Loyola Consumer Law Review

Volume 29 | Issue 1 Article 6

2016

Manipulating Trust on Facebook

Ari Ezra Waldman

Recommended Citation
Ari E. Waldman *Manipulating Trust on Facebook*, 29 Loy. Consumer L. Rev. 175 (2017).
Available at: https://lawecommons.luc.edu/lclr/vol29/iss1/6

MANIPULATING TRUST ON FACEBOOK

Ari Ezra Waldman[1]

INTRODUCTION

Between 2005 and 2011, both total sharing and privacy-seeking behavior on Facebook increased.[2] That means that Facebook users were sharing a lot of personal information even as they were changing their privacy settings to ostensibly make their data more secure. It seems counterintuitive: if we are concerned that Facebook does not protect our privacy, we should share less, not more. This is a particularly jarring contradiction given that Facebook's voracious appetite for data is not sated by the information we actively submit; it also sweeps in data from our clicks, third-party apps, and our interactions with its partners and advertisers. But Facebook users do not make perfectly

[1] Associate Professor of Law and Director, Innovation Center for Law and Technology, New York Law School. Affiliate Scholar, Princeton University, Center for Information Technology Policy. Ph.D., Columbia University; J.D., Harvard Law School. A version of this essay was presented at the Loyola University Chicago School of Law Consumer Law Review symposium, "Advertising in Digital Media: Disclosures and Transparency in Social Media." A variation on this essay is derived from a more in depth look into the connection between trust and privacy, *Privacy, Sharing, and Trust: The Facebook Study*, forthcoming in the Case Western Reserve Law Review. Thank you to all conference participants for their questions, comments, and important feedback. In particular, I would like to thank Angela Campbell, Deborah Gerhardt, Matthew Sag, and Ari Scharg. Special thanks to Jonathan Frankle, Staff Technologist at the Center on Privacy and Technology at the Georgetown University Law Center, for selflessly and eagerly sharing his knowledge and expertise with me. All errors, however, are my own, and I trust you will forgive me for them.

[2] Fred Stuntzman, Ralph Gross, & Alessandro Acquisti, *Silent Listeners: The Evolution of Privacy and Disclosure on Facebook*, 2 J. PRIVACY & CONFIDENTIALITY 7, 8-9 (2012).

rational sharing decisions. As James Grimmelmann has argued, Facebook is designed to nudge us to share. It is a social platform that "scratch[es] its users' social itches."[3] This may explain the paradox: we make social sharing decisions for social reasons, egged on by design strategies deployed to encourage us to share.

To Grimmelmann, Facebook is like a carmaker. When Alex does silly, stupid, or dangerous things with his otherwise functionally-sound Accord, we don't usually blame Honda for the damage Alex causes. We blame Alex. Similarly, Facebook isn't "hijack[ing]" our privacy away from us, Grimmelmann notes. Rather, it "offer[s] its users a flexible, valuable, socially compelling tool." Its users are the ones making decisions that put their privacy at risk.[4]

Grimmelmann is right, to a point. This essay argues that Facebook encourages us to share personal information by designing its platform to cue trust among its members. Trust, a resource of social capital between or among two or more persons concerning the expectation that others will behave according to accepted social norms, is at the core of how and why we decide to share personal information in the first place.[5] It also pervades Facebook design. And we use proxies for trust to assess the risk of sharing in a given social situation.[6] Sometimes, those proxies are inadequate if we want to protect our privacy online.

[3] James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1151 (2009).

[4] *Id.* at 1140.

[5] *See* Ari Ezra Waldman, *Privacy As Trust: Sharing Personal Information in a Networked World*, 69 U. MIAMI L. REV. 559 (2015) (arguing that privacy law should be focused on protecting relationships of trust); Ari Ezra Waldman, *Privacy, Sharing, and Trust*, 67 CASE W. RES. L. REV. __ (forthcoming 2017), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2726929 (providing quantitative evidence from a survey of Facebook users that trust is an important factor in our decisions to share personal information on online social networks).

[6] *See* Waldman, *Privacy, Sharing, and Trust*, *supra* note 5. In *Saving Facebook*, Grimmelmann used the word "trust" several times. However, he stopped short of using trust as an umbrella conceptualization of privacy.

That isn't Facebook's fault, Grimmelmann argues correctly. But Facebook also uses design tactics that leverage the trust we have in our friends to manipulate us into sharing personal information with websites, advertisers, and third party partners we've never met or heard of. When it does, Facebook crosses the line from carmaker into carjacker, from a conduit of social sharing to a manipulative for-profit scheme where users are reduced to the terabytes of data they generate.

