PRIVACY AS PRODUCT SAFETY

James Grimmelmann*

I. Introduction

Start with a story. Two young women, Andrea and Hannah, were on vacation in St. Tropez.[1] They met up with a male friend who was in a band, had cocktails at a bar on the beach, took a stroll

---

* Associate Professor of Law, New York Law School. My thanks to the attendees of A Workshop on Federal Privacy Regulation at New York University School of Law on October 2, 2009, and to the symposium on Internet Expression in the 21st Century: Where Technology & Law Collide at Widener University School of Law in Harrisburg, Pennsylvania, on February 22, 2010, where I presented earlier versions of this paper. Aislinn Black, danah boyd, Danielle Citron, William McGeveran, and Lior Strahilevitz provided useful suggestions in conversation. Dominic Mauro provided research assistance.

[1] James Tapper, *Saint Bono and the Angels of St Tropez; but What Will the U2 Singer's Wife Have to Say About His Partying with Two Teenage Girls?*, MAIL ON SUNDAY (London), Oct. 26, 2008, at 3, *available at* http://www.dailymail.co.uk/tvshowbiz/article-1080636/What-St-Bonos-wife-say-partying-teenage-girls.html.

along the shore, and ended up on a private yacht as the sun went down.[2] It was a good day.

I know all of this because Andrea posted her photos on Facebook.[3] This in itself might not have been a big deal, except that her musician friend was named Bono and his band was an outfit called U2.[4] The tabloids jumped at the chance to run pictures of the middle-aged rocker partying in the sun with two nymphets whose ages combined added up to less than his.[5] So much for a private little walk on the beach.

The story is noteworthy because it features a celebrity, but similar things happen on social software everyday.[6] An education major lost her teaching placement–and with it her degree–after a photo of her as a " 'drunken pirate' " along with an unflattering MySpace post came to the attention of her school's superintendent.[7] Another college student faced criminal charges after the police used Facebook to link him to a friend he denied

---

[2] Tapper, *supra* note 1, at 3.

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] *See* James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1164-65 (2009) (describing instances where disclosure on Facebook has caused harm). *See generally* danah michele boyd, Taken Out of Context: American Teen Sociality in Networked Publics (Fall 2008) (unpublished Ph.D. dissertation, University of California, Berkley), http://www.danah.org/papers/TakenOutOfContext.pdf (describing social networks and communities); Chris Peterson, *Losing Face: An Environmental Analysis of Privacy on Facebook* (Jan. 2010) (unpublished draft on file with author) (using Facebook as a case study). In this essay, I will use Facebook as the leading example, but most of the discussion will be relevant to other social software as well. I will also presume familiarity with Facebook. For an overview of Facebook, see Grimmelmann, *supra*, at 1144-49; Welcome to Facebook, http://www.facebook.com/ (last visited May 14, 2010). I will use the umbrella terms 'social software' and 'social media' to describe websites and other computer applications designed to facilitate social interactions. These terms include social network sites like Facebook and also include blogs, Twitter, ChatRoulette, instant message programs, texting, and a whole ocean of other new software-based communications media. *See generally* CLAY SHIRKY, HERE COMES EVERYBODY (2008) (giving examples of social software).

[7] *See* Snyder v. Millersville Univ., No. 07-1660, 2008 U.S. Dist. LEXIS 97943, at *12-22 (E.D. Pa. Dec. 3, 2008).

knowing.[8] Say the wrong thing on Facebook–or rather, say it without realizing who might see it–and you could lose your job.[9] The smaller losses of dignity are so routine that there are now entire websites devoted to cataloguing them.[10] On Facebook, Andrea is an everywoman.

This essay will take up two questions suggested by Andrea's example: is the loss of privacy in social media something lawmakers ought to worry about and, if so, what should they do? Part II will answer the first question with a clear yes: users want privacy, deserve privacy, and cannot easily secure privacy for themselves. Part III will suggest, somewhat more tentatively, that lawmakers could benefit from thinking about the problem of privacy in social software as one of safe product design. I will use Facebook as the principal example, with Andrea's story[11] serving as a recurring motif. Near the end of this article, I will illustrate that my theory is not Facebook-specific by showing that it also helps us make sense out of a recent privacy controversy involving Google Buzz.

II. THE MYTHS OF PRIVACY ON FACEBOOK

The first question raised by Andrea's story is whether there is a problem here at all. The very fact that so much personal information is available on Facebook could be an argument *against* legal intervention. How so? Here are three things one might say about privacy in social software, using Andrea as a representative example of her fellow users:

---

[8] *See* Jodi S. Cohen, *Cop Snares College Pals in Own Web*, CHI. TRIB., Aug. 3, 2006, at C1.

[9] *See* John Gonzalez, *Cold Eagles Sure Are Thin-Skinned*, PHILA. INQUIRER, Mar. 9, 2009, at E02 (describing how a Philadelphia Eagles employee was fired after criticizing the decision to trade a football player on Facebook).

[10] They are often referred to as 'fails.' *See* Facebook Fail Blog – Funny Profiles, Photos, Status Updates, Comments, Groups, and Pages, http://facebookfails.com/ (last visited May 14, 2010); Failbooking – Funny Facebook Status Messages (Failbook), http://failbooking.com/ (last visited May 14, 2010).

[11] *See supra* text accompanying notes 1-5. The references to Andrea throughout the rest of this article are pulled from the illustration used in the introduction of this essay. *Id.*

- Andrea does not care about privacy.
- Andrea makes rational privacy choices.
- Andrea's desire for privacy is unrealistic.

If even one of these claims is true, then the law should keep its hands off. If Andrea does not want privacy, the law should not force it on her. If she wants privacy but is capable of securing it for herself, then she does not need help from the law. If she wants privacy in the same unrealistic way that five-year-olds want to be surgeon princesses and astronaut ninjas, then there is little the law could do about it.

In reality though, all three of these claims are false.[12] They are myths about privacy.[13] Users of Facebook care passionately about privacy, but they have great trouble achieving it.[14] That trouble is not their fault; it arises out of the quite natural difficulty they have in understanding what will happen to their personal information once they post it.[15] However, a substantial part of what they mean by 'privacy' is readily achievable–at least most of the time.[16]

To these three myths about privacy on Facebook, we should add a fourth half-myth about privacy *law* and Facebook:

- Regulating Facebook as a database will solve Andrea's privacy problems.

It is true that Facebook and other social network sites have enormous databases of personal information on their users.[17] It is also true that privacy law can and should prevent misuse of those databases–so Facebook, for example, should be required to take reasonable steps to secure its site from hackers. But the *social* nature of this social software means that database regulation alone is insufficient–and, indeed, can be counterproductive if not carefully handled.[18] Database regulation is thus a half-myth: a good idea, but also a distraction from other privacy issues.[19]

---

[12] *See infra* pt. II.A-D.
[13] *See id.*
[14] *See infra* pt. II.A.
[15] *See id.*
[16] *See id.*
[17] *See* Harry Lewis, *How Facebook Spells the End of Privacy*, BOSTON GLOBE, June 14, 2008, at A11.
[18] *See infra* pt. II.D.
[19] *See id.*

A. Myth 1: Facebook Users Don't Care About Privacy

Webster's New World Dictionary selected "overshare" as its "2008 Word of the Year."[20] As its press release explained, "[I]n an era of online social networking and instant digital broadcasts, this type of unsolicited and often embarrassing communication is an inescapable sign of the times."[21] That is certainly true on Facebook: there are days–perhaps most days–when the site can seem like a single global case of TMI.[22] Whether it is women posting their bra colors,[23] bosses posting pink slips,[24] or people's simple narcissism,[25] you can find it all on Facebook.

This let-it-all-hang-out attitude seems, on its face, flatly inconsistent with anything resembling privacy as we have traditionally understood it, leading to the obvious conclusion that the Facebook generation has turned its back on privacy. As columnist Robert J. Samuelson wrote, "[M]illions of Americans are gleefully discarding–or at least cheerfully compromising–their right to privacy. . . . People seem to crave popularity or celebrity more than they fear the loss of privacy."[26] Or, as Emily Nussbaum summed up the "disgusted, dismissive squawk" of an "older generation": "Kids today. They have no sense of shame. They have

---

[20] Press Release, Webster's New World, Overshare Is *Webster's New World Dictionary*'s 2008 Word of the Year (Dec. 1, 2008), http://newworldword.com/press-release-overshare-is-word-of-the-year/.

[21] *Id.*

[22] "Too [m]uch [i]nformation." Urban Dictionary: tmi, http://www.urbandictionary.com/define.php?term=tmi (last visited May 14, 2010).

[23] *See* Posting of Hortense to Jezebel, http://jezebel.com/ (Jan. 9, 2010, 12:40 EST).

[24] *See Woman Fired via Facebook After Rant*, WORLD NEWS AUSTL., Aug. 10, 2009, http://www.sbs.com.au/news/article/1070187/Woman-fired-via-Facebook-after-rant.

[25] *See How Does Facebook Make Overt Self Obsession Ok?*, METEUPHORIC, Feb. 4, 2010, http://meteuphoric.wordpress.com/. *See generally* Christine Rosen, *Virtual Friendship and the New Narcissism*, NEW ATLANTIS, Summer 2007, at 15, *available at* http://www.thenewatlantis.com/docLib/TNA17-Rosen.pdf (discussing digital self-portraits and their relation to virtual friends).

