In 2008, I published a column about identities, including a brief discussion about how I sometimes turn to social networks such as LinkedIn or Facebook to find people because their information in the social network tends to be more current and reliable than their “home-pages.” I also mentioned an old acquaintance who seemed to have simply “fallen off the grid” and become unreachable through the usual methods. Given some recent experiences and articles in the media, I thought it a good time to revisit this topic.

Social networks have become ubiquitous. When I briefly encountered someone I hadn’t seen in some time, and later wanted to look him up, Facebook seemed like the logical place to turn. Our status as ever-connected “friends” would make posting a friendly note on his wall simple. Yet, try as I might, I just couldn’t find him in my friend directory. My first reaction was that he had (gasp!) “unfriended” me — perhaps we didn’t interact enough, or perhaps he was dropping friends to improve the signal-to-noise ratio in his news feed. But I couldn’t find him on Facebook at all. So either he had both unfriended me and set his account to be unsearchable, or he had left Facebook.

I resorted to old-fashioned email. It turned out that he had indeed closed his Facebook account due to a combination of not using it much and concerns over privacy. He sent me a link to an MSNBC article entitled “Details of 100 Million Facebook Users Published Online” (www.msnbc.msn.com/id/38463013/ns/technology_and_science-security), which discussed how an online security consultant crawled public Facebook data and made a single compendium of users’ profile data. The article pointed out that this snapshot essentially ensured that any data a user previously kept public and subsequently protected would always stay public.

Problem? Not in my book. With the creation of the “Wayback Machine” (www.archive.org/web/web.php) years ago — a website that crawls and archives webpages and allows users to view webpages as of a point in time in the past — social network data isn’t the only information that can take on a life of its own; any data on the Web that was ever public is presumed to be accessible indefinitely. If someone put their birthday publicly in their Facebook profile and thought better of it later, the damage has really already been done. It’s not reasonable to complain to either Facebook management or the people who collect these snapshots and argue that they invaded users’ privacy — these users made the information public! (Of course, if you limit access to your birthday or other personal information to friends only, that data shouldn’t turn up in a public snapshot, right? Right.)

The Element of Surprise

My acquaintance is neither the first person I know to abandon Facebook nor the first example of a social network link withering away. The problem for me isn’t that my connections might decide to leave either our personal link or the entire system, but rather the subterfuge with which it happens. Social networks like Facebook and LinkedIn are really geared toward establishing connections: notifying users when others ask them to connect with them, when invitees accept their invitations, and when they might be acquainted with other users they aren’t currently linked to. But these same networks are really bad, perhaps intentionally, at notifying users about the reverse … but why? When I posted political content on Facebook during the 2008 US election, one of my “friends” quietly dropped me rather than see my posts. As in the case I described earlier, I noticed this only by accident. But, in this case, I could see the account existed, so I was clearly removed by design. (I should add that I was reinstated, along with a few others, when the person learned there were other ways to tone down our impact on his feed.)
And what if you do want to abandon Facebook? In general, you can “deactivate” a Facebook account but must then go a full two weeks without using it for the account to be deleted entirely. In the meantime, they tell you how much so-and-so and so-and-so will miss you and hope that you’ll change your mind. (As an aside, according to a rumor [http://yro.slashdot.org/story/10/07/26/1240257/Facebook-Adds-Delete-Account-Option], Facebook has apparently decided to make it easier to entirely delete your account, so deletion might be expedited in the future.) But what should happen when the deletion takes place? Maybe so-and-so really will miss you ... and deserves to know you’ve moved on to a better place.

Seriously, as painful as the news that someone has unfriended you might be (or not), the change to your relationship should be made apparent, right? A message that “John Smith has left Facebook” would be particularly helpful — you don’t even have to take the departure personally! Of course, not everyone necessarily wants to know about these changes, and some people (especially teenagers) could well be in such volatile networks that they would be a distraction, but on the whole I like the option.

Social Presence and Lack Thereof

Because I’m on the topic of removing social network presence, I’ll finish with a comment on the care and feeding of your online persona. I imagine that the vast majority of IC readers have tried at least one or two major social networks by now, even if they don’t use them regularly. Similarly, many of us have other types of Web presence, such as blogs, more static homepages, and so on. But what if we don’t, or what if our presence doesn’t convey what it should?

As I wrote this in late July, two recent news items caught my eye (or ear). NPR ran a piece about modern motorcycle gangs and how the US government can’t do much about them unless they can infiltrate them (see www.npr.org/templates/story/story.php?storyId=128826377). I was both surprised and amused to hear that biker gangs now do “background checks” on people trying to join:

The strategy poses some risks [for the government]. [Terry] Katz, the long-time gang investigator, says biker gangs have gotten sophisticated. Some use polygraphs and private investigators to check out new members. Others scour

Technical cosponsor:

IEEE Internet Computing
IEEE Computer Society Publications Office
10662 Los Vaqueros Circle
Los Alamitos, CA 90720 USA

Editorial. Unless otherwise stated, bylined articles, as well as product and service descriptions, reflect the author’s or firm’s opinion. Inclusion in IEEE Internet Computing does not necessarily constitute endorsement by IEEE or the IEEE Computer Society. All submissions are subject to editing for style, clarity, and length.

Submissions. For detailed instructions, see the author guidelines (www.computer.org/internet/author.htm) or log onto IEEE Internet Computing’s author center at Manuscript Central (https://mc.manuscriptcentral.com/cis-ieee). Articles are peer reviewed for technical merit.

Letters to the Editors. Email content editor Rebecca Deuel-Gallegos, re.deuel-gallegos@computer.org.


Subscribe. Visit www.computer.org/subscriptions.

Subscription Change of Address. Send requests to address.change@ieee.org.

Missing or Damaged Copies. Contact help@computer.org.

To Order Article Reprints. Email internet@computer.org or fax +1 714 821 4010.

court records for evidence that applicants to the gang may have testified in a criminal case against bikers.

The other item came from Bruce Schneier’s blog (www.schneier.com/blog/archives/2010/07/technology_is_m.html), reporting that technology makes it easier for counter-espionage groups to foil espionage. One aspect of this is that “ubiquitous collection of personal data makes it harder to maintain a false identity.” So, what happens when a government agency wants to place an agent in a gang, or a country wants to pass someone off as a national of a different country, living there long-term? The back story to establish them with a particular background gets harder the more our lives are public, open books, intertwined with so many others. Even if a sophisticated organization can fabricate a fully mature, established online persona, an even more sophisticated organization can tear that apart by looking not only at what someone looks like today but also at what databases such as the Internet Archive or the Facebook crawler say about how that person looked sometime in the past. Sounds like a good plot for a movie, anyway.

The creation of a mythical online persona is just one facet of the institutionalized social snooping I’ve described. It seems widely accepted that some employers, and possibly colleges, check out applicants online. It boggles the imagination — mine, anyway — to think about some of the things that people expose on social networks like Facebook. And, although I don’t condone attempts by prospective employers to break down the wall between what is shared publicly and what is private (http://tinyurl.com/job-applicant-screening), cases also exist of people opening the door quite explicitly (http://tinyurl.com/friend-your-admissions-officer). Who needs to worry about suppressing the photo of that drunken extravaganza when you make your life an open book? Crazy teenagers!

Acknowledgments
The opinions expressed in this column are my personal opinions. I speak neither for my employer nor for IEEE Internet Computing in this regard, and any errors or omissions are my own. I thank my own teenager, Allison Douglos, for her very helpful comments on this column.

Reference

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