This essay proceeds in three parts. Part I discusses how Facebook collects information. Part II defines trust and shows how it is an important factor in our decision to share. The balance of this section describes how some elements of Facebook's design that nudge us to share are all based on trust. This section explicitly builds on Grimmelmann's argument in his article, *Saving Facebook*,[7] reinterpreting his analysis in light of the relationship between privacy and trust. Part III describes several examples of when Facebook's use of trust steps over the line from dynamic social space into unfair and manipulative tool. This section concludes with design and policy recommendations to protect privacy on Facebook and other social networks.

I. SHARING ON FACEBOOK

Facebook is an online social network. A network is just a set of objects[8]—people, cells, power plants—with connections among them—social encounters, synapses, grids. They are all around us: a family is a (social) network, as is the (neural) network in a brain and the (distribution) network of trash pick-up routes in New York City.[9] Facebook is the paradigmatic modern

[7] *See* Grimmelmann, *supra* note 3.

[8] DUNCAN J. WATTS, SIX DEGREES: THE SCIENCE OF A CONNECTED AGE 27 (2003).

[9] Network structure is diverse. A simple search of "network visualization" in Google Images shows the wide range of visual representations of networks. *See* https://www.google.com/search?q=network+visualization&espv=2&biw=1680&bih=881&source=lnms&tbm=isch&sa=X&ved=0CAYQ_AUoAWoVChMIyLeWnPrYxgIVTFU-Ch0clg3n.

online social network: it has nearly 1.65 billion nodes (members),[10] but it also has billions of subnetworks, where nodes overlap, interact, and share information. It is the network's ability to invite, disseminate, and retain information that concerns us.

danah boyd and Nicole Ellison argue that social network sites offer three common elements: profiles, contacts, and community.[11] Public profiles allow network members to craft their identities and, as Erving Goffman argued, to manage how others in the network perceive them.[12] Contacts allow users to interact with others and create overlapping communities that form part of their identities. These three elements are part of what make Facebook and Instagram so compelling: they allow us to show our best side, even if reality is far more complicated;[13] they allow us to deepen or extend our connections with others, even when we're far apart;[14] and they allow us to become part of something bigger than ourselves.[15]

Achieving these social goals requires information. A lot of it. We hand some of that data over to Facebook directly. To sign up for an account, for example, we have to provide our names, email addresses or mobile numbers,[16] dates of birth, and

[10] Facebook Stats, at http://newsroom.fb.com/company-info/ (last visited June 22, 2016) (referring to monthly active users).

[11] danah m. boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. COMPUTER-MEDIATED COMM. 210, 211 (2008). Ms. boyd prefers not to capitalize her name. *See* http://www.danah.org/name.html (last visited June 22, 2016).

[12] *See* ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE 2-5 (1959).

[13] *See* Jessica Winter, *Selfie-Loathing*, SLATE (July 23, 2013, 12:27 PM), http://www.slate.com/articles/technology/technology/2013/07/instagram_and_self_esteem_why_the_photo_sharing_network_is_even_more_depressing.html.

[14] *Facebook Helps Promote Long Distance Relationships*, TELEGRAPH (July 17, 2008, 10:55 AM), http://www.telegraph.co.uk/news/uknews/2420501/Facebook-helps-promote-long-distance-relationships.html.

[15] Causes on Facebook, https://apps.facebook.com/causes/ (last visited June 22, 2016).

[16] If you do not provide your mobile number upon registration,

genders. After that, we are asked to allow Facebook to mine our email contacts so we can see which of our friends are already members and which we can invite to join.[17] These contacts will constitute the core of our network, aptly called "friends." Then we can get started filling out our profiles by uploading a picture and a "cover" photo that sits at the top of our profile page. If we can't think of anything to post, Facebook is there with a helpful nudge: "Select a photo to appear at the top of your profile. It could be from a recent trip or something you're proud of." Goffman would be proud. Facebook is designed to make image management easy.

Adding a profile photo, Facebook reminds us, is the best way for other people to know who we are. Facebook's design lets us easily drop in employment, education, and professional information, as well as location data (past and present), contact information, a personal website URL, what gender of person we're interested in meeting, the languages we speak, our political and religious views, our relationship status, family members, and even how to pronounce our names (Ari is pronounced like the two letters "R" and "E", or AH-ree). Life events—birth, graduation, marriage, braces removed, or that memorable trip to Florence—come next. We can add sports teams that we support, music that we enjoy, movies and television shows that we watch, books that we have read, and athletes, celebrities, and even restaurants that we like.[18]

Once our profile is ready and we are active on the platform, data sharing only increases. We can upload photos of ourselves and others and "tag" them, or

Facebook will frequently remind you to provide it to "make your account more secure." *See* Help Center, Why am I being asked to add my phone number to my account?, https://www.facebook.com/help/1137953062904148 (last visited June 22, 2016).