[26] Robert J. Samuelson, *A Web of Exhibitionists*, WASH. POST, Sept. 20, 2006, at A25.

no sense of privacy. They are show-offs, fame whores, pornographic little loons who post their diaries, their phone numbers, their stupid poetry – for God's sake, their dirty photos! – online."[27]

Behind the generation gap and the apprehension of a socially disruptive new technology, there is a genuine sociological theory at work here. It asserts that the kids these days simply do not care about privacy. A collection of attitudes–personal dignity, post-Nixonian suspicion of government surveillance, patience with slower analog media, and willingness to think about the future–that kept older generations from revealing too much about themselves have all fallen by the wayside. Meanwhile, mass culture is now dominated by *Jersey Shore*,[28] *The Real Housewives*,[29] *Celebrity Rehab*,[30] and other reality TV offerings that conflate public exposure with personal fulfillment. There is little wonder that today's teens and young adults see only benefits in sharing their every move online, with little concern for the consequences of foregone privacy. Facebook use is just a symptom of an underlying unconcern for the private–visible confirmation that oversharing is the new black.

It is an elegant theory, except for the inconvenient fact that it does not fit the available data. Actual Facebook users act in ways that indicate that they very much care about privacy. When Facebook rolled out News Feed, there were massive user protests to the point that Mark Zuckerberg had to apologize to the Facebook community.[31] The same thing happened a year later with Facebook's Beacon advertising system[32] and a year after that with

---

[27] Emily Nussbaum, *Say Everything*, N.Y. MAG., Feb. 12, 2007, http://nymag.com/news/features/27341/index1.html.

[28] *Jersey Shore* (MTV television broadcast).

[29] *The Real Housewives of Atlanta* (Bravo television broadcast); *The Real Housewives of New Jersey* (Bravo television broadcast); *The Real Housewives of New York City* (Bravo television broadcast); *The Real Housewives of Orange County* (Bravo television broadcast).

[30] *Celebrity Rehab* (VH1 television broadcast).

[31] *See* Tracy Samantha Schmidt, *Inside the Backlash Against Facebook*, TIME, Sept. 6, 2006, http://www.time.com/time/nation/article/0,8599,1532225,00.html.

[32] *See* Louise Story & Brad Stone, *Facebook Retreats on Online Tracking*, N.Y. TIMES, Nov. 30, 2007, at C1.

a change to its data-retention policy.[33] Meanwhile, when Facebook users find out that others are looking at their Facebook profiles, such as employers,[34] relatives,[35] or police,[36] they also object.[37] These are the protests of people for whom privacy matters.

It is not cheap talk. Facebook users also act in ways that show a regard for privacy. Consider Andrea. Her choice to use Facebook was actually a privacy-positive move. Her alternative, after all, was the web. Facebook is a controlled network; Andrea chose which networks to belong to and whom to 'friend.' She may have failed at keeping her pictures private, but she did at least try–and so does everyone who uses Facebook and puts any effort into choosing friends or adjusting privacy settings.

In fact, as soon as you scratch beneath the surface of Facebook social practices, carefully modulated privacy management is everywhere. danah boyd has documented how teens on Facebook, MySpace, and other social media use fake profiles, fake names,

---

[33] Bobbie Johnson & Afua Hirsch, *Facebook Backtracks After Online Privacy Protest*, GUARDIAN (London), Feb. 9, 2009, at 9, *available at* http://www.guardian.co.uk/technology/2009/feb/19/facebook-personal-data.

[34] *See* Jeff Cain, *Online Social Networking Issues Within Academia and Pharmacy Education*, AM. J. PHARMACEUTICAL EDUC., Feb. 15, 2008 (citing M. Sisson & C. Wiley, Nat'l Ass'n of Colls. & Employers, Ethics, Accuracy, and Assumption: The Use of Facebook in Recruiting (May 30, 2007)), *available at* http://www.ajpe.org/view.asp?art=aj720110&pdf=yes (forty-two percent of students surveyed considered Facebook use by employers a violation of privacy). There are legal risks to the employer just from looking at applicants' Facebook profiles:

> Employers, however, may face liability under federal, state and local law for using any information learned from social media about an applicant's protected class status— race, age, disability, religion, sexual orientation, etc.—in a hiring decision. It may be hard for the employer to prove in later litigation that it only viewed, but didn't actually use, the information obtained in a social medium when making its hiring decision.

Renee M. Jackson, *Social Media Permeate the Employment Life Cycle*, NAT'L L.J., Jan. 11, 2010, at 16, 16, *available at* http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202437746082.

[35] *See* Peterson, *supra* note 6, at 2 (citation omitted) (quoting Facebook user's status update saying " 'my grandmother just friend requested me . . . no. Facebook, you have gone too far!' ").

[36] *See* Cohen, *supra* note 8.

[37] *See* Avner Levin & Patricia Sanchez Abril, *Two Notions of Privacy Online*, 11 VAND. J. ENT. & TECH. L. 1001, 1025-27 (2009).

fake ages, and a cloud of other minor lies to keep their profiles safe from prying (usually parental) eyes while also connecting with their peers.[38] Meanwhile, college students coming back from a night of partying have learned that the first thing they need to do is check Facebook and untag their names from any photos of them doing keg stands, lest their athletic coaches or campus police catch them drinking.[39]

The point is not that these "Digital Natives" prize privacy above all else or that they experience privacy in the same way previous generations did or that the social content of privacy is stable.[40] The privacy they care about is social and relational, perhaps less concerned with databases and governmental surveillance than their parents' and grandparents' privacy.[41] They are constantly trading their privacy off against other social opportunities and making pragmatic judgment calls about what to reveal and what to keep hidden.[42] However, they do care about privacy, and they act accordingly.

B. Myth 2: Facebook Users Make Rational Privacy Choices

Why, then, does the idea that Facebook users reject privacy have such resonance? The ideal appeals, in part, because of a related idea: people make rational, cost-benefit tradeoffs when evaluating privacy online. If Facebook users are choosing online options that lead to low-privacy outcomes, they must have a good reason for it.

Again, the thought has a certain logic to it. Just as it may not be rational for people to invest in picking good passwords if someone else bears the risk from computer intrusions,[43] it may not

---

[38] *See* boyd, *supra* note 6, at 148-59.

[39] Lisa Guernsey, *Picture Your Name Here*, N.Y. TIMES, July 27, 2008, at E6.

[40] *See* JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES 7 (2008) (discussing how young Internet users think about privacy and proposing the term "Digital Natives").

[41] *See id.* at 7 ("Digital Natives' ideas about privacy, for instance, are different from those of their parents and grandparents.").

[42] *See id.* at 56.

[43] *See* Cormac Herley, *So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users*, *in* QUEEN'S COLL. UNIV. OF

be rational for them to invest in privacy.[44] This is particularly the case if they have something to gain by exposing their personal information. In Ed Felten's words, " 'Given the choice between dancing pigs and security, users will choose dancing pigs every time.' " [45] The behavioral advertising industry (which Facebook has been trying mightily to break into), for example, describes highly targeted advertising as a benefit to consumers, something they willingly seek out.[46] If this were right, then we could treat the fact that thirty-five percent of Facebook users adjusted their privacy settings after its latest design changes as evidence that they are carefully reviewing the pros and cons of privacy–that would be 100,000,000 well-informed users.[47] The other sixty-five percent–some 250,000,000 strong–must have fully approved of Facebook's changes.[48]

Just as the death of privacy was a myth, however, so too is the belief in rational privacy balancing. For one thing, users massively misunderstand Facebook's privacy architecture and settings. One study found that over half of Facebook users surveyed were unaware that their profiles were searchable by millions of other Facebook users.[49] Another found that two-fifths of Facebook users

---

OXFORD, UK, 2009 NEW SECURITY PARADIGMS WORKSHOP 133-34 (Richard Ford et al. eds., 2010) (arguing that it is rational for users to choose poor passwords).

[44] *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 549-50, 565 (2008) (arguing that it is rational for users not to read privacy policies).

[45] Mozilla Security Review and Best Practices Guide, http://www.mozilla.org/projects/security/components/reviewguide.html (last visited May 14, 2010).

[46] *See generally* Eric Goldman, *A Coasean Analysis of Marketing*, 2006 WIS. L. REV. 1151 (arguing that well-tailored marketing benefits both consumers and advertisers).

[47] *See* E.B. Boyd, *A Third of Facebook Users Customized Their Privacy Settings After the Policy Changes (And Why Facebook Thinks That's a Good Thing)*, BAYNEWSER, Jan. 29, 2010, http://www.mediabistro.com/baynewser/privacy/a_third_of_facebook_users_customized_their_privacy_settings_after_the_policy_changes_and_why_facebook_thinks_thats_a_good_thing_150409.asp.

