

Peer-Produced Privacy Violations

Social Media and the Commodification of Community
Roundtable Workshop
University of Haifa Faculty of Law
30 May 2008

James Grimmelman

New York Law School
57 Worth St.
New York, NY 10013
james.grimmelman@nyls.edu

This work may be freely reused under the Creative Commons Attribution 3.0 United States license
<http://creativecommons.org/licenses/by/3.0/us/>

I'm going to talk about privacy and social network sites.

It might seem that these sites would be better at preserving privacy than sites with a broadcast-to-the-world model, since information flows can be limited to one's network. In fact, the nature of information-sharing on them leads to recurrent conflicts and misunderstandings among users, with consequences that are often experienced as privacy violations. I'll spend most of my time talking about how it happens, and conclude with a few tentative lessons we might draw.

Following boyd and Ellison, I'm taking a social network site to be a web-based service that allow individuals to

- (1) construct a personal profile
- (2) articulate a list of other users with whom they share a connection,
- (3) view and traverse their list of connections and those made by others

This is a narrower definition than some other speakers have used. I'm focusing on sites that make the social graph explicit (like Facebook), and which are really built around it, rather than on sites with heavy user-generated content (like YouTube) or sites with less formally structured socializing (like discussion boards.)

The literally defining feature of these social networks is that they invite users to craft social, networked identities. At one level, this means creating a persona for the site: you are what you present yourself as, to your contacts, in the context of the site, using the site's lexicon of profile questions and communication features. The near unreadability of many Myspace pages, for example, comes from the same source as the weird clothes kids these days wear: it's an aesthetic that says, "peers, I'm one of you; adults, this isnt for you."

Each person's personal information is then used to induce others to contribute their own. If you post your relationship status, I need to post mine to reciprocate. By creating a profile and friending you, I gain access to your circle of contacts. And if you have 250 (notice how sites so helpfully display totals), maybe I want to have 300.

The presence of this personal information also inclines us to perceive the network as both "private" and "safe" space, even subconsciously. It's hard to estimate the risk that releasing a little private information now will bite us later, so we use our peers' actions as a heuristic to tell us whether it's safe to speak freely here. If they share, we share.

The net result is that a great deal of personal information flows into one's network. Not social security numbers, but information about relationships, friendships, residence, interests, affiliations, background, and activities.

Say it with me: Facebook is a privacy virus: i.e. an organism that reproduces itself within a social network by turning hosts' self-defense mechanisms against themselves and then convincing the hosts to use their replication mechanisms to spread it to others.

Consider some of the results:

- College officials look at Facebook pages for photos of students binge drinking.
- If I didn't know you were on the site, and one of my contacts adds you as a contact, whoops: you've now got access to my profile.
- What if one of your students adds you as a contact, and then starts pumping embarrassingly badly-written messages to your Wall?
- Or take Beacon. The way that one actually explodes is that outside information about your purchases is pushed out to your network. Now everyone knows what awful movie you rented.
- And Facebook now has as a “photos of” feature; it's one click from your profile to every awful photo of you every posted by anyone to the site and tagged as being a photo of you.

Thus, we return to the darker side of the fact that these sites are about social, networked identity. First, what's at stake in these examples is control over your self-presentation. Beacon disrupts this by telling everyone what movies I *actually* rented, not that idealized subset I'd rather use to say who I am. The same goes with the tagged photos and the wall posts; your contacts are now saying, in effect, who you are, and they don't always say things that match who you want to be. Bracket the question of whether these *are* privacy harms. They're subjectively experienced as privacy harms, which should be enough for us to be concerned.

Second, by making the network—the social graph—explicit, they force lots of issues out into the open. Perhaps I can deal with talking to you in real life, although I dread the experience. On a social network, I can't exclude you from my network without being open about it.

And third, many pieces of personal information now have multiple “owners.” You post a photo; she tags it as being a photo of me. That's three of us now implicated in the photo. Even the social graph itself has this feature: every link has two endpoints. Indeed, we're now learning that it's possible to infer things about people just from looking at the network: if I have lots of friends at Barnett College, maybe I go there, too, even if I don't list it in my profile!

Let me list a few of the consequences that I think follow:

Note, please, that these are privacy harms inflicted by peers, not by marketers or government. Of course, these other forms may also be present, and the decisions made by the social network will affect what your peers can do to you, but these are still primarily user-to-user issues.

Note also that given the nature of these privacy issues — information flows where it's not wanted within a social network — we ought to be very careful about data portability. As appealing as it may be to require strong portability as a way of reducing power imbalances vertically, so that users aren't locked into one platform and can't be abused by the network, doing so undercuts whatever privacy rules are baked into a user's network of choice. Unless we're prepared to dictate the exact set of features every social network has, portability creates a privacy race to the bottom.

I'd also tentatively say that I doubt any set of technical rules can properly preserve user privacy in social networks from other users. People have social motivations for wanting to know things about each other and to communicate with each other. Indeed, these are their motivations for using these sites in the first place. The privacy trouble comes as soon as any two of us have even slightly different ideas about the norms of information-sharing. Think about social life and the complexities of relationships and about privacy and confidences, and I think it's clear that ambiguities and disagreements will arise all the time. Better network design will not magically resolve them for us.

Given this, while there are better and worse social networks for privacy purposes (some of Facebook's lurches come to mind), and while there is a role for law in pushing networks from worse towards better (some of Facebook's lurches again come to mind), some measure of these peer-produced privacy violations will, I think, be inevitable in any social network worth using. We use them for the same social reasons that lead to the trouble. I'm not entirely sure that law ****could**** get rid of social networks at this point, and I very much doubt that it should. It could be that our concepts of privacy and identity are in for some very large shifts. But if they are, the transition is going to be ugly.