information and personally identifiable?

- Who was the recipient? Are we certain that a breach in fact occurred? (that the method used to send the information is not secure does not necessarily mean that a breach has occurred. A text between a physician and a staff member including PHI is not secure, but it is not a breach until that data is made more widely available – after, for instance, one of them loses his or her phone).

- Does anyone else have access to the devices at issue?

- If a device was lost or stolen, may it be "remotely wiped?" (remotely wiping data from a device, available for many corporately configured devices and some personal devices, like the IPhone, entails removing all data from the phone via a website or similar service, even though the phone is no longer in the user's possession.) Can such a "remote wipe" occur before the current possessor has had time to view or copy the PHI on the device?

Questions?

Contact us for more information:

Jim Wieland	|	jbwieland@ober.com
Sarah Swank	|	seswank@ober.com
Carla Murphy	|	cnmurphy@ober.com
Josh Freemire	|	jjfreemire@ober.com

About Ober|Kaler

Ober|Kaler is a national law firm that provides integrated regulatory, transaction and litigation services to financial, health care, construction and other business organizations. The firm has more than 130 attorneys in offices in Baltimore, MD, Washington, DC and Falls Church, VA. For more information, visit www.ober.com.

This publication contains only a general overview of the matters discussed herein and should not be construed as providing legal advice.