[48] *See id.*

[49] Alessandro Acquisti & Ralph Gross, *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*, *in* PRIVACY

were willing to add a green plastic frog as a friend.[50] The frog's name, in a nice touch, was " 'Freddi Staur,' " an anagram for " 'ID Fraudster.' "[51] Suddenly, the inactivity of the sixty-five percent who left their privacy settings untouched sounds less like agreement and more like ignorance. Of course, one also starts to wonder how effective the choices made by the other thirty-five percent were.

Consider Andrea again: she posted the photos to her seemingly private Facebook account, thinking that they would be visible only to her friends and networks.[52] The trouble is that one of her networks was "New York City," whose membership by default consisted of anyone in New York City with a Facebook account.[53] Over 1,000,000 other users were able to view Andrea's photos of herself with Bono. It is hard to describe this as a rational choice about privacy.[54] Facebook itself eventually eliminated this 'feature' of networks, having presumably concluded that users were never going to understand how networks worked.[55]

Facebook users who attempt to weigh the privacy costs and benefits of each individual act of participation systematically get the balance wrong.[56] The design of social networking sites plays into plenty of well-understood, social cognitive biases. The most basic heuristic of privacy self-help–know your audience–is hard to

---

ENHANCING TECHNOLOGIES: SIXTH INTERNATIONAL WORKSHOP, PET 2006 CAMBRIDGE, UK, JUNE 2006 REVISED SELECTED PAPERS 36, 53 (George Danezis & Philippe Golle eds., 2006), *available at* http://privacy.cs.cmu.edu/dataprivacy/projects/facebook/facebook2.pdf.

[50] *Sophos Facebook ID Probe Shows 41% of Users Happy to Reveal All to Potential Identity Thieves*, SOPHOS, Aug. 14, 2007, http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html.

[51] *Id.*

[52] Tapper, *supra* note 1.

[53] *Bono's Bikini Party Photos Exposed by Facebook Privacy Flaw*, SOPHOS, Oct. 29, 2008, http://www.sophos.com/pressoffice/news/articles/2008/10/bono.html [hereinafter *Bono's Bikini Party*].

[54] *But see* Lauren Gelman, *Privacy, Free Speech, and "Blurry-Edged" Social Networks*, 50 B.C. L. REV. 1315, 1316-19 (2009) (describing reasons users might choose to post quasi-private material to places viewable by anyone, expecting that only those with a legitimate interest will choose to view it).

[55] Posting of Mark Zuckerberg to The Facebook Blog, http://blog.facebook.com/ (Dec. 1, 2009, 18:23 EST).

[56] *See* Grimmelmann, *supra* note 6, at 1160-64.

use in an electronically mediated environment that gives you little feedback on who any given communication is visible to. Instead, social networking sites activate the subconscious cues that make users think they are interacting within bounded, closed, *private* spaces. Indiscretions follow because users are cognitively distracted from the work of predicting the social consequences of their activities.

Moreover, in many cases of Facebook privacy trouble, the victim has made every reasonable effort to keep the information confidential. Miss New Jersey 2007 was blackmailed by someone who got a hold of some mildly racy photographs that she posted to what she thought was a Facebook photo album restricted to friends only.[57] As between blackmailer and victim, the fault is clear. Similarly, Facebook's ill-fated Beacon advertising program utilized users' names and faces to hawk the products that they bought on other sites, like Blockbuster or Zappos.[58] Nothing in their previous online experience would have led them to expect such a model of information sharing and exposure.[59]

Indeed, the social-network aspects of social media mean that even information that people deliberately try to keep offline can find its way online. A group of students at MIT were able to identify gay users on Facebook with surprisingly high accuracy, simply by looking to see whether they had gay friends, even when the users themselves had not posted their sexual orientation.[60] Photo tagging is another good example: the entire untagging ritual is possible–and necessary–because Facebook allows users to tag photos of each other *before* the taggee has a chance to object.[61]

---

[57] *See* Austin Fenner, *N.J. Miss in a Fix over Her Pics*, N.Y. POST, July 6, 2007, at 5.

[58] *See generally* William McGeveran, *Disclosure, Endorsement, and Identity in Social Marketing*, 2009 U. ILL. L. REV. 1105 (discussing Beacon).

[59] *See generally id.*

[60] *See* Carolyn Y. Johnson, *Project 'Gaydar'*, BOSTON GLOBE, Sept. 20, 2009, http://www.boston.com/bostonglobe/ideas/articles/2009/09/20/project_gaydar_an_mit_experiment_raises_new_questions_about_online_privacy/.

[61] Help Center, Facebook, http://www.facebook.com/help/?page=831 (last visited May 14, 2010).

C. Myth 3: Facebook Users' Desire for Privacy Is Unrealistic

If users want privacy and fail in their efforts at obtaining it, it is tempting to tell them to stop trying, to dismiss their desire as a pipe dream, a relic of the preinformation age. A decade ago, Sun's Scott McNeely said, " 'You have zero privacy anyway . . . Get over it.' "[62] Google's Eric Schmidt echoed the sentiment when he said, "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."[63] In legal filings, his company has argued that "even in [a] desert, complete privacy does not exist."[64] The argument echoes those made by legal scholars such as Richard Posner, who has compared privacy "to the efforts of sellers to conceal defects in their products."[65]

This too is a myth. It is true that Facebook regularly smashes its users' fragile and precious hopes for privacy. Although it may be wise to remember that anything posted to the site could become public knowledge,[66] it does not follow that full and open publicity is natural, desirable, or inevitable. Facebook users' desire for privacy is realistic, and we should search for ways to help them achieve it.

The vast majority of things posted to Facebook do not wind up on the metaphorical front page of the *New York Times*. Andrea is

---

[62] Polly Sprenger, *Sun on Privacy: 'Get Over It'*, WIRED, Jan. 26, 1999, http://www.wired.com/politics/law/news/1999/01/17538.

[63] *Google CEO on Privacy (VIDEO): 'If You Have Something You Don't Want Anyone to Know, Maybe You Shouldn't Be Doing It'*, HUFFINGTON POST, Dec. 7, 2009, http://www.huffingtonpost.com/2009/12/07/google-ceo-on-privacy-if_n_383105.html. It should be noted that this is the same man who instituted a company policy against talking to CNET reporters after one of them reported details on his family's finances. *See* Jennifer Westhoven, *CNET: We've Been Blackballed by Google*, CNNMONEY.COM, Aug. 5, 2005, http://money.cnn.com/2005/08/05/technology/google_cnet/.

[64] Defendant Google, Inc.'s Memorandum of Law in Support of Its Motion to Dismiss Complaint at 2, Boring v. Google, Inc., 598 F. Supp. 2d 695 (W.D. Pa. 2008) (No. 08-cv-694).

[65] RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 46 (7th ed. 2007).

[66] *See Obama Advises Caution in Use of Facebook* (YouTube broadcast), http://www.youtube.com/watch?v=si1gNXqH7iw (last visited May 14, 2010) ("I want everybody here to be careful about what you post on Facebook, because, in the YouTube age, whatever you do, it will be pulled up again later somewhere in your life.").

the exception, not the rule. This should not be a surprise. The site is not designed to be fully public, and that is not how people use it. Instead, it facilitates back-and-forth conversations among small groups,[67] social contexts not intended to be intelligible to outsiders, and bounded spaces for interaction. The same network structure that helps people communicate also predictably limits the spread of what they say.[68] Facebook's moves towards making more information public have been necessary, from Facebook's point of view, precisely *because* people were sharing information less widely than the site would have liked.[69]

Recognizing this truth about sociality and information-sharing, most people are willing to say at least a few things about themselves on Facebook that they would not shout from the rooftops. They expect not to be harmed, and most of the time, they are right.[70] At some point, this expectation starts to create its own reality–to become the kind of expectation that creates enforceable duties at law. Privacy law is full of them, from criminal procedure's 'reasonable expectation of privacy'[71] to the "reasonable person" standard of offensiveness used in the intrusion on seclusion,[72] public disclosure of private facts,[73] and false light[74] torts.

---

[67] Welcome to Facebook, *supra* note 6 ("Facebook helps you connect and share with the people in your life.").

[68] *See* Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 958-59 (2005).

[69] *Compare* Posting of Mike Masnick to Techdirt, http://www.techdirt.com/ (May 4, 2009, 13:57 EST) ("Facebook, however, with its fine-grained privacy controls . . . is pretty limited in how much it can open up. The more it tries to become like Twitter, the more its own setup gets in the way."), *with* Posting of Marshall Kirkpatrick to ReadWriteWeb, http://www.readwriteweb.com/ (Jan. 9, 2010, 21:25 EST) ("Now that it has 350 million people signed up . . . now Facebook decides that the initial, privacy-centric, contract with users is out of date. That users actually want to share openly, with the world at large, and incidentally . . . that it's time for increased pageviews and advertising revenue, too.").

[70] *See* James Grimmelmann, *Accidental Privacy Spills*, J. INTERNET L., July 2008, at 3, 10-12 [hereinafter *Accidental Privacy Spills*].

[71] *See, e.g.*, Smith v. Maryland, 422 U.S. 735, 740 (1979).

[72] RESTATEMENT (SECOND) OF TORTS § 652B (1977).

[73] *Id.* § 652D(a).

[74] *Id.* § 652E(a).

