

A Comment on James Grimmelmann's *Saving Facebook*

Susan Freiwald*

In *Saving Facebook*,¹ Professor James Grimmelmann analyzes what draws users to Facebook and why they misunderstand the privacy dangers they encounter there. He argues that one cannot propose proper policy interventions without thoroughly understanding what Facebook users do and why they do it, or, in other words, their “social dynamics.”² Grimmelmann draws on sociological and psychological studies and from his own experiences to explain what motivates Facebook users to divulge so much personal information on the site. While users derive considerable social benefits from sharing their stories on Facebook, Grimmelmann posits that they would disclose less if they approached the privacy risks more rationally. Instead, users reason according to misleading “heuristics”³ that lead them to over-divulge. As a result, they subject themselves to the six patterns of privacy violations, such as surveillance and denigration, which are common on social network sites.⁴ Having set out the problems, Grimmelmann determines what things “won’t work” to solve them and what will (at least “sometimes”) work.⁵ He considers different institutional approaches, including letting market forces operate unhindered, using tort claims to redress harm, and drafting specifically targeted legislation. Grimmelmann seeks to “start a conversation” about “better and worse ways” to help social network users understand the consequences of their actions and to protect them from harm.⁶

Grimmelmann’s article contributes significantly to our understanding of how Facebook works today—or at least how it has worked in the recent past. By raising our knowledge about the intricacies of Facebook

* Professor, University of San Francisco School of Law. Many thanks to Peter Volz for his fine research assistance.

1. James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137 (2009).

2. *See id.* at 1149.

3. *See generally id.*

4. *Id.* at 1163–75 (describing the six types of privacy harms and how they relate to Facebook).

5. *Id.* at 1178, 1195.

6. Grimmelmann, *supra* note 1, at 1202.

interactions, Grimmelmann's article serves a valuable function: It raises the likelihood that future legislators interested in drafting laws to regulate Facebook and similar social network sites will know the beast before they try to tame it. In the cyberspace arena, Congress has not always recognized that one risks making a problem worse by regulating it before truly understanding it. For example, Congress faced well-warranted criticism for its knee-jerk venture into online-indecency legislation in the mid-1990s.⁷ Spurred to action by one faulty study of online smut, Congress became convinced that indecency was the gateway to child predation. With neither hearings nor studies, Congress drafted a draconian criminal law that obviously violated the First Amendment.⁸ Five years later, just following the tragic attacks of September 11, 2001, Congress drafted a panoply of provisions to address the terrorist threat. Unfortunately, Congress bowed to pressure and fear, rather than to reason, in those areas affecting cyberspace. For example, Congress updated the pen-register statute to permit online pen registers without either clarifying what information they could obtain or providing meaningful judicial oversight of their use.⁹ While not all of the USA PATRIOT Act is misplaced, much of it demonstrates that Congress does not do its best work when it moves quickly in response to crisis to regulate new cyberspace technologies.¹⁰

Grimmelmann's thorough study of Facebook and its users substantially increases the likelihood that Congress will know more about social networks before it tries to regulate them or their uses. As the current generation of Congresspeople migrates to Facebook, or as the generation already on Facebook migrates to Congress, the possibility that lawmakers will target Facebook for new laws grows. Grimmelmann's article will be an essential reference when that day comes. Not only does it describe the current dynamics, but it also evaluates possible policy responses, both of which should be useful to a Congress interested in regulating Facebook and its ilk.

As a caveat, it must be said that the target is fast-moving. Facebook aficionados may not believe it, but the risk that a new and different social network tool will shortly replace Facebook looms large. Perhaps rapidly expanding Twitter will draw users away from Facebook. Perhaps something

7. See LAWRENCE LESSIG, *CODE VERSION 2.0*, at 249–50 (2006).

8. See *Reno v. ACLU*, 521 U.S. 844, 882 (1997) (describing the Act as “casting a far darker shadow over free speech” than a prior statute also found to be unconstitutional); see also *id.* at 879 (noting the lack of congressional findings or hearings on the statute).

