Social Networking Technologies are Internet-based platforms that enable individuals and organizations to connect with other users of the platform and share information about themselves. The participant's information is displayed as a profile describing the user as well as varying degrees of additional, identifying information. Participants can then view, and at times engage with, the information of the other users with whom they have made a formal connection. Participants can also view the information of users whose information is public.

While there is some debate about which Internet-based platform was the first Social Networking Technology, GeoCities and Sixdegrees.com were two of the earliest precursors to the modern concept. GeoCities, which began operating as such in 1995, provided users an opportunity to easily create free personalized webpages. Those webpages were located within communities called "neighborhoods," which were groupings of webpages that shared similar content. Webpage owners within a community could then search and access the webpages of users who shared similar interests or characteristics. Sixdregrees.com began in 1997 and took a more intentional approach to connecting users. Members of the website could communicate with other users with whom they formalized a connection and could invite non-members to join. Members could also seek out other users on the site and view their relationship to those users. GeoCities ended operations in 2009, ten years after having been acquired by Yahoo!, and Sixdegrees.com ended operations in 2001.

After GeoCities and Sixdegrees.com began the idea of utilizing the Internet to form and maintain relationships between users of a particular platform, Friendster was founded in 2003 with the intent of allowing people to create personalized pages, and then connect and more intimately interact with the personalized pages of others. Friendster took on the form of what is now considered a modern Social Networking platform as it also allowed users to tailor their profile pages with media and other online content. Friendster, however, was plagued with slow connections, which frustrated users and caused them to abandon the service. As Friendster saw its usage decline, MySpace and Facebook, launched in 2003 and 2004 respectively, began to take over and fulfill the public's desire for interconnected relationships on the web. MySpace, however, struggled to keep users as it was ill-equipped and reluctant to accommodate third-party developers; whereas Facebook remained open to their applications. By 2009, Facebook had more than 200 million users while MySpace had 100 million users. Facebook continued its success and by 2013 had over 1 billion users. Facebook's initial structure was premised on empowering users by allowing them to accept or reject requests to access each other's profiles. Therefore, the presumption was that users acted as their own gatekeepers by limiting other's access to the information they present via the platform. Twitter, another Internet platform founded in 2006, presumed open access to information requiring users to affirmatively privatize their information sharing. Unlike Facebook's initial structure, Twitter users could track the sharing of information by other Twitter users without an affirmative, approved bidirectional relationship. As new platforms come online, they increasingly add new options for more intimate sharing of information. For example, sites like FourSquare and Instagram, as well as some of the more established platforms, have allowed users to share the time and location of their activities. As new means are developed to share an increasing amount of information, new platforms are created to facilitate and capitalize on it.

Social networking technologies have been celebrated for their democratization of the exchange of ideas. They have allowed billions of people to access and contribute to public discourse regardless of one's notoriety or affluence. While access to the effective means of communication historically resided with powerful and influential public figures, social networking technologies allow users of the same platform to access and engage with each other's social, political and religious views. Users can instantly approve, share, and respond to other's ideas in a fluid and synchronous manner. These attributes have led some to credit social networking technologies with facilitating substantial social change. For example, the effective use of social networking technology has been recognized as key to U.S. President Barack Obama's 2008 election. Social networking technology is credited with coordinating and enabling the protests that ultimately pushed the communist party from power in Moldova in 2009. Many have also argued that social networking technology played a vital role in the Arab Spring, which was a series of revolutions and civil unrest in the Middle East beginning in 2010 and leading to the overthrow of governments in Tunisia, Egypt, Libya and Yemen.

While social networking technologies have arguably assisted in ushering in social change, they have also enabled the intentional and unintentional sharing of vast amounts of private information. In some cases, social media technologies have been used to disseminate private information about others without their permission and have resulted in civil lawsuits. For example, a medical clinic worker in Minnesota allegedly accessed embarrassing medical information about a patient without the patient's authorization. The clinic worker then disclosed the information to others, which ultimately resulted in a MySpace page containing the information about the patient. The patient sued the clinic worker and the clinic for, among other things, invasion of privacy. Lawsuits have also resulted from the republication of information shared on personal, private social media pages.

In New Jersey, a paramedic maintained a private Facebook page where others could only view her posts if they had permission. The paramedic had permitted friends and coworkers access, however did not give permission to her employer, an emergency medical service provider. After her employer was informed about the paramedic's controversial Facebook post, the employer allegedly coerced some of the paramedic's coworkers to access her account while a supervisor looked on. The supervisor then copied the post and forwarded it on to the state paramedic licensing board alleging that the post demonstrated unprofessional behavior. The paramedic sued her employer and claimed that sharing her private Facebook post was an invasion of privacy. Courts, however, are divided on these sorts of civil claims of invasion of privacy. Some courts have determined that privacy is lost when one posts information on a publicly accessible Internet site, even if their privacy settings are highly restrictive. Other courts have found that an invasion of privacy can occur where the user has created a password protected, private account and limits those who can view it. The question has yet to be resolved.