Indeed, not just privacy law but *privacy itself* is socially constructed in just this way. My anger when you take a 'Wall' post and forward it to my employer is grounded in your violation of the norms of our relationship–of the social context that defined the post in its original venue.[75] To treat everything on Facebook as fair game is to run a steamroller over the millions of differentiated, localized social contexts on Facebook, each with its own norms of what is appropriate behavior and how information should flow. Those norms are inseparable from the sociality of the site itself: the self-expression, relationships, and communities it helps its users build.[76] People are not really trading off privacy against socializing on Facebook so much as using it to define them both, simultaneously, in relation to each other.

Examples may help clarify the point. Take Andrea. Her photographs were taken to memorialize a frozen moment. They were an attempt to tell the story of her day on the beach with Bono with an aura of seemingly unmediated, authentic truth,[77] Andrea used Facebook as such: she posted the photos to it to make them visible to what she thought was a small group of friends.[78] The closeness of her relationship to those friends was bound up with the closeness of her relationship with Bono–the latter became an element of the former. Both of these relationships were more meaningful to her because of the photographs and because she did not indiscriminately show them to the world. When the photographs escaped from that social context, their meaning changed; suddenly Andrea was a participant in a tabloid driven "scandal" about Bono's seemingly debauched behavior.[79] When interviewed, she protested: "I think that for somebody who's much

---

[75] *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 58-62 (2010).

[76] *See* Grimmelmann, *supra* note 6, at 1206.

[77] *See generally* SUSAN SONTAG, ON PHOTOGRAPHY 5 (1977) ("Photographs furnish evidence. Something we hear about, but doubt, seems proven when we're shown a photograph of it."); Opinionator, http://opinionator.blogs.nytimes.com/category/errol-morris/ (last visited May 14, 2010) (collecting a *New York Times* series of blog posts by Errol Morris on the truthfulness and deceptiveness of photographs).

[78] SONTAG, *supra* note 77, at 5.

[79] Tapper, *supra* note 1.

older than I am . .no thank you … No . . . God no! He's a friend of mine and that's pretty much it."[80]

Consider the women who posted their bra colors to Facebook.[81] The point was to raise awareness of breast cancer;[82] however, had a male coworker approached them the next day and said "So you wore a pink bra yesterday; what color are you wearing today?" it would have been not just socially inappropriate, but potentially actionable as workplace sexual harassment.[83] The bra-color posts were designed for the social context of Facebook, but what is acceptable in one context becomes a privacy violation when decontextualized.

The bra-color example also illustrates the deeper point that privacy itself cannot be understood apart from the social contexts that make it meaningful.[84] The zing of the meme came from making 'public' a typically 'private' subject–mirroring the consciousness-raising agenda of making breast cancer a political subject, rather than just a personal issue for afflicted women. Women who posted their bra colors were engaged both in an act of self-expression and in conscious affiliation with a larger community of women.[85] The inappropriateness of the male coworker's comment comes not so much from the fact that bra color is a private subject as from its violation of the very specific way the meme constructs the public/private divide in a socially embedded fashion.

---

[80] Tapper, *supra* note 1.

[81] Posting of Hortense to Jezebel, *supra* note 23.

[82] *Id.*

[83] *See* Meritor Savings Bank, FSB v. Vinson, 477 U.S. 57, 63-68 (1986) (establishing the hostile work environment standard for title VII liability); McPherson v. City of Waukegan, 379 F.3d 430, 434, 439 (7th Cir. 2004) (finding that questions about the plaintiff's bra color were not actionable standing alone, but were "inappropriate" and ultimately considered by the court in determining whether the harassment was "pervasive").

[84] *See* NISSENBAUM, *supra* note 75, at 148.

[85] Posting of Hortense to Jezebel, *supra* note 23.

D. Myth 4: Database Regulation Will Make Facebook Privacy-Safe

If, as I have been arguing, privacy mistakes are endemic on social networking sites, the next question is what the law can and should do about it. Much of the time, the answer will be nothing. Many privacy harms, embarrassing though they may be, are beneath the threshold at which the law ought to take notice. The fact that your mother found out your plans to attend International Skip School Day is not, and should not be, a legally cognizable harm.[86]

Moreover, there are often good reasons to let people make even serious privacy mistakes. Respecting a person's autonomy to make privacy choices requires us to give him or her the freedom to fail. Indeed, some privacy mistakes are good for society, like the one made by the burglar who checked his Facebook account from his victim's computer and forgot to log out.[87] Even a privacy 'fail' can be an important learning experience. Youthful experimentation, bumps and bruises included, is a significant part of how people come to understand how privacy works and what it means to them.[88]

Most of the time, there are good policy reasons for making users the stewards of their own online privacy. Privacy is an intensely personal good, especially in the social dimensions at stake on social networking sites. That means it is impossible for anyone but the user to define what privacy is important for him or her. The user is also the best-motivated person to protect his or her privacy because the user is generally the cheapest cost-avoider. Even though the privacy harms of Facebook use are real, so are the

---

[86] *See, e.g.*, Posting of 15 Funny Facebook Fails to Oddee, http://www.oddee.com/ (Jan. 11, 2010) (listing fifteen humorous "Facebook [f]ails").

[87] *See* Edward Marshall, *Burglar Leaves His Facebook Page on Victim's Computer*, JOURNAL (Martinsburg, W. Va.), Sept. 16, 2009, http://www.journal-news.net/page/content.detail/id/525232.html.

[88] *See* boyd, *supra* note 6, at 286 (describing how a teenager's notion of privacy is often different from his or her parents' notion of privacy); *see also* Anupam Chander, *Youthful Indiscretion in an Internet Age*, *in* THE OFFENSIVE INTERNET: SPEECH, PRIVACY, AND REPUTATION (Saul Levmore & Martha C. Nussbaum eds., forthcoming Jan. 2011).

social benefits–if the walls of your house are made of glass, throwing stones is not the solution to your privacy problems.

That, however, still leaves a substantial rump of cases in which legal intervention is justifiable. Some, like Miss New Jersey's case of blackmail,[89] are easily addressed under existing law. Others, like Beacon, are trickier: Blockbuster's participation in Beacon clearly violated the Video Privacy Protection Act,[90] but Zappos and Epicurious are less clearly troublesome given the lack of omnibus privacy protections in the United States.[91] Many harms–Andrea's photographs of herself with Bono come to mind–may not rise to the level justifying ex post tort liability under current law,[92] but would be good to prevent ex ante if at all possible.

The dominant modern approach to information privacy regulation focuses on limiting misuse of databases.[93] In the United

---

[89] *See supra* text accompanying note 57.

[90] *See* 18 U.S.C. § 2710(b)(1) (2006) (providing for liability against "[a] video tape service provider who knowingly discloses" a consumer's personal information).

[91] *See* Jennifer McClennan & Vadim Schick, *"O, Privacy" Canada's Importance in the Development of the International Data Privacy Regime*, 38 GEO. J. INT'L L. 669, 675 (2007) ("The United States has adopted a much less regulated approach to data privacy protection.").

[92] *See, e.g.*, Purcell v. Ewing, 560 F. Supp. 2d. 337, 344 (M.D. Pa. 2008) (dismissing a defamation complaint pertaining to statements made about the plaintiff on an online message board because "[r]easonable readers of [the poster's] comments would understand[] them as the unsubstantiated opinions and imprudent tirades of one who harbored intense dislike for [the plaintiff]."). In the Bono example, it is not clear that the publication would have been found to be 'highly offensive,' even if it was embarrassing. *See supra* text accompanying notes 1-5. Moreover, Bono's celebrity status creates a potential newsworthiness defense. *See* Virgil v. Time, Inc., 527 F.2d 1122, 1129 (9th Cir. 1975) (quoting RESTATEMENT (SECOND) OF TORTS § 652F cmt. f (Tentative Draft No. 13, 1967)) (discussing the legal standard for the newsworthiness defense).

[93] *See, e.g.*, SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., U.S. DEP'T OF HEALTH, EDUC., & WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973), *available at* http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm (defining " 'fair information practice' "); *Fair Information Practice Principles*, FED. TRADE COMM'N., http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited May 14, 2010) [hereinafter *Fair Information*].

States, the so-called 'Fair Information Practices' are not binding law but are used by the Federal Trade Commission and industry self-regulation groups to set benchmarks of good conduct.[94] In Europe, the Data Protection Directive makes them enforceable.[95] The high-level idea is to ensure that personal data is collected only with disclosure of the legitimate purposes that it will be used for–and then to ensure it is used only for those purposes.[96] In the words of the Data Protection Directive, personal information must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."[97]

This database frame is useful. The secret, error-riddled, and sprawling database has a uniquely Kafkaesque tone.[98] The Fair Information Practices approach tries to tame the database by keeping it open, accurate, and limited to its original uses.[99] That is a good way of thinking about credit card data or a collection of search queries: essential for daily life but highly dangerous in the wrong hands (think of a small-town sheriff with personal grudges). Informed consent at the time of collection legitimates the primary use; secondary uses are forbidden.