9. See Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 60–61, 69–73 (2004) (discussing how the government has interpreted the pen-register statute as allowing surveillance of a significant amount of online information).

10. Congress did a much better job when it passed the Video Privacy Protection Act of 1998 to reduce the availability of video-rental records. The threat to divulge Judge Bork's videotape-rental records during his confirmation hearings spurred Congress to action. See Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949, 1013–16 (1996) (discussing the protections of the Video Privacy Protection Act).

else will. Early devotees of America Online probably thought it would last for decades rather than years. One does not have to be a cyber historian to recognize that Internet applications come and go, which means that tying one's scholarly work to a particular technology risks obsolescence as its subject fades.

Grimmelmann seems to be fully cognizant of that risk, and his paper therefore offers much more than a moment-in-time analysis of a current cyberspace trend. The analyses he offers of the various reasons why people share more than they should and the harms that follow from that will be useful in privacy work on future technologies that scratch the same "social itches," as Grimmelmann colorfully writes.¹¹ Grimmelmann nicely ties the various privacy harms to the privacy-interest taxonomy that preeminent cyber-privacy scholar Daniel Solove has developed.¹² Solove's framework and Grimmelmann's application of it to the Facebook (or social network) context will have further use for new iterations of social networks, whatever Facebook's fate.

Grimmelmann points out that Facebook users have an erroneous expectation of privacy on the site. He alerts Facebook users to the fact that they have much less control over the fate of the data they post than they would imagine or like. If that message sinks in to current and future Facebook users, they may release less of the information that makes them vulnerable in the first place (although I believe, and Grimmelmann recognizes, that the message is least likely to sink in to those who most need to hear it). Whatever the problem with young people today, Grimmelmann recommends good education as an important means to inhibit privacy harms, and his paper's careful study provides just that.¹³

From a more purely legal standpoint, Grimmelmann provides a blueprint for how to engage in legal analysis and make policy recommendations that draws upon the insights of institutional scholars. One such insight is that one must compare policy choices against realistic alternatives rather than idealized ones.¹⁴ Grimmelmann deftly employs the

11. Grimmelmann, *supra* note 1, at 1151.

12. See DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 101–70 (2008) (identifying four groups of activities that affect privacy: information collection, information processing, information dissemination, and invasion). See generally Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006) (same).

13. At the same time, there may be a limit to readers' interest in the details of particular Facebook applications, particularly for those readers who are neither members of the Facebook community nor sociologists.

14. See Susan Freiwald, *Comparative Institutional Analysis in Cyberspace: The Case of Intermediary Liability for Defamation*, 14 HARV. J.L. & TECH. 569 (2001) (using comparative institutional analysis in a cyberspace context). See generally NEIL K. KOMESAR, IMPERFECT ALTERNATIVES: CHOOSING INSTITUTIONS IN LAW, ECONOMICS, AND PUBLIC POLICY (1994) (developing framework for analysis that takes account of practical constraints on all institutions).

observations of sociologists to make his predictions of likely responses to legal change more realistic. Merely by considering and comparing different policy approaches to the Facebook privacy problem, Grimmelmann does much more than many others have done with similar projects.¹⁵ The typical law-review analysis identifies a legal problem and then exhorts Congress to fix it. Grimmelmann warns that such an approach could easily be ineffective; worse, it could backfire. For example, he argues that greater technical controls over privacy can backfire by becoming so complex as to overwhelm users who then ignore them altogether.¹⁶ Again, Grimmelmann's concern that we not legislate in a knee-jerk fashion by mandating some behaviors and prohibiting others without thinking through the repercussions is well-taken.

