

Digital culture: What does it mean for the future of American privacy?

Today, there are more than 400 million Facebook users. More than 75 million people have a Twitter account. According to the Nielsen Co., text messaging now outpaces phone calls among mobile-phone users. Taken together, these trends represent more than simple shifts in communications technology.

Changes in the digital realm have altered how we communicate, what we communicate about, and even the nature of our interpersonal relationships. Before 2004, Facebook did not exist. Today, many Americans choose to divulge significant amounts of personal information via such online social networks. Spurred by evolving technology and changing social mores, the line between the public and the private has become increasingly indistinct.

Within the past few years, there has been much commentary about the psychological and social aspects of these trends. Timely works such as the 2009 documentary film "We Live in Public" have examined the attractions — and costs — of our culture's digital obsession. What is less well understood is how changing technology and cultural norms are outpacing — and altering — the legal mechanisms that govern American privacy.

Privacy and government searches

The changes that have affected America's privacy landscape are many and varied. Some phenomena — such as the rapid adoption of social networking — are easy to recognize. Others are comparatively hidden. For example, as Americans have rushed to take advantage of the explosion of Internet technology, few have stopped to consider the relatively murky legal protections afforded to online activity.

In our legal system, privacy protections against government searches are provided by state and federal laws, and by the Constitution's Fourth Amendment, which provides that "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."

Over time, courts have developed different frameworks as they have grappled with how to apply the original intentions of the Fourth Amendment to new social circumstances.

Originally, the Fourth Amendment was understood to protect physical assets — one's house, for instance — against unreasonable searches. Later, as technology and court doctrine evolved, other protected categories were added. In its 1967 decision *Katz v. United States*, the Supreme Court recognized Fourth Amendment protection for private telephone calls.

Not every search and seizure decision by the Supreme Court has represented an expansion of Fourth Amendment parameters. For instance, a 1976 decision involving "third party" records exempted many seizures from Fourth Amendment requirements. It is this framework — set out by the *United States v. Miller* case — that governs how federal courts view much of what happens online today.

The third-party doctrine

Under the "third party doctrine" established by *Miller*, personal materials held by a third party (such as a bank) are not treated the same as personal materials held by an individual.

To obtain a warrant for the search of a home, police must first demonstrate "probable cause" of a crime to a judge, who then evaluates whether evidence of a crime might be uncovered by the search. Third-party searches, on the other hand, can be conducted without meeting the Fourth Amendment's probable-cause requirement.

The 1976 *Miller* decision dealt explicitly with bank documents. Subsequent decisions expanded the third-party doctrine to cover incoming/outgoing call records and other materials. Now, in the age of the Internet, *Miller* has far-reaching ramifications for online activities. We operate in a world in which more and more personal information is held by third parties. Indeed, the vast majority of online material is hosted on third-party servers.

The more tech savvy (and the younger) that you are, the more likely it is that you have significant amounts of personal material stored online. Many Internet business models are predicated on this very assumption. Google, for instance, has endeavored to become the central storehouse for people's personal and business documents. The company's Google Docs service

allows users to upload material to a so-called "cloud" storage system that can be accessed from any computer, making document retrieval easy by decoupling it from dedicated hard drives.

This convenience comes with drawbacks, however. The third-party doctrine exposes these materials in ways than conventional, physical storage does not. While some may think that documents sitting in a desk drawer and documents hosted on a remote, password-protected server have the same level of privacy, current case law can view these two scenarios very differently.

Digital search doctrine continues to develop

Federal courts have not comprehensively re-evaluated the third-party doctrine in light of new technological developments. In some ways, this is due to the generally slow pace of the U.S. legal system. For example, only within recent years have some federal courts begun to hold that e-mail content is protected by the same Fourth Amendment standards as telephone calls.

To be sure, this issue is not unique to digital communications. In many areas of our society, developments in life outpace developments in the law. Interestingly, defenders of the third-party doctrine make just this point. They contend that attempts to develop detailed Fourth Amendment rules for rapidly developing technologies are likely to be overly complex and burdensome.

At some point, courts are bound to revisit the third-party doctrine as it applies to digital searches. For now, federal search-and-seizure law rests in a murky place, just as third-party digital storage races ahead.

Social media and privacy

Issues involving digital privacy currently sit at a unique tipping point. On one hand, federal courts have not yet recognized that aspects of the digital realm should be governed by traditional notions of privacy. On the other hand, our digital culture is moving in a direction that may undermine the recognition of such expectations. In large part, social media are at the forefront of this countervailing trend.