For some threats, the database frame is also a useful way of thinking about Facebook. Facebook's huge reservoirs of personal information are tempting to outsiders. That is a reason why its general counsel told an audience of lawyers that Facebook would vigorously contest subpoenas for personal information, saying,

---

[94] *See* Gaia Bernstein, *The Paradoxes of Technological Diffusion: Genetic Discrimination and Internet Privacy*, 39 CONN. L. REV. 241, 268 (2006) ("Congress did not implement the FTC's recommendations for legislation codifying the fair information practices principles."); *see also Fair Information*, *supra* note 93, at pt. (A) n.28.

[95] *See generally* Council Directive 95/46, 1995 O.J. (L 281) 31 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (discussing "the protection of individuals with regard to the processing of personal data and . . . the free movement of such data").

[96] *Id.* art. 6.1(b).

[97] *Id.*

[98] See Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1423 (2001).

[99] *See Fair Information*, *supra* note 93, at A.1-.4.

" 'We're itching for that fight.' "[100] The fear of secondary use is also at work when privacy advocates worry that Facebook will turn its user data over to third-party advertisers.[101]

As useful as the database frame is in thinking about the data processing taking place on the back end, it is not so helpful in thinking about the social interactions taking place on the front end. Neither 'limited data collection,' 'no secondary use,' nor 'full disclosure' really gets at the user-user relationships on Facebook.

In the first place, Facebook's social nature means that there is nothing so personal that it is entirely off-limits. A typical Facebook profile contains answers to most of the questions employers are not allowed to ask of job applicants: race, sex, age, national origin, religion, and marital status.[102] People are voluntarily uploading it all because they are social and because Facebook scratches social itches. If you were to tell Facebook that it could not collect these types of information, you would kill it. Given the profound social benefits that social media offer, that would be a tragic outcome.

Trying to limit secondary use is also surprisingly difficult. The problem comes in defining the original purposes for which the data is collected. Defined broadly–in the words of Facebook's mottos, to "connect and share with the people in your life"[103] or "the power to share and make the world more open and connected"[104]–it is a purpose that swallows everything on the site. Everyone who uses Facebook gives it personal data for the express purpose of sharing that data with other users, which implies that pretty much anything other users do or see on the site falls within the original, legitimate purpose.

---

[100] Amy Miller, *Facebook GC Tells Lawyers He's Looking for a Fight*, LAW.COM., Feb. 2, 2010, http://www.law.com/jsp/article.jsp?id=1202441887703.

[101] *See, e.g.*, Complaint, Request for Investigation, Injunction, and Other Relief at 1, *In re* Facebook, Inc., F.T.C. (Dec. 17, 2009), *available at* http://www.epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.

[102] *See* David Phelps, *HR and Facebook: It's Complicated*, STAR TRIB. (Minneapolis, Minn.), Feb. 7, 2010, at 1A (quoting law professor Deborah Schmedemann as saying, "If you have that information and if it goes into the decisionmaking process, that would be illegal").

[103] Welcome to Facebook, *supra* note 6.

[104] Facebook, http://www.facebook.com/facebook (last visited May 14, 2010).

Defining purpose narrowly, on the other hand, would render the site unusable. If you think the flood of Facebook notifications is bad now, just wait until Facebook asks you for fresh, specific consent for each transfer of personal data to an individual user. Demanding explicit consent every time information is shared with someone other than its specific, original audience could require hundreds of prompts, per user, per day. It would make viewing one's News Feed or clicking from Wall to Wall impossible. It is, in other words, incompatible with the very reasons that people use Facebook and other social software.[105]

In between those two extremes, however, it is difficult to make the concept of 'secondary use' bear much weight. If it means 'any use not originally contemplated by the user,' then all we have managed to do is restate the problem. We got into this mess precisely because users have been unable to predict all the ways in which their information might be seen. We need a way to get more intellectual traction on the question of which uses they expect and which ones they do not–and on how to bring their expectations more closely in line with reality.

That sounds like the problem of disclosure, but disclosure as usually practiced by commercial data controllers is weak tea in a social setting. The law does not demand that friends give each other full disclosure of their data collection practices when they are catching up to each on the last few months. Transpose that conversation to Facebook, and they are still not giving or expecting disclosure. The confidences are regulated by implicit social norms, rather than by explicit promises. Facebook can easily disclose its own practices; however, when it comes to what other users might choose to do, it cannot say much more than "anything can

---

[105] *See* Grimmelmann, *supra* note 6, at 1151.

> [P]eople have *social* reasons to participate on *social* network sites, and these social motivations explain both why users value Facebook notwithstanding its well-known privacy risks and why they systematically underestimate those risks. Facebook provides users with a forum in which they can craft social identities, forge reciprocal relationships, and accumulate social capital. These are important, even primal, human desires, whose immediacy can trigger systematic biases in the mechanisms that people use to evaluate privacy risks.

Id.

happen."[106] Again, the database-oriented Fair Information Practices approach is not wrong. It just does not provide enough leverage on the specific problem of social privacy in social media.

III. PRIVACY AS PRODUCT SAFETY

To review: people use Facebook in complicated ways, sometimes leading to privacy trouble. There is often a significant gap between what users expect will happen with their personal information and what actually does happen. Overall, the beneficial uses of Facebook outweigh its dangers, but it would be good to find ways of preventing some of the specific privacy harms. Facebook probably cannot be made perfectly safe for privacy, but it could almost certainly be made safer.

Put this way, there is a natural affinity between the privacy law challenges facing Facebook and another area of the law: product safety. It is true that using Facebook can be hazardous to your privacy, but a hammer can be hazardous to your thumb. People need tools, and sometimes they need dangerous tools. Hammers are physically dangerous; Facebook is socially dangerous. We should not ban hammers, and we should not ban Facebook. The challenge for policymakers is to ensure that the tools people do use are not *unnecessarily* dangerous.

Thus I would like to suggest that some of the lessons the law has learned in dealing with product safety could usefully be applied to the analogous problem of privacy safety. Unlike database regulations, which tend to focus only on the flow of information in itself, a product-safety approach can also consider how people use social media. After a survey of previous work on this metaphor, this part will tentatively map the products liability doctrine onto the problem of making social media safe for privacy. The fit is not perfect, but it is surprisingly good. This part will conclude with a case study of another recent, high-profile online privacy debacle: the launch of Google Buzz.[107] I will argue that

---

[106] Privacy Policy, Facebook, http://www.facebook.com/policy.php (last visited May 14, 2010) ("You understand that information might be re-shared or copied by other users.").

[107] *See* Miguel Helft, *Anger Leads to Apology from Google About Buzz*, N.Y. TIMES, Feb. 15, 2010, at B3 [hereinafter Helft, *Anger*]; Miguel Helft,

Buzz was a defective product–one that was unreasonably dangerous to personal privacy.

A. Previous Work

Despite their different historical roots and paths of development in the twentieth century, privacy law and product liability law fit squarely within the intellectual and doctrinal system of modern tort law. Indeed, the scholar most closely identified with the field of torts as a whole, William L. Prosser,[108] played critical roles in the development of both. In the same remarkable year, he published both the essential modern codification of the privacy torts[109] and the authoritative history of the rise of strict liability for the sellers of defective products,[110] both of which have been highly influential in the adoption of these causes of action by courts.[111] As the reporter for the *Restatement (Second) of Torts*, he brought both within the *Restatement*'s overall doctrinal and intellectual project.[112]

Modern scholars have sought to use the Prosser-led transformation of products liability law in the 1960s as an institutional model for the transformation of privacy law today. Eric Jorstad has observed that privacy regulation today looks a lot

---

Critics Say Google Invades Privacy with New Service, N.Y. TIMES, Feb. 13, 2010, at B1.

[108] *See generally* WILLIAM L. PROSSER, HANDBOOK OF THE LAW OF TORTS (1941). Professor Prosser was also the reporter for the *Restatement (Second) of Torts*; therefore, it is unsurprising that it bears his influence. *See* RESTATEMENT (SECOND) OF TORTS I (1965) (listing Prosser as the reporter).

[109] *See generally* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960) (discussing the privacy torts among the fifty states).

[110] *See generally* William L. Prosser, *The Assault upon the Citadel (Strict Liability to the Consumer)*, 69 YALE L.J. 1099 (1960) [hereinafter *Strict Liability*].

[111] *See, e.g.*, Greenman v. Yuba Power Prods., Inc., 377 P.2d 897, 901 (Cal. 1962) (in bank) (citing *Strict Liability*, *supra* note 110, at 1124-34) (adopting the rule of strict liability in product liability action).

[112] *Compare* RESTATEMENT (SECOND) OF TORTS §§ 652A-652I (1977) (privacy torts), *with id.* §§ 388-408 (product liability), *and id.* § 402A(1), (2)(a) (imposing liability on the seller of "any product in a defective condition unreasonably dangerous to the user . . . although . . . the seller has exercised all possible care"). The *Restatement* thus subjected both areas to its general rules, such as its common defenses and remedies. *Id.* §§ 887-895, 901-932.

like product safety regulation before the strict liability and regulatory revolution of the 1960s.[113] Benjamin Sachs traces the connection further back, drawing a parallel between the rise of the industrial economy around the turn of the twentieth century and the information economy around the turn of the twenty-first century.[114] Their common point about society and the law is that an era in which individuals could generally protect themselves has given way to an era in which social and technological forces make it far harder for consumers to be successful stewards of their own safety.[115] The law caught up with the changes in how products were made and sold; the question we face today is how the law will catch up with the changes in how information is made and sold.