But leaving Facebook privacy protection to the "free market" will also be ineffective, according to Grimmelmann. He persuasively argues that Facebook users are unlikely to negotiate for the level of privacy protection they truly desire at the time they establish their Facebook relationship. Even if individuals valued privacy more than Facebook offered, the company would hardly negotiate privacy terms with individual users, let alone with non-users who may face privacy loss at the hands of Facebook users.¹⁷ As noted, Facebook users also believe, incorrectly, that they will have more privacy on Facebook than they actually will. Highlighting a problem with the prediction that people will contract to the correct amount of privacy protection, Grimmelmann explains that people rarely think about privacy until they have lost it or until they are old enough to regret that they did not demand it earlier. Grimmelmann's interesting discussion of how inexperience inhibits young peoples' ability to protect their privacy now because they will want it in the future buttresses his lack of confidence in the "do nothing" approach. Similarly, his assault on privacy policies as "beautiful irrelevanc[ies]" due to the fact that users neither read them nor understand them nicely counters the "informed-choice" argument that opposes more intrusive legal rules.¹⁸

Despite Grimmelmann's arguments against a market approach to privacy protections, I am not sure that the evidence he marshals fully supports his point. In several of the stories recounted in the article, Facebook users themselves exerted strong pressure on the site to change its

15. To be fair, much of the cyberlaw literature is drafted by law students, who face significant time and resource constraints.

16. Grimmelmann, *supra* note 1, at 1184 ("[W]hen given the choice, users almost always spurn or misuse technical controls . . .").

17. By the same token, Facebook users cannot effectively negotiate with third parties to whom Facebook will grant data access. *See id.* at 1181 (describing the limits of Facebook's privacy policy and its inapplicability to third parties).

18. As Grimmelmann points out, privacy policies usually enhance the company's power to do what it wants with user data rather than constrain it. *See id.* at 1180–81 (outlining the uses of private data that Facebook reserves).

ways, and the site did. For example, Grimmelmann details how Facebook retreated from its Beacon implementation by offering a more user-friendly opt-out.¹⁹ Facebook also retreated in the face of other criticisms.²⁰ The market functions not just when contracts are made (as when users join Facebook) but also when users make credible threats to leave in response to dissatisfaction. When Facebook users vote with their feet, or threaten to, they bring market pressure—the pressure to join an alternative site that better meets their needs—to bear on Facebook. Grimmelmann does raise the concern that users may hesitate to leave if they cannot take their data with them,²¹ but, to the extent that it works, exit may obviate more formal legal intervention.

For those cases in which Facebook users are unable adequately to protect their own rights, I think that some new legal rules will need to impose obligations directly on Facebook.²² Unlike prohibiting cars or car windows to stop ghost riding the whip, imposing direct obligations on Facebook will often be the right answer.²³ The issue is not that Grimmelmann rejects legal liability for Facebook, but rather that he dismisses the privacy problems Facebook's own actions raise as "orthogonal."²⁴ I have never understood the need to prioritize privacy concerns (Question: Is the threat greater from the government or private entities? Answer: Yes). There are no privacy-threat awards; instead there are plenty of privacy problems to work on for those so inclined. For that reason I find it curious, as well as unconvincing, when Grimmelmann emphasizes the peer-production of privacy harms and minimizes the need to regulate Facebook directly. I question his decision to put commercial-data rules in

19. For another recounting of how Facebook acceded to user demands for a comprehensive opt-out from Beacon, see generally Yasamine Hashemi, Note, *Facebook's Privacy Policy and Its Third-Party Partnerships: Lucrativity and Liability*, 15 B.U. J. SCI. & TECH. L. 140 (2009).

20. Another example that Grimmelmann refers to in passing is Facebook's immediate disabling of a feature that was rumored to permit users to find out who was searching for information about them. Grimmelmann, *supra* note 1, at 1162 nn.166–67. While the feature's function was never clear, Facebook apparently pulled it within hours of a story about it appearing on a popular website. Caroline McCarthy, *Facebook Pulls "Stalker List" Tool After Gawker Exposes It*, CNET NEWS, May 13, 2008, http://news.cnet.com/8301-13577_3-9943285-36.html. Facebook apparently also let two users back on to the service when they protested being kicked off. Grimmelmann, *supra* note 1, at 1195 n.375.