In some ways, the widespread use of social media has turned the traditional American privacy paradigm on its head. Rather than being concerned about

their inclusion (and exposure) in a computer database, potential users are generally eager to participate in online social networks. Individuals have been joining such networks in droves in recent years, creating communication loops that are only accessible to other network users. In order to participate in these conversations, outsiders are required to join, thus expanding the networks.

Today, Facebook reigns as the premiere social networking company. Since 2006, it has been trying to develop a sustainable business model around its demonstrated ability to attract millions of users who willingly enter untold terabytes of personal information. Facebook's attempts to monetize this information have resulted in many novel flaps regarding online privacy.

Starting in 2007, Facebook's Beacon program automatically tracked online purchases a user made at partner sites, and then sent notifications to the user's "friends" on the Facebook network. For example, renting a movie on the Blockbuster Video website triggered a Facebook notification about the user's future movie-viewing plans.

Facebook CEO Mark Zuckerberg apparently reasoned that younger users would not be troubled by the sharing of such information, since privacy norms have changed. Among older user sets, this assumption backfired. In late 2007, MoveOn.org mounted a noisy public campaign to modify Beacon. Ultimately, Facebook allowed users to "opt-in" to Beacon, rather than making it an automatic network feature.

Facebook has also been criticized by some who claim that there is no truly effective mechanism for removing personal information from the network. Others have complained that the service tries to push more and more "private" information — such as profile photos and lists of friends — into the public realm.

Ultimately, these controversies boil down to clashes between user expectations and a corporate culture that does not hold the same privacy values. Users of social media, it should be noted, have actively chosen to share their information, and are bound by the "terms of use" that govern a particular networking service. However, there is sure to be a spate of litigation over the transparency of these terms in coming years.

Beyond these controversies, the popularity of Facebook raises an even more fundamental question: Is social media undermining our basic cultural assumptions about privacy?

The changing nature of privacy expectations

Last year, a friend tried to persuade me to join Facebook. He spoke passionately about the benefits that it afforded — particularly its utility for keeping track of far-flung friends. Our talk eventually turned to the Beacon feature, and the data-mining of personal Facebook information. My friend was blunt on this point. "Twenty years ago," he told me, "People would have taken to the streets over something like that. Today, it doesn't bother me."

Since its spread from college and high-school communities to the wider society, Facebook has been embraced by people of all ages. At the same time, its most vigorous users have tended to be younger adults who came of age when the line between the "public" and the "personal" was being increasingly blurred by digital technology. These flexible social perceptions will inevitably have an impact on the legal standards that govern our lives.

Members of "Generation X" are just now starting to be appointed to the bench. They will be followed in a few years by the even more digitally attuned "millennials." Going forward, it is these individuals that will determine which searches, for instance, are "reasonable" under the Constitution's Fourth Amendment.

This could cut in two directions. A diminished sense of the private could generate case law that views privacy in a very narrow sense, and authorizes a broad view of "reasonable" digital searches. On the other hand, ongoing changes in society and technology could eventually force a legal consensus that additional protections are warranted. For example, in the early years of the telephone, the Supreme Court held that warrantless wiretaps were permissible, due to the fact that the tap was not a search of a person's physical property. It took Congress and the courts several decades to arrive at the Title III system we now use to govern telephone privacy.

The future of American privacy

What transpires on the privacy front in the coming years will have long-term ramifications. There will be ongoing debates in courts and legislatures, of course, but there will also be more individualized decisions to be made. The

ways in which we manage our own digital footprints will be at the heart of these decisions.

At some fundamental level, Americans are going to have to ask themselves about the degree to which they are willing to openly expose their personal information within the digital environment. In short, how much "Facebooking" is too much? These aggregate, individual decisions have the potential to affect us all. Fourth Amendment conceptions of "reasonableness," after all, are predicated on social expectations of privacy. An American society without coherent cultural notions of "public" and "private" would have no reliable benchmarks for constraining the growth — or the uses — of the government's search powers.

Changes to our culture's privacy framework are not incidental matters. Conceptions of personal privacy cut to the heart of our national identity, and undergird our country's institutions. In 1928, Supreme Court Justice Brandeis wrote that the "right to be let alone" is among the cultural values most cherished by civilized people. It is a value, he wrote, that flows directly from those who framed our Constitution.

The challenge for our culture — and our legal system — in the coming decades will be to determine to what extent this value will continue to guide us.

Originally published at Minnpost.com | Monday, March 29, 2010