

Saving Facebook: A Response to Professor Freiwald

*James Grimmelmann**

My thanks to Professor Susan Freiwald for her generous and thoughtful comment¹ on *Saving Facebook*.² I wrote the article to spark discussion, and her comment is an encouraging indication that privacy scholars are engaged in a serious conversation about social network sites. In this brief response, I address three of Freiwald's points, all of which go to the heart of my project in *Saving Facebook*.

First, Freiwald asks whether Facebook is just a technological mayfly, shortly to go the way of Webvan—and if so, whether articles about Facebook will soon be just as obsolete as articles about the dial-up version of America Online. Though she kindly goes on to say that *Saving Facebook* transcends Facebook, the deeper question remains: *why Facebook?* If my goal was to make enduring points about the social nature of online privacy, why tie them to a platform that may turn out to be a flash in the pan?

My answer, such as it is, is in the first sentence of the article: “The first task of technology law is always to understand how people actually use the technology.”³ Legal scholarship in general, and Internet law scholarship in particular, suffer from a surfeit of theory and a sometimes distressing inattention to facts. *Saving Facebook* goes deep into the details of Facebook because unless it went deep into the details of some social network site, it would be neither correct nor persuasive. I argue that social-network-site privacy is pervasively tied up with the patterns of socialization on those sites; my argument is meaningless without a factually rich portrait of those patterns.⁴ Perhaps, like Buddhists, we scholars can abandon our boats once we're on the far shore of enlightenment, but we'll never get there without sustained, careful attention to factual specifics.

* Associate Professor of Law, New York Law School. Internet citations are formatted according to conventions suggested by the author, which may be found at <http://james.grimmelmann.net/essays/CitationPrinciples.pdf>.

1. Susan Freiwald, *A Comment on James Grimmelmann's Saving Facebook*, 95 IOWA L. REV. BULL. 5 (2009), http://www.uiowa.edu/~ilr/bulletin/ILRB_95_Freiwald.pdf.

2. For the full article, see James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137 (2009).

3. *Id.* at 103.

4. *Id.* at 115–22.

Second, Freiwald stages—with a mercifully gentle touch—a Grimmelmann-vs.-Grimmelmann debate on what we ought to expect in the way of user demands for privacy from Facebook. On the one hand, I argue that Facebook users will expect more privacy than they get and that the market won't help them get more. On the other, I tell multiple stories about how Facebook backed away from privacy-destroying moves in the face of fierce user protests.⁵ *Touché*.

This is a recognized, recurring problem in Internet privacy policy—under what circumstances will vocal user protest lead to real privacy protections?²—and it deserves more sustained attention in the Facebook context than I have given it. A brief answer might be that user protest will be both over- and under-inclusive. The user protest over News Feed led to a “compromise” that would have been unacceptable to most Facebook users if you had asked them about it a month before the launch.⁶ Facebook users also get almost absurdly agitated about trivialities: a redesign of the profile pages drew protests almost as fierce as the ones over News Feed and Beacon. One might conclude that Facebook users are like goldfish: they hate change, but they have very short memories.

This view may, however, be too simplistic. The latest Facebook uprising concerned a change to the copyright provisions in the site's terms of use.⁷ This time, to placate the angry mob, Facebook involved users in drafting a “Statement of Rights and Responsibilities” to replace its terms of use and promised to put any future changes to a user vote.⁸ There's reason to be skeptical that these commitments have any teeth in them—the user votes require a turnout of thirty percent to be binding, and thirty percent of 200 million users is a lot more than have been involved in *anything* on Facebook.⁹ Still, the possibility of user governance on Facebook is worth watching closely. There's something profoundly social about the nature of engagement on Facebook that may open up some new possibilities when it comes to collective decision-making about privacy.

Third, Freiwald is worried when I reject “commercial-data rules.” I dismiss the privacy harms Facebook itself might directly cause to users as “orthogonal” to the harms Facebook users cause each other—the “peer-to-peer privacy violations,” in my term.¹⁰ She's right to call me on it. In her words, “There are no privacy-threat awards; instead there are plenty of

5. *Id.* at 140–42.

6. *Id.* at 130–31.

7. See Brad Stone & Brian Stelter, *Facebook Withdraws Changes in Data Use*, N.Y. TIMES, Feb. 18, 2009, at B1, <http://www.nytimes.com/2009/02/19/technology/internet/19facebook.html>.

8. Scott Duke Harris, *Facebook Users Vote for 'Bill of Rights'*, MERCURY NEWS (San Jose), Apr. 24, 2009.

9. Statement of Rights and Responsibilities, <http://www.facebook.com/terms.php?ref=pf> (last visited Dec. 18, 2009).

10. Grimmelmann, *supra* note 2, at 148–51.

privacy problems to work on for those so inclined.”¹¹ The commercial-data-sharing threats are as real on Facebook as they are on any other online site with personal data on millions of deeply engaged users, and I definitely don’t want to be understood as minimizing either those threats or the need for legal interventions to keep Facebook (and other such sites) from misbehaving.

Still, I put “commercial-data rules” in the “what won’t work” section for a reason, and that reason is the true heart of my argument in *Saving Facebook*. When I give talks on the subject, this is the part where I start shouting. Just as paying attention to peer-to-peer privacy violations shouldn’t lead us to underestimate privacy threats from companies and government, the reverse is also true: responding to privacy threats from companies and government shouldn’t distract us from the peer-to-peer privacy threats. I’ve found that this latter point is a little outside the comfort zone of some privacy scholars; they don’t see it unless I start shouting. (On reflection, maybe the shouting produces nods of politeness, rather than insight.)

And this is why I resort to a little “your favorite privacy protection sucks” provocation in Part III. Commercial-data rules “won’t work” in the sense that they won’t fix peer-to-peer privacy violations on social network sites. That doesn’t mean they aren’t a good idea when it comes to data sharing with governments, direct marketers, and other such entities. But the Fair Information Practices aren’t a cure-all; when it comes to Facebook users snooping on each other, they’re more of a placebo.

Indeed, unless they’re applied with some caution, commercial-data rules can be actively harmful on social network sites. Every other user of Facebook is a potential third party. Requiring Facebook to obtain specific informed consent from its users before releasing each individual piece of information to each individual other user would be frustrating, so frustrating that users would simply fall into the habit of automatically always clicking “yes.” This is a way in which Facebook really is different from Webvan. Sharing information about yourself with your social group was never a goal of Webvan, so restrictions on data transfer would never have interfered with the core essential functionality of Webvan, the way they would on Facebook.

And thus—as perhaps hinted by my choice of Webvan as an example—we circle back to the first issue Freiwald flagged: *why Facebook?* There are some fine and subtle distinctions to be made in mapping commercial-data rules onto social network sites, and policy-makers must be careful to make them. For that, close factual engagement is essential. People don’t use Facebook for macroscopic, commercial reasons. They use it for a million different microscopic, social motivations. To understand that—to really understand it—there’s no substitute but to get down in the trenches with

¹¹ Freiwald, *supra* note 1, at 9.

users as the friend requests and Wall posts fly back and forth and their privacy explodes around them.

Preferred Citation

James Grimmelman, *Saving Facebook: A Response to Professor Freiwald*, 95 IOWA L. REV. BULL. 13 (2009), http://www.uiowa.edu/~ilr/bulletin/ILRB_95_Grimmelmenn.pdf.