21. Grimmelmann, *supra* note 1, at 1191–92.

22. As Grimmelmann's examples suggest, lawmakers do not need to change traditional legal rules for social networks, such as those providing recovery for defamation or prosecution for harassment or fraud. *Id.* at 1175–77.

23. See Patricia Sanchez Abril, *A (My)Space of One's Own: On Privacy and Online Social Networks*, 6 NW. J. TECH. & INTELL. PROP. 73, 87 (2007) (advocating greater restrictions on service providers as "the best situated actors to carry some of these [privacy protective] burdens").

24. Grimmelmann, *supra* note 1, at 1187.

the section of his article covering approaches that won't work.²⁵ These rules will not solve the problems that arise when users themselves tag embarrassing photos or reveal intimate information in ways that cause harm, but they may be needed to correct the significant data-privacy threat Facebook itself poses.²⁶

In fact, some of the most significant privacy harms that Grimmelmann identifies resulted when Facebook changed its practices without sufficient notice to users. In one case, Facebook made "limited profiles" available on the "public internet," but did so after users had "formed [their] privacy expectations around the way the site originally worked."²⁷ Grimmelmann also calls foul that Facebook launched Social Ads and Beacon with insufficient notice and opt-out. Grimmelmann seems to advocate that consumer-protection laws protect users against such privacy "lurches."²⁸ But surely that means legal liability for Facebook (perhaps via a claim for failure to adhere to its privacy policies or representation). While subjecting Facebook to legal liability will not always be the answer, it often will be.²⁹

Nonetheless, Grimmelmann argues convincingly that a closer look at understanding the social dynamics of Facebook users leads us to question the efficacy of the standard privacy solutions. He covers new ground when he discusses how data portability and "ownership" by users will likely cause more privacy harm than good by defeating the privacy expectations of those who shared information with the data "owner." His engaging discussion of the perverse reactions that users will have to privacy controls counsels in favor of greater scrutiny of "easy" technological solutions. As previously discussed, Grimmelmann's thorough analysis of users' reactions to privacy policies (neither to read them nor to understand them) counters the conventional (and often governmental) wisdom that greater disclosure of privacy practices cures most ills. Finally, his call for greater scrutiny and

25. Grimmelmann's argument that data-collection rules could unduly inhibit social networks could have used more development. *Id.* at 1189. Examples of how proposed limits would inhibit actual practices would have been helpful.

26. In fact, Grimmelmann mentions that other countries are investigating Facebook's data practices. *Id.* at 1183, 1188. I will not explore here the Fourth Amendment problems inherent in Facebook sharing personal information too readily with government investigators, except to note that I, along with Patricia Bellia, have written about Fourth Amendment interests in stored data. See Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. LEGAL F. 121. Though he does not discuss it at length, Grimmelmann supports a warrant requirement when law-enforcement agents compel Facebook to divulge information. Grimmelmann, *supra* note 1, at 1196.

27. Grimmelmann, *supra* note 1, at 1168.

28. *Id.* at 1200.

29. When Grimmelmann discusses what Facebook should and should not do about letting users leave the service and tracking non-users, it is not clear whether he is advocating that the law back up his suggestions. *Id.* at 1197-99. When he argues that "[r]egulators should . . . prohibit such practices" as viral incentives, he clearly advocates that the law ensure that Facebook do "the right thing." *Id.* at 1202.

nance in the law's approach to disclosure as "all or nothing" is quite well taken.

Ultimately, Grimmelmnn concludes that educating users in their own cultural vocabulary and with an understanding of their own social dynamics is essential. As a non-Facebook user, I certainly could not do that. As someone who is admirably versed in the ins and outs and the hows and whys of Facebook, and is well grounded in the copious sociological literature as well as the relevant legal theory and doctrine, Grimmelmnn will likely pull it off. In the meantime, he will surely have succeeded in educating the rest of us.

Preferred Citation

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