IT@UC
INFORMATION SECURITY

Information Security and Social Media Sites

What happens with the information that we post on social media sites?

When you post information onto a social media site, it will be stored on that site's computer equipment/servers. Often that information is kept indefinitely, even if you choose to delete it later on. Also, the equipment hosting social media site is spread out all over the world to ensure quick response times and high availability. Laws vary as to whom owns data hosted on the server within those geographical territories. In addition, there are a number of legitimate companies that crawl throughout the internet, including social media sites, and build complete profiles as to how those sites look at a point-in-time. Your data may be picked up and stored by such companies.

In what ways is our online information protected?

This is a challenging question to answer. It depends on laws and regulations in different countries, and on corporate security/privacy policies. The most common way of protecting online data is by using a username and password. The majority of legitimate social media sites encrypt communication between your computer or phone and their computer equipment/server that way no one can "listen" to the communication and capture data in motion. Some sites, such as Facebook, automatically remove geo location data from pictures users post to protect the identity and physical location of their users.

Can businesses and companies get access to our online information or social media information?

Most information is publicly available by using Google or other search engines. Searching in this way is perfectly legal. The vast majority of businesses/companies are limited to viewing only user's public profile, unless you accept that business/company as a "friend." Some employers may require job candidates to provide

access to their social media profiles. This is a controversial practice, but it does occur.

Can the government get access to our online information without permission or a warrant?

This depends on laws within different jurisdictions. In the US, law enforcement is allowed to view public profiles. In the majority of states, it is legal for law enforcement to pose as somebody else and send out friend requests. Additionally, the answer to the above question depends on the particular social media site. Some companies are very strict when dealing with law enforcement agencies, and will require a subpoena to release data. Other companies merely confirm that the request came from a legitimate law enforcement or police agency and willingly turn over user data.

What are your views on social media?

Privacy is a luxury that is becoming harder and harder to achieve in a modern high-tech society. Social media sites provide great tools for people to connect and stay connected with their friends, family members, co-workers, business partners, like-minded people, etc. These sites are wonderful for advertising, and building your personal or business brands. The downside to social media is that once you make a post (private or public) or post a picture, you lose control over that data, and you never know who may be able to view that post or picture. Thus, there is very little, if any privacy, on social media sites. People are often responsible for their own loss of privacy. Never post anything that you would not be comfortable w/the entire world knowing one day. Never assume your profile is private (or that it will stay that way).