A few summers ago two University of Illinois students spent an evening barhopping. In between stops, one of them urinated behind a bush. Campus police spotted him, but he was able to slip away. A cop did question the student’s friend, who claimed he didn’t know the fleeing drinker. But when the officer later looked on the friend’s Facebook page, he discovered that wasn’t exactly true—the two students were indeed friends (or Facebook friends at least). Long story short: The urinator was fined $145; his friend faced a heavier penalty ($195) for obstruction of justice.

As we begin to live parallel lives on the web, our privacy rights are slipping away. Colleges and companies routinely search Facebook and Twitter to determine whether to admit students or hire employees. According to a 2009 Harris poll, 35 percent of employers have rejected job applicants because of information gleaned from social networks—the person may have dressed provocatively in photos, written about drinking or complained about past employers, co-workers or clients. A 16-year-old girl was fired from a U.K. marketing firm for writing on Facebook that her job was boring, even though the company’s name wasn’t mentioned. And when workers at a New Jersey restaurant established a password-protected MySpace page to grouse about their employer, their online complaints cost them their jobs.

Insurers, too, seek access to social-media posts. In New Jersey, the parents of two teenage girls sued Horizon Blue Cross Blue Shield for coverage of medical expenses related to eating disorders. Horizon argued that the disorders were due to emotional and social pressures, not a medical condition. The judge granted Horizon’s request for access to the girls’ “writings” related to eating disorders on social-networking sites. The case was settled when Horizon granted broader coverage. But in other instances, a legal order to expose social-network information may cause plaintiffs to drop a case to avoid the emotional distress of having their most private thoughts made public.

When the founding fathers drafted the Constitution, they sought to protect people’s privacy in their homes. And as new technologies have emerged, the Supreme Court has continued to value privacy. In 1967, after cops placed a wiretap on an L.A. phone booth and recorded a local man calling Boston and Miami bookies, the Supreme Court protected his privacy, enunciating a legal test that is still used today: Did the person have an “expectation of privacy”?

But what is our expectation of privacy in the era of social media? In 2009 a California appellate court declared “no reasonable person would have had an expectation of privacy” for a social-network post. But courts are abdicating their responsibility to protect privacy when they come to such a conclusion. This is like saying we shouldn’t have laws against Peeping Toms since, if you own a house with windows, anyone can look in. By defining the expectation of privacy as an objective matter (all digital information is accessible by someone), the courts have failed to recognize that people often believe their postings are available only to their friends.

What can be done to ensure that people who join social networks have as much privacy protection as people who enter phone booths? Here are my suggestions:

Courts and legislatures need to recognize the importance of privacy. Disclosure of private posts and e-mails can be emotionally devastating. When a college student briefly posted a derogatory poem about her hometown on her MySpace page, the high school principal gave the poem to the local newspaper, which published it under the student’s name. Her family received death threats and had to abandon their business. While the court refused to acknowledge the girl’s privacy rights, it did say she might have a legal claim for intentional infliction of emotional distress.

People should be able to control their privacy settings. About 25 percent of Facebook users employ privacy settings, but many others may just not know how. And some privacy choices are thwarted when a social network changes its protocols. A 2009 complaint filed by the Electronic Privacy Information Center with the Federal Trade Commission shows the harm that occurred when Facebook changed its policy so that lists of friends and affiliations were designated as public information no longer subject to users’ privacy controls. In Iran, authorities questioned or detained the Facebook “friends” of Tehran’s U.S.-based critics. Facebook subsequently reversed its policy and now allows users to control the privacy of their friends list. To protect against such abuses, privacy settings should be designed so people have to “opt in” to wider dissemination rather than having to “opt out.”

Fake friending to obtain information should be forbidden.
The California legislature recently passed an "e-personation" ban, making it a crime to impersonate someone within a social-media network. In 2009 the Philadelphia Bar Association’s Professional Guidance Committee concluded that lawyers can’t ask other people to “friend” a witness to gather evidence to impeach the witness. The committee was adamant that it didn’t matter if the person was willing to accede to all friend requests: “Deception is deception, regardless of the victim’s wariness in her interactions on the Internet and susceptibility to being deceived.” A lawyer claimed that fake friending was no different from videotaping a plaintiff in a personal-injury case to show she wasn’t really injured. The committee disagreed, considering social networks to be a private space. While lawyers may be able to videotape a witness in public, fake friending would be like posing as a utility worker and using a hidden camera to film someone inside her home.

Employers and insurers should be forbidden from using social-network information. In the U.K., insurers want to raise home-insurance rates for people who merely possess a Facebook page because thieves—including a robbery ring in New Hampshire—use posts about vacations as a guide for break-ins. In contrast, proposed legislation in Germany would restrict the use of social media by employers so they can’t deny employment or promotion based on social-network postings.

If judges don’t correctly apply existing privacy doctrines to social networks, new laws should be enacted. When Robert Bork was nominated for the Supreme Court in 1987, *Washington City Paper* attempted to discredit him by publishing his movie-rental records. In response, Congress passed a law protecting the privacy of such information. The bill’s sponsor, Vermont Democratic senator Patrick Leahy, noted that privacy protections are needed in “an era of interactive television cables, the growth of computer checking and checkout counters, of security systems and telephones, all lodged together in computers.” If what I rent from Netflix can remain a secret, then the more intimate information about my political affiliation, workplace woes and opinions about friends should be even better protected.

Court decisions on the use of social-media information test the boundaries of privacy and free speech—and raise emotional issues of stigmatization, betrayal and discrimination. If we don’t act quickly, our long-revered tradition of privacy will soon be as antiquated as the Commodore 64.

Lori Andrews is a law professor at Chicago-Kent College of Law, where she directs the Institute for Science, Law and Technology.