[17] Step 1, Find Your Friends, https://www.facebook.com/gettingstarted/?step=contact_importer (last visited June 22, 2016).

[18] This summary—and it is only a summary—is based on the Author going through the steps necessary to create a Facebook account from scratch.

identify them with a link to their profile.[19] Sometimes, users have to consent before someone else can tag them, but even if they decline, their unlinked name still appears on the photo or in its caption. We can send direct "Messages" to others or "Poke" someone to flirt.[20] We can play any of the multitude of apps and games on the Facebook platform.[21] We can post comments to a friend's "timeline" or tag them in posts on our own.[22] We can also tag a location for those posts, so the Facebook universe knows where we are.[23] And unless we change certain settings, most of those posts will appear in a "Newsfeed," the running list of stories, interactions, and contributions that we see when we log in.[24] We can then comment on these posts, share them with our own network, share them on another network like Twitter, and "react" to the post with one of five

[19] How Tagging Works, https://www.facebook.com/about/tagging (last visited June 22, 2016).

[20] *See* Jackie Cohen, *5 Rules of Facebook Flirting*, SOCIAL TIMES (Apr. 14, 2009, 11:11 AM), http://www.adweek.com/socialtimes/facebook-flirting/308415 (last visited June 22, 2016) ("A girlfriend recently asked me to explain the concept of 'poking' on Facebook. I told her that it meant that someone is flirting with her, of course. I mean, isn't it obvious? Back in second grade, the boys would chase us around the room, grab, hit and poke us until we giggled so hard we had 'accidents'. Or was that just me?").

[21] *See, e.g.*, Farmville, https://www.facebook.com/FarmVille/ (last visited June 22, 2016). *But see* Saqib Khan, *How to Block Annoying Game Requests from Your Facebook Friends*, VALUE WALK (Mar. 4, 2013, 3:17 PM), http://www.valuewalk.com/2014/03/block-game-requests-on-facebook/.

[22] What is Timeline, https://www.facebook.com/help/1462219934017791 (last visited June 22, 2016).

[23] According to some sources, there are 17 billion location-tagged posts per day on Facebook. *See* Kevin Ho, *41 Up-to-Date Facebook Facts and Stats*, WISHPOND (2014), http://blog.wishpond.com/post/115675435109/40-up-to-date-facebook-facts-and-stats.

[24] How Newsfeed Works, https://www.facebook.com/help/327131014036297/ (last visited June 22, 2016).

reactions: Love, Laugh, Wow, Sad, Angry, and, of course, Like.[25]

The Facebook "Like" button, a right-handed, white thumbs up on the Facebook blue background,[26] may be the greatest source of information that Facebook collects. According to some sources, there have been a total of 1.13 trillion "likes" since Facebook started in 2004. Today, there are approximately 4.5 billion "likes" per day and 3.1 million per minute.[27] As we "like" our friends' posts, pictures, and comments, we are doing two things: first, we are engaging in image and reputation management by showing our Facebook networks what interests and engages us;[28] second, we are rounding out an already reasonably rich picture of ourselves for Facebook. If we "like" several posts about the Democratic candidate for President alongside posts about the need to reduce our carbon footprint, increase infrastructure spending, and fight against discrimination, Facebook has a pretty good idea about the kinds of candidates and causes we will support. It could, then, use that data to influence us.[29]

The "Like" button also crosses the divide between information that we voluntarily hand over to Facebook and data that the platform collects from tracking us online. To understand how Facebook's "Like" button helps it gather information about us, we need a brief primer on data tracking.[30]

[25] Reactions Now Available Globally, http://newsroom.fb.com/news/2016/02/reactions-now-available-globally/ (last visited June 22, 2016).

[26] *See* Leo Widrich, *Why Is Facebook Blue? The Science Behind Colors in Marketing*, FAST COMPANY (May 6, 2013, 6:02 AM), http://www.fastcompany.com/3009317/why-is-facebook-blue-the-science-behind-colors-in-marketing.

[27] *See* Ho, *supra* note 23.

[28] *See* Veikko Eranti & Markku Lonkila, *The Social Significance of the Facebook Like Button*, FIRST MONDAY (June 2015), http://firstmonday.org/ojs/index.php/fm/article/view/5505/4581#3a.

[29] *See* Robinson Meyer, *How Facebook Could Tilt the Election*, THE ATLANTIC (Apr. 18, 2016), http://www.theatlantic.com/technology/archive/2016/04/how-facebook-could-tilt-the-2016-election-donald-trump/478764/.