When it comes to specific proposals, Sachs argues that data collectors should be held strictly liable in tort for failure to secure the data they store.[116] His emphasis is on back-end data breaches–harms caused when unauthorized intruders gain access to the stored data on users[117]–and thus can easily be reconciled with the database model of privacy discussed above.[118] Sarah Ludington, also noting the institutional parallel to product safety,[119] offers a similar proposal of a tort for the misuse of stored personal data, one that would explicitly enforce the Fair Information Practices.[120]

Other than the historical parallel, the product safety metaphor is not doing as much work in these proposals as it could. Sachs' and Ludington's proposals are substantively similar to those made

---

[113] Eric Jorstad, *The Privacy Paradox*, 27 WM. MITCHELL L. REV. 1503, 1511-12 (2001).

[114] *See* Benjamin R. Sachs, *Consumerism and Information Privacy: How Upton Sinclair Can Again Save Us from Ourselves*, 95 VA. L. REV. 205, 231-33 (2009).

[115] *See id.* at 219-23 (providing a discussion of the four primary breach of privacy issues and their effects on individuals).

[116] *Id.* at 240.

[117] *Id.* at 219-23.

[118] *See generally* Solove, *supra* note 98 (discussing the database model of privacy).

[119] *See* Sarah Ludington, *Reining in the Data Traders*: *A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 171-72 (2006).

[120] *Id.* at 171-87 (discussing 5 U.S.C. § 552a(b), (d)-(e) (2006)).

by scholars who have not relied on the metaphor.[121] Indeed, the database-centric Fair Information Practice approach has been the basis for most of the information privacy law the United States actually has.[122] To the extent that we seek a common-law tort metaphor for imposing a duty to carry out back-end data processing securely and confidentially, Danielle Citron's invocation of strict liability under *Rylands v. Fletcher* may be even more on point than products liability.[123] In her description, large "reservoirs" of personal data are akin to large reservoirs of water: both are liable to cause great damage if their contents escape.[124] The duty to handle personal data securely has relatively little to do with how the data was acquired: the same concerns arise whether it is consciously entered into an online quiz or generated invisibly by a grocery-store scanner.

Instead, the greatest–and, so far, largely untapped–potential of the product safety metaphor is on the front end. The parts of an online service that users actually see and interact with are more like a 'product' than the largely invisible back-end data processing. Users have expectations about what the service will do; a site that acts otherwise frustrates those expectations. A site that violates their privacy causes harms, and when those harms are preventable with better design choices or more careful programming, it makes sense to ask whether the site operator should be held accountable for them. What follows, then, are a few thoughts about how

---

[121] *See, e.g.*, Corey A. Ciocchetti, *The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practices*, 26 J. MARSHALL J. COMPUTER & INFO. L. 1, 27-30, 44-45 (2008).

[122] *See* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 922 (2009) ("Overall, the approach in the United States to information privacy law in the private sector has been through sector-specific laws containing [Fair Information Practices], which have been enacted by federal and state lawmakers.").

[123] *See* Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 244 (2007) (citing Rylands v. Fletcher, (1868) 3 L.R.E. & I. App. 330 (H.L.)).

[124] *Id.* at 278-80. Citron also raises institutional and societal parallels similar to those that Sachs and Jorstad invoke. *Compare id.* at 280-83 (citations omitted), *with* Sachs, *supra* note 114, at 231-32, *and* Jorstad, *supra* note 113, at 1511-12.

product-safety law–principally, the branch of tort law known as products liability–may have useful lessons for thinking about privacy and social software.

B. The Basics of Product Safety Law

The starting point of the simile is the starting point of products liability: holding sellers liable for the harms their products cause. As the *Restatement* puts it, "One engaged in the business of selling or otherwise distributing products who sells or distributes a defective product is subject to liability for harm to persons or property caused by the defect."[125] This rule, simple as it may seem, has several important consequences.

The first point implicit in the basic duty of sellers to make their products safe is that sellers can be held liable even when the consumer is at fault in the accident.[126] The consumer's recovery may be reduced by principles of comparative fault,[127] but the seller could still be held liable for selling the consumer a defective product in the first place.[128] All that is required is the usual but-for and proximate causal connection.[129] Even the consumer who

---

[125] RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 1 (1998).

[126] *See id.* § 1 cmt. a.

> Courts early began imposing liability without fault on product sellers for harm caused by such defects, holding a seller liable for harm caused by manufacturing defects even though all possible care had been exercised by the seller in the preparation and distribution of the product. In doing so, courts relied on the concept of warranty, in connection with which fault has never been a prerequisite to liability.

Id.

[127] *Id.* § 17(a). Evaluating the user's actual conduct under comparative fault is more respectful of his or her agency than a broad rule that the social network site has no duty at all to him or her, which makes the user's own conduct irrelevant under all circumstances.

[128] *See id.*

[129] *See id.* § 15 ("Whether a product defect caused harm to persons or property is determined by the prevailing rules and principles governing causation in tort."); DAVID G. OWEN, PRODUCTS LIABILITY LAW §§ 11.1-.2, 12.1-.3 (2d ed. 2008) (providing a discussion of cause in fact, proximate cause, and the various "[t]ests and [p]roof of [c]ausation"); John D. Rue, Note, *Returning to the Roots of the Bramble Bush: The 'But For' Test Regains Primacy in Causal Analysis in the American Law Institute's Proposed Restatement (Third) of Torts*, 71 FORDHAM L. REV. 2679, 2719-20 (2003) (discussing the American Law Institute Reporters' support for the but-for causation rule).

misuses the product can sometimes recover; after all, certain kinds of misuse are foreseeable at the time of sale.[130] If Andrea was careless in sharing her photos with the New York network, this was a carelessness that Facebook, arguably, should have anticipated and guarded against.

A second implicit point in the basic duty of sellers to make their products safe is that disclaimers are not a substitute for a safe product. The *Restatement* makes disclaimers unenforceable "for harm to persons,"[131] and many states have laws forbidding the disclaimer of product warranties.[132] This rule has particular importance for services like Facebook, which require users to 'consent' to contractual agreements when they sign up, along the way disclaiming all liability on Facebook's part for any harms in this life or the next.[133] The products liability paradigm calls into question the appropriateness of allowing such waivers.[134]

A third point is that sellers are liable for generic design defects as well as for individual manufacturing defects.[135] Even if

---

[130] OWEN, *supra* note 129, § 13.5 (explaining the doctrine of misuse).

[131] RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 18 (1998).

[132] OWEN, *supra* note 129, § 4.9 (citing CONN. GEN. STAT. ANN. § 42a-2-316(5) (West 2009); ALA. CODE § 7-2-316(5), -719(4) (LexisNexis 2006); D.C. CODE § 28:2-316.01 (2001); ME. REV. STAT. ANN. tit. 11, § 2-316(5) (1995); MD. CODE ANN. COM. LAW § 2-316.1 (LexisNexis 2002); MASS. GEN. LAWS ANN. ch. 106, § 2-316A (West 1999); MISS. CODE ANN. § 75-2-315.1, -719(4) (1972); N.H. REV. STAT. ANN. § 382-A:2-316(4) (1994); R.I. GEN. LAWS § 6A-2-329(2) to (3)(a) (2001); VT. STAT. ANN. tit. 9A, § 2-316(5) (1994); WASH. REV. CODE § 62A.2-316(4) (2007)).

[133] *See* Statement of Rights and Responsibilities, Facebook, http://www.facebook.com/terms.php (last visited May 14, 2010) ("WE ARE PROVIDING FACEBOOK 'AS IS' WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES . . . OUR AGGREGATE LIABILITY ARISING OUT OF THIS STATEMENT OR FACEBOOK WILL NOT EXCEED THE GREATER OF ONE HUNDRED DOLLARS ($100) OR THE AMOUNT YOU HAVE PAID US IN THE PAST TWELVE MONTHS.").

[134] *See* Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425, 436-41, 456-57, 471 (2008) (discussing contractual waivers).

[135] RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 2(a)-(b) (1998). The substantive standard of liability differs between them: manufacturing defects are judged according to a rule of strict liability, whereas design defects are judged according to a more negligence-like, risk-utility calculus. *Compare id.* § 2(a) (manufacturing defects), *with id.* § 2(b) (design defects).

troublesome in practice,[136] this equivalence makes intuitive sense. A gas tank manufactured with slipshod welding and one designed with excessively thin walls will cause the same damage if they rupture and explode, and the carmaker is equally culpable for selling an exploding car.[137] Given that the most striking privacy harms on Facebook stem from design mistakes, rather than one-off bugs afflicting individual users, it again makes sense not to take design decisions off the table entirely.[138]

This attention to *design* is a critical and valuable feature of products liability law. The *Restatement* explicitly requires courts to consider the costs and benefits of the design alternatives open to the seller; the definition of a design defect requires proof that the actual design was inferior to a "reasonable alternative design" that would have prevented the harm.[139] The court, in other words, must

---

[136] *See generally* James A. Henderson, Jr., *Judicial Review of Manufacturers' Conscious Design Choices: The Limits of Adjudication*, 73 COLUM. L. REV. 1531 (1973) (discussing the difficulties faced by courts in rendering judgments concerning design defects).

