A
ticle 20 of the Universal Declaration of Human Rights protects the right to freedom of peaceful assembly and association. In the US, the First Amendment to the Constitution similarly protects freedom of association: “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.” The US Supreme Court has strongly protected this right.

In the 1950s, the state of Alabama required organizations doing business in the state to give the state their membership lists. The phrase “doing business” was broad enough to include nonprofits involved in political activity. In the mid-1950s, if the National Association for the Advancement of Colored People (NAACP) had handed over its membership lists, the organization would have put members’ lives at risk.1,2 In 1964, in the case of the National Association for the Advancement of Colored People v. Alabama, the Supreme Court ruled that information on with whom you associate is private.3,4 Basing its decision on “the right of the people peaceably to assemble,” the court ruled that the NAACP need not release its membership list to the state of Alabama. Privacy by association was a right with teeth.

But is the guarantee of association privacy still real in the US—or anywhere else?

Privacy and Democracy
One of the hallmarks of a democracy is that voting is private. You go into a booth, draw the curtain, mark your ballot, and leave. Yet, in the US, voting is essentially public. You log on to Facebook and connect with your friends. Even if you haven’t “friended” Barack Obama or Mitt Romney, your vote for president can likely be deduced if a sufficient number of your friends
have friended a particular candidate. Or if that’s not the case, your interests likely give away your electoral preferences. These predictions don’t arise from pie-in-the-sky thinking. Alex Lundry notes, “Think of that blue-collar Independent that sat out the last election and lives in an overwhelmingly Democratic precinct—traditional targeting most likely leaves that voter untouched. Micro-targeting allows you to look at that voter and see that he also drives a truck, owns a gun, has three kids and is very angry about illegal immigration.” From those interests alone, you have a high likelihood of knowing how this person will vote in an election between Obama and Romney, even though you’ve never polled him.

Is democracy possible in a state in which everyone’s political interests are visible on Facebook? Indeed, is privacy possible in a state in which everyone’s interests are visible via their postings—and those of their friends—on online social networks (OSNs)? This special issue of IEEE Security & Privacy tackles these issues.

**In This Issue**

There are many ways to view OSN privacy issues; this issue includes several.

“Privacy and Online Social Networks: Can Colorless Green Ideas Sleep Furiously?,” a survey article by Balachander Krishnamurthy, covers both policy and technical efforts, laying out the cat-and-mouse game of privacy protections in the OSN world. Krishnamurthy asks why these protections have largely failed. He persuasively argues that the problem is that proposed techniques are syntactic, whereas semantic protections are needed.

The next article, “All the Better to See You with, My Dear’: Facial Recognition and Privacy in Online Social Networks,” by Norberto Nuno Gomes de Andrade, Aaron Martin, and Shara Monteleone, examines biometrics and OSNs. With facial-recognition systems increasingly ubiquitous on the Internet, you’re no longer anonymous when walking into a bar or bookstore. What’s the impact of the combination of facial-recognition technologies and OSNs on the privacy of users in “meatspace”—the part of the world where we meet in person? Can laws and government policies preserve a modicum of privacy? The authors provide an analysis on the policy, legal, and business implications for privacy when biometrics and OSNs meet in the real world.

What is privacy anyway? Is it protecting the protester in Tahrir Square? Or is it protecting the privacy of an OSN user in San Francisco? In “Two Tales of Privacy in Online Social Networks,” Seda Gürses and Claudia Diaz take the murk out of political activists’ and consumers’ differing privacy requirements. After all, privacy solutions are only as useful as a researcher’s or developer’s understanding of the underlying problems. By providing clear-cut distinctions, the authors clarify what protections are necessary to address diverse issues of OSN users around the world.

The next article takes a view from a different vantage point. Computer scientists think about bits and bytes, whereas social scientists think about people. They ask deep questions about users that more technical folks often don’t consider. Although technologists build and support OSNs, the networks are ultimately about people. In “New Strategies for Employment? Internet Skills and Online Privacy Practices during People’s Job Search,” Eszter Hargittai and Eden Litt examine how demographic factors affect users’ self-presentations on OSNs. Surveying more than 500 young adults, the authors discover how gender and ethnic background influence the ways users protect their privacy. In seeking to provide privacy protections in OSNs, we have much to learn from our colleagues studying the “softer” sciences. This article provides our community with an excellent start.

For many, the OSN world is beginning to look quite grim (or as the old line goes, “You have zero privacy anyway. Get over it!”). We computer scientists are engineers. We build things. The final two articles of the special issue consider how we might design for privacy in OSNs.

In “Twitsper: Tweeting Privately,” Indrajeet Singh and his colleagues present a simple Twitter add-on that lets users share messages with any subset of their subscribers. Backward compatible with Twitter, the new technology provides privacy without impacting Twitter’s commercial interests. It’s a small idea, elegantly executed. One can’t ask for more.

Finally, in “Must Social Networking Conflict with Privacy?,” Jonathan Anderson and Frank Stajano take a different approach to building OSNs with privacy. What happens if we relax the requirement that an OSN be free for its users? With the customer no longer necessarily the commodity, various choices arise for protecting users’ information. Private information could be encrypted at the OSN or distributed among several sites; friends of friends could be found indirectly rather than through the OSN. Using economics as a guiding principle, the authors explore options. They conclude with the example of Footlights, a privacy-oriented OSN platform that lets users run distributed social applications without having to unconditionally trust the apps.

Whether offline or online, privacy protections remain critical in today’s civil rights battles. As of this writing, nine US states and several nations in South and Central America and Europe have legalized
same-sex marriage. But only 15 years ago, a young man in Laramie, Wyoming, was lured from a bar, kidnapped, beaten, and then tied to a fence post where he died—all because he was gay.7 In many parts of the world, same-sex activities are illegal.8 Discrimination and violence against gay people is not only tolerated but is sometimes actually encouraged by the government.

Even without an explicit acknowledgment, the fact that someone is gay is relatively easy to determine on the basis of his or her Facebook friends.9 In the world of OSNs, politics, love, and death aren’t private matters. That doesn’t mean they shouldn’t be. If the set of articles in this special issue helps in developing privacy protections for OSN users, the authors and I will have done our jobs.

References

Susan Landau is a Guggenheim Scholar at Privacyink.org. Contact her at susan.landau@privacyink.org.

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.