Criminal charges are also possible where social media technologies have been used to disseminate private information. In 2010, Dharun Ravi used his Twitter account to announce that his college roommate, Tyler Clementi, had asked to use their shared room until midnight. In addition, Ravi stated that he had accessed his computer's webcam and observed his roommate becoming intimate with another man. Ravi then live streamed Clementi's tryst via iChat. Three days later Clementi posted a message on his Facebook page announcing that he was going to commit suicide, and did indeed do so.

Ravi was charged with, among other things, the crime of invasion of privacy, which makes it illegal to record and disseminate another's sexual encounter without his or her consent. In 2012, Ravi was found guilty and sentenced to 30 days in jail, a $10,000 fine, three years of probation, and 300 hours of community service.

While social media technologies often present the appearance of privacy by permitting users to selectively limit access by other users, the government can often access the information shared via social media technologies. If the government is accessing the information, the question arises whether it must obtain a warrant. In *Katz v. United States* (1967), the United States Supreme Court determined that FBI agents could not record an individual's phone call in a telephone booth without a warrant. The Court determined that the Fourth Amendment protected the individual from unreasonable search, not just private places. In his concurrence, Justice Harlan articulated a test that has been used by the Court since. He stated that the government must attain a warrant before a search if: the person to be search has a reasonable expectation of privacy and the expectation is one that society would recognize as reasonable.

In the 1970's, the Supreme Court decided two cases, *Smith v. Maryland* and *United States v. Miller*, which created what is known as the "third-party doctrine." Individuals in those cases had transmitted information to a third-party, a telephone company and a bank respectively. The Court determined that the transmittal of information to a third-party invalidated an individual's expectation of privacy in the information and that the government could access it without a warrant. Social networking technology users often allow some other users of the platform, however few, to view the information they post. In addition, any information posted to a social media platform is, at the least, shared with the organization that owns the platform. Therefore, most courts have found that the government can lawfully obtain that information without a warrant. For example, in a case in New York, a defendant's Facebook "friend" allowed the government to access the defendant's Facebook posts through the friend's account. When the defendant challenged the use of the posts against him in his criminal trial, the court found that the government did not need a warrant, obtained the information from his account legally, and could use it against him in court.

It is not only the government that can take advantage of the lack of privacy protection associated with social networking technologies. Third-parties, as well as the social media platforms themselves, can access and use the information user's share. Information that is publicly shared on social media platforms is often collected and aggregated by third-party organization, including for-profit corporations. These organizations can then use the information to construct a portrait of the user's likes and dislikes, activities, location, and propensities. The constructed portrait is valuable to companies that would use it for the purposes of marketing their products. It is can also be used by companies to anticipate the likelihood a user will default on a loan or be an insurance risk. Additionally, politicians use the information gleaned from social networking technologies to micro-target their messages and get-out-the vote efforts. The social networking platforms also use the information their users share in similar ways. Users that express interest in a particular product, share their location and activities, or share a major life experience will often see advertisements directed to those characteristics.

Criminals have also been known to use the lack of privacy in social networking technologies for nefarious purposes. While many social networking platforms allow users to share their location, some primarily rely on user's posting their activities and locations so that other users can find recommended businesses and services. In addition to intentionally sharing one's location and activities, sharing pictures via social networking platforms can unintentionally reveal location through geotagging—geographically identifiable metadata. Whether intentional or otherwise, criminals can use this, and other information, to their advantage. For instance, users have been burglarized after sharing their location and revealing that they are not home or plan not to be home at a particular time. Cyberstalkers are able to use information posted on social media platforms to learn their victims' patterns and more easily threaten, harass, or attack them. Criminals can also build a picture of users by collecting available, personal information and ultimately steal the user's identity.

Social media technologies have had a significant impact on societies throughout the world. Since their beginnings, they have served to connect people to one another, facilitate relationships, and foster the sharing of information and ideas. However, along with this virtually unfettered freedom to share ideas, social media users may find themselves making a trade-off. When users engage with the technology they find themselves, almost necessarily, giving up some of their privacy. In the digital age we are faced with a Hobson's choice. We can protect our privacy to the greatest degree possible by avoiding social media technology, thereby missing out on all it has to offer. In the alternative, we can embrace the technology knowing that, in doing so we, we give up a claim to some of the privacy we would otherwise have.

Further Reading:

Reinecke, Leonard; Trepete, Sabine. *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*. New York, NY: Springer Publishing Company, 2011.

Silverman, Jacob. *Terms of Service: Social Media and the Price of Constant Connection*. New York, NY: HarperCollins, 2015.

Cross-References:

Arab Spring

Barack Obama

Facebook

Katz v. United States

MySpace

Twitter

Contributor:

Douglas B. McKechnie, Assistant Professor, United States Air Force Academy. BA, Ohio University; JD University of Pittsburgh School of Law. Professor McKechnie teaches in the Legal Studies Department at USAFA; his scholarship focuses on the intersection between civil liberties and technology. The views expressed herein are Professor McKechnie's and do not necessarily reflect the official policy or position of the United States Air Force Academy, the U.S. Air Force, the Department of Defense or the U.S. Government.