[137] *See* RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 3 & cmt. b (1998).

> [O]occasionally a product design causes the product to malfunction in a manner identical to that which would ordinarily be caused by a manufacturing defect . . . Section 3 allows the trier of fact to draw the inference that the product was defective whether due to a manufacturing defect or a design defect. Under those circumstances, the plaintiff need not specify the type of defect responsible for the product malfunction.

Id.

[138] *Cf.* Scott, *supra* note 134, at 459-60, 467-70 (discussing ambiguity of software defects between "manufacturing" and "design"). I would add that the replicability of software means that every user's copy of the "product" is actually identical. *See generally* James Grimmelmann, Note, *Regulation by Software*, 114 YALE L.J. 1719 (2005) (discussing the predictable consequences of using software as a regulator). This fact collapses the most obvious distinction between manufacturing defects (in which a single product falls short of the usual standard for its class) and design defects (in which the entire class falls short). Michael Scott would make the distinction based on the point during the software production process at which the mistake was introduced. Scott, *supra* note 134, at 459. I am not so sure. In addition to the evidentiary costs of such an approach, it seems unnecessary in light of the purposes of products liability law. Whether Facebook ought to be liable for users' privacy harms ought to depend on policy choices and evidence of the specific software features at issue, rather than details of the software design and testing process.

[139] RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 2(b) (1998); OWEN, *supra* note 129, § 8.5.

think through the same kinds of tradeoffs that a reasonable seller would–which puts legal pressure on actual sellers to choose better overall designs. While Facebook is not about to explode like a poorly designed gas tank–its privacy harms are extensions of "normal" use rather than catastrophic accidents–there are ways in which better designs can make it more privacy-safe.

For one thing, good product design discourages or prevents particularly hazardous uses. For example, guards on a punch press keep the operator from sticking his or her hand in at the wrong time,[140] while the safety on a pistol protects the user who drops it.[141] Similarly, good software interfaces can suggest low-risk actions and make high-risk ones less tempting. Facebook already uses this principle to good effect. Its private messages have a 'reply' button but no 'forward' button–you cannot, within Facebook itself, easily violate the privacy of your correspondents.[142] That is a smart, safe design choice.

For another thing, good product design makes consequences predictable. Sharp spinning blades can be handled safely–provided you know where they are. The on-by-default New York City network that caused Andrea and Bono such trouble was a feature with unintuitive, hard-to-predict consequences.[143] Similarly, the reason that Beacon and News Feed were such disruptive, destructive changes is that nothing Facebook had done–indeed, nothing anyone had done–prepared users for the sudden shift in how their personal information would be used.[144] The smaller the gap between expected and actual exposure, the safer; good design can help close that gap.

---

[140] *See, e.g.*, Rhoads v. Service Mach. Co., 329 F. Supp. 367, 369-70, 376-77 (E.D. Ark. 1971) (holding that a manufacturer's failure to equip a press with safety guards raised a jury question on the defendant's negligence).

[141] *See, e.g.*, Sturm, Ruger, & Co. v. Day, 594 P.2d 38, 41, 44 (Alaska 1979) (holding that a gun manufacturer may be liable for a defective safety on a pistol).

[142] *Cf. Accidental Privacy Spills*, *supra* note 70, at 8 (discussing the feasibility of software limits on forwarding).

[143] *See Bono's Bikini Party*, *supra* note 53.

[144] *See* Grimmelmann, *supra* note 6, at 1200-02 (discussing the dangers of unpredictable software "lurches").

Product safety law also scrutinizes consumers' expectations about products.[145] While the 'consumer expectations' test itself–which focuses on consumers' expectations of how safe a product should be, rather than on how they expect it to function–is troublesome to apply in practice;[146] in a broader sense, consumer expectations pervade products liability. If consumers were perfectly informed about exactly what a device would do in every case, there would be no accidents. They would not have bought the trampoline with the wobbly leg or they would not have done handstands on it or they would have stopped jumping a minute sooner. Every accident is an example of frustrated consumer expectations. Asking how its users expect Facebook to work–and when their expectations go wrong–again directs our attention to the right place.

In addition to scrutinizing design decisions, products safety law also pays attention to the quality of warnings.[147] A good warning can point out hidden dangers to help a user avoid them or even make an informed decision to avoid the product entirely.[148] Here again, tort law shows some common sense. Some defects are so obvious that there is no duty to warn against them;[149] others are so serious that no warning can cure them.[150] Facebook's blistering pace of design innovation has often outstripped its ability to document the changes or explain them clearly to users.[151] Sensible

---

[145] *See generally* Douglas A. Kysar, *The Expectations of Consumers*, 103 COLUM. L. REV. 1700 (2003) (discussing the role of consumer expectations in product safety law).

[146] *See* James A. Henderson, Jr. & Aaron D. Twerski, *Consumer Expectations' Last Hope: A Reply to Professor Kysar*, 103 COLUM. L. REV. 1791, 1792 (2003).

[147] RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 2(c) (1998).

[148] *See* Liriano v. Hobart Corp., 170 F.3d 264, 270 (2d Cir. 1999).

[149] RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 2 cmt. j (1998) ("In general, a product seller is not subject to liability for failing to warn or instruct regarding risks and risk-avoidance measures that should be obvious to, or generally known by, foreseeable product users.").

[150] *See, e.g.*, Glittenberg v. Doughboy Recreational Indus., 491 N.W.2d 208, 216 (Mich. 1992) (citation omitted) ("A warning is not a Band-Aid to cover a gaping wound, and a product is not safe simply because it carries a warning.").

[151] *See, e.g.*, Posting of Jason Kincaid to TechCrunch, http://techcrunch.com/ (Apr. 6, 2009) ("Facebook can be downright baffling for new users.").

policy would focus on encouraging Facebook to make salient a few truly important facts about how it works, with good contextual help for the rest.

In at least one important respect, Facebook is in a better position than most product sellers. Given the fact that the products are out in the wild wreaking havoc, even the seller who learns of the dangers may not be able to do much to limit the harms–or its liability. Contrariwise, products liability law recognizes only limited duties of postsale warning[152] and recall,[153] so there is little legal pressure to make existing products safer. Facebook, however, runs a service that can be patched on the fly.[154] Facebook has used this power to ill effect with Beacon and News Feed, but when it turned off geographic networks, it instantly improved privacy for all its users.[155]

Finally, perhaps the most important lesson of product safety law is that there is no silver bullet. The field is complicated and controversial, as one might expect when the stakes can be so high. Nor has product-safety law made products fully safe. As of this writing, Toyota has recalled 9,000,000 cars to fix faulty gas pedals and brakes.[156] Tort law is a useful tool as part of a comprehensive effort but is not a solution by itself. Regulation, tort liability, consumer education, and conscientious design all play into making products physically safe; we should expect them all to play a role in making social software safe for users' privacy.[157]

---

[152] RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 10 (1998).

[153] *Id.* § 11.

[154] *See generally* Randal C. Picker, *Rewinding Sony: The Evolving Product, Phoning Home and the Duty of Ongoing Design*, 55 CASE W. RES. L. REV. 749 (2005).

[155] Story & Stone, *supra* note 32, at C1; Schmidt, *supra* note 31; Posting of Mark Zuckerberg to The Facebook Blog, *supra* note 55.

[156] *See* Micheline Maynard, *Toyota's Woes Grow as Prius Is Questioned*, N.Y. TIMES, Feb. 4, 2010, at A1.

[157] *See* Sachs, *supra* note 114, at 233-34, 237 (discussing a combination of regulatory and tort approaches to product safety and drawing inspiration for online privacy protection).

C. A Case Study: Google Buzz

To illustrate the value of the product-safety frame, consider a ripped-from-the-headlines example of privacy trouble: Google Buzz.[158] This new service from the search giant is a mash-up of e-mail, blogging, and social networking.[159] Buzz users post items such as photos, videos, random thoughts, and hyperlinks in order to share them with others.[160] These items can then be viewed and commented on by other Buzz users.[161] What differentiates Buzz from a blog is its tight integration with e-mail. Gmail users can receive Buzz updates the same way they receive regular e-mails, and reply to them too, all within Gmail.[162] Google also built social-networking features into Buzz at a deep level: choosing other users whose updates you want to follow is as easy as clicking a checkbox to let Buzz import your list of most-e-mailed contacts from Gmail.[163]

It was this last design decision that caused the privacy trouble. Google also required Buzz users to set up public profile pages–public profile pages that listed their Buzz contacts.[164] Turning on Buzz, therefore, automatically published a list of users' most-e-mailed Gmail contacts.[165] In Nicholas Carlson's words, this step "made Google Buzz a danger zone for reporters, mental health professionals, cheating spouses and anyone else who didn't want to tell the world who they emailed or chatted with most."[166] For a

---

[158] Google Buzz, http://www.google.com/buzz (last visited May 14, 2010).

[159] *See* Posting of Edward Ho to Gmail Blog, http://gmailblog.blogspot.com/ (Feb. 9, 2010, 11:00 EST) (describing Buzz).

[160] *Id.*

[161] *Id.*

[162] *Id.*

[163] Posting of Todd Jackson to Gmail Blog, http://gmailblog.blogspot.com/ (Feb. 13, 2010, 15:53 EST).

[164] *See* Nicholas Carlson, *WARNING: Google Buzz Has a Huge Privacy Flaw*, BUS. INSIDER: SILICON ALLEY INSIDER, Feb. 10, 2010, http://www.businessinsider.com/warning-google-buzz-has-a-huge-privacy-flaw-2010-2.

[165] *Id.*

[166] Nicholas Carlson, *How Google Went into "Code Red" and Saved Google Buzz*, BUS. INSIDER: SILICON ALLEY INSIDER, Feb. 16, 2010, http://www.businessinsider.com/how-google-went-into-code-red-and-saved-google-buzz-2010-2 [hereinafter Carlson, *Code Red*].

business lawyer conducting confidential negotiations or a criminal lawyer corresponding with witnesses, this kind of exposure could easily be a sanctionable violation of client confidences.[167] Others had even more to fear. As blogger Harriet Jacobs wrote:

> I use my private Gmail account to email my boyfriend and my mother.
> There's a BIG drop-off between them and my other "most frequent" contacts.
> You know who my third most frequent contact is?
> My abusive ex-husband.
>
> Which is why it's SO EXCITING, Google, that you AUTOMATICALLY allowed all my most frequent contacts access to my Reader, including all the comments I've made on Reader items, usually shared with my boyfriend, who I had NO REASON to hide my current location or workplace from, and never did.[168]

As a political analyst put it, "If I were working for the Iranian or the Chinese government, I would immediately dispatch my Internet geek squads to check on Google Buzz accounts for political activists and see if they have any connections that were previously unknown to the government."[169] Google quickly moved to turn off this feature,[170] but not before triggering both a Federal

---

[167] *See* MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2008); *see also* United States v. Monnat, 853 F. Supp. 1301, 1305 (D. Kan. 1994) (citation omitted) (discussing the identity of a client as confidential information).

[168] *See* Posting of Robin Wauters to TechCrunch, http://techcrunch.com/ (Feb. 12, 2010) (quoting Posting of Harriet Jacobs to Fugitivus, http://fugitivus.wordpress.com/ (Feb. 11, 2010) (entitled "Fuck You, Google")). In a fitting twist, the original post has been password-protected, presumably for privacy reasons. *See* Posting of Harriet Jacobs to Fugitivus, *supra*.

[169] Net Effect, http://neteffect.foreignpolicy.com/ (Feb. 11, 2010, 06:20 EST).

[170] *See* Helft, *Anger*, supra note 107.

Trade Commission (FTC) complaint[171] and a class-action lawsuit.[172]

The book on Buzz is still open, but in the mere eight days from launch to lawsuit, the debate over Buzz hit on almost every point made above as to why product safety is a useful frame for thinking about privacy-threatening social software. Buzz as a whole is a powerful, possibly revolutionary product[173]–however, it also launched with a serious design defect. Just as an otherwise useful buzzsaw is still unreasonably dangerous to life and limb if it sports a flimsy handle, the auto-add feature made the otherwise useful Buzz unreasonably dangerous to users' privacy.

In particular, Buzz was dangerous because it abused users' expectations. E-mail address books are traditionally private. By default, so is the list of blogs you read. Even Facebook, which officially treats your list of contacts as publicly available, does not by default push the complete list out to a publicly accessible webpage.[174] When Buzz made users' contact lists public, it used their information in a way that none of their previous experience had primed them to expect.

This by itself need not have been fatal. There is a first time for everything, including new forms of social software. However, Google's innovative Buzz design was poorly documented: the window asking permission to create a user profile did not explain that its "publicly viewable follower lists are made up of people you most frequently email and chat with."[175] Nor did Google clearly explain how to undo the move once users realized what happened.[176] Instead, it fell to bloggers to create their own guides to disabling Buzz, adding increasingly detailed instructions as they

---

[171] Complaint, Request for Investigation, Injunction, and Other Relief at 1, *In re* Google, Inc., F.T.C. (Feb. 16, 2010), *available at* http://epic.org/privacy/ftc/googlebuzz/GoogleBuzz_Complaint.pdf.

[172] *See generally* Class Action Complaint, Hibnick v. Google, Inc., No. 5:10-cv-00672-JW (N.D. Cal. Feb. 17, 2010), *available at* http://docs.justia.com/cases/federa/district-courts/california/candce/5:2010cv00672/224341/1/.

[173] *See, e.g.*, Posting of Tim O'Reilly to O'Reilly Radar, http://radar.oreilly.com/ (Feb. 9, 2010, 11:00 EST).

[174] *See* Privacy Policy, *supra* note 106.

[175] Carlson, *supra* note 164.

[176] *See* Jessica Dolcourt, *Buzz Off: Disabling Google Buzz*, CNET, Feb. 11, 2010, http://news.cnet.com/8301-17939_109-10451703-2.html.

painstakingly reconstructed how Buzz worked.[177] In product-safety terms, Google failed to supply Buzz with sufficient instructions and warnings. Even if opening up your list of contacts to the world was a user mistake, it was an eminently foreseeable mistake that Google should have expected and guarded against.[178]

What is more, Google had reasonable alternative designs available to it. The first change Google made to Buzz was to add an explicit checkbox to the sign-up process, allowing users to show or hide their lists of contacts on their profile.[179] This checkbox could have been present all along; it was clearly achievable and imposed few costs on Buzz's utility.[180] Ultimately, Google disabled the auto-add feature entirely, merely providing suggestions of other users to follow.[181] At the same time, Google made Buzz easier to disable entirely.[182] In addition to demonstrating the existence of feasible but less dangerous designs, this rapid response also illustrates the importance of being able to patch a software service on the fly.[183] Whether and to what extent Google ought to be held liable in the pending FTC complaint and lawsuit are more difficult questions–but the power of the product-safety approach in cutting straight to the essentials of the Buzz story should be clear.

IV. CONCLUSION

I am not calling for the direct application of products liability law to online privacy. For one thing, some doctrines of products-liability law, taken at face value, would bar its application to privacy harms altogether. For example, products liability tort suits

---

[177] *See, e.g.*, Dolcourt, *supra* note 176.

[178] *See, e.g.*, Raw Meat, http://qblog.aaronsw.com/post/400531264/heres-to-the-crazy-ones (Feb. 20, 2010) ("Buzz is a clear example that testing on Google employees just isn't enough.")

[179] *See* Nicholas Carlson, *Google Buzz Still Has Major Privacy Flaw*, BUS. INSIDER: SILICON ALLEY INSIDER, Feb. 12, 2010, http://www.businessinsider.com/googles-nice-improvements-to-buzz-dont-correct-major-privacy-flaw-2010-2.

[180] *See id.*

[181] Posting of Todd Jackson to Gmail Blog, *supra* note 163.

[182] *See id.*

[183] *See* Carlson, *Code Red*, *supra* note 166.

do not compensate plaintiffs for economic loss and other nonphysical injuries[184] and are limited to defective "products."[185] These doctrines serve important gatekeeping functions within product liability law itself, and blithely discarding them is likely to do violence both to products liability and to privacy law.[186] Moreover, products-liability law has its own doctrinal problems, such as the confused split of authority between risk-utility balancing and consumer expectations as the test for whether a design is defective.[187] There is no good reason to import the full details of these doctrines, warts and all, into privacy law.

Instead, I am suggesting a process of thoughtful conversation and translation between two bodies of law that have a common history and more in common than scholars and lawyers sometimes realize. Products-liability law may not hold all of the answers to privacy law, but it does ask the right kind of questions to help make sense of the confusing world of online social privacy. In the words of the reporters of *Restatement (Third) of Torts: Products Liability*,[188] "[t]here are no easy answers — only good questions."[189]

---

[184] RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 21 (1998); *see also* Scott, *supra* note 134, at 453-56, 470-71 (discussing the economic loss rule and then applying it to products liability).

[185] RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 19 (1998) (defining products); *see also* Scott, *supra* note 134, at 461-67 (discussing definition of software as a "product").

[186] *See, e.g.*, Wilson v. Midway Games, Inc., 198 F. Supp. 2d 167, 169 (D. Conn. 2002) (holding that "Mortal Kombat" is not a " 'product' " with respect to information it contains, when the game was allegedly responsible for inducing one adolescent to believe he was a game character and to fatally stab another). Drop the "products" part of "products liability" without careful thought as to what will replace it and those who make and sell computer software will face forms of liability that raise serious First Amendment concerns. *See, e.g.*, *id.* at 178-82 (discussing U.S. CONST. amend. I) (describing the First Amendment's protection of video games).

[187] OWEN, *supra* note 129, §§ 5.6-.7.

[188] *See* RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. (1998) (reported by James A. Henderson, Jr. and Aaron D. Twerski).

[189] JAMES A. HENDERSON, JR. & AARON D. TWERSKI, PRODUCTS LIABILITY: PROBLEMS AND PROCESS, at xxi (6th ed. 2008).