[30] Much of the following discussion is based on Franziska

Websites need to remember us as we travel around the web. To do this, they leave cookies, or tiny files, on our computers that allow websites to identify who is visiting their platform and what they did there. Cookies, then, are the internet's tags. Thanks to Amazon's cookie, for example, I can put a plush Judy Hopps (from the Disney movie, *Zootopia*)[31] in my Cart, close the window, and have the item back in my Cart when I visit Amazon days later. The cookie Amazon put on my computer, tagged uniquely to identify me, helps create this seamless, convenient, and tailored internet experience.[32]

It is also central to information flows and tracking. Consider the New York Times website, www.nytimes.com, which runs several ads on its homepage. When I visited that site for this essay, some of the ads I saw were from Penguin Random House, the Hillary Clinton Victory Fund, Indochino, 11 Beach ("luxury condominiums detailed for Tribeca"), the New York Times itself, EMC (a computer storage company), and Southwest Airlines.[33] When a friend with different interests and different web histories visits the site, she might see different ads. These ads sit within "iframes," or pages within the main nytimes.com page.[34] It has to

Roesner, Tadayoshi Kohno, & David Wetherall, *Detecting and Defending Against Third-Party Tracking on the Web*, 9TH USENIX SYMPOSIUM ON NETWORKED SYSTEMS DESIGN AND IMPLEMENTATION (2012), https://www.usenix.org/system/files/conference/nsdi12/nsdi12-final17.pdf, and on email conversations with Jonathan Frankle, Staff Technologist at the Center for Privacy and Technology at Georgetown University Law Center. Notably, none of this is explained in Facebook's Data Policy. *See* Data Policy, https://www.facebook.com/policy.php (last visited June 23, 2016).

[31] It's adorable. *See* https://www.amazon.com/Zootopia-Large-Plush-Office-Hopps/dp/B016LBYL42/ref=sr_1_4?s=toys-and-games&ie=UTF8&qid=1466705009&sr=1-4&keywords=judy+hopps+plush.

[32] Roesner, Kohno, & Wetherall, *supra* note 30, at 2.

[33] *See* NEW YORK TIMES, http://www.nytimes.com/ (last visited June 23, 2016).

[34] Roesner, Kohno, & Wetherall, *supra* note 30, at 2. *See also* E-mail from Jonathan Frankle, Staff Technologist, Center for Privacy and Technology, Georgetown University Law Center (June 23,

be this way. Otherwise, the code behind the advertisements would have to be mixed with the code of the nytimes.com. That could erode the security surrounding the data nytimes.com keeps about its users. As a page within a page, these ads also drop cookies onto our computers, allowing them to tag and track us wherever we go, like tagging and tracking released endangered animals.[35] This explains why similar advertisements from the same company tend to follow us around the web, and why different users see different ads on the same website.

"Like" buttons operate in a similar way. Many websites have an embedded "Like" button that begs us to "Like Us on Facebook" with a simple click.[36] When we visit these pages, Facebook may receive a significant amount of information, including the amount of time we spend on the page, what we clicked on, and the browser and operating system we use, to name just a few. What's more, since 2012, Facebook has been collecting data about our internet behavior even from websites that do not have a "Like" button.[37] And Facebook channels that information into user-targeted advertisements.[38] When we "like" a post by JCrew or ask our networks for advice on where to get a reasonably priced, yet modern suit for work, JCrew advertisements start popping up on Facebook and everywhere else we go online. It makes sense, then, that Facebook has

2016, 8:27 AM) (on file with author).

[35] *See* Rebecca Boyle, *It's Incredible We Knew About Cecil the Lion At All*, POPULAR MECHANICS (July 29, 2015), http://www.popularmechanics.com/science/animals/news/a16665/tracking-cecil-lion/.

[36] Any developer can visit https://developers.facebook.com/docs/plugins/like-button to get the code for the "Like" button and drop it onto their page.

[37] Tom Simonite, *What Facebook Knows*, MIT TECHNOLOGY REVIEW (June 12, 2012), https://www.technologyreview.com/s/428150/what-facebook-knows/.

[38] Tom Simonite, *Facebook's Like Buttons Will Soon Track Your Web Browsing to Target Ads*, MIT TECHNOLOGY REVIEW (Sept. 16, 2015), https://www.technologyreview.com/s/541351/facebooks-like-buttons-will-soon-track-your-web-browsing-to-target-ads/.

collected more than 300 petabytes of data on us.[39] It is truly a data behemoth.

II. TRUST AND SHARING ON FACEBOOK

Those petabytes of data are outrageously profitable. In just the first quarter of 2016, Facebook earned $5.2 billion in advertising revenue.[40] That puts it on pace to far eclipse the $17.1 billion it collected in all of 2015.[41] Some estimates expect that number to jump to nearly $27 billion by 2017.[42] Facebook earns this money by selling advertisements, and it can charge hefty sums for those ads because its petabytes of data allow it to target us for products and services it knows we want. Those of us who have told Facebook that we're gay—perhaps by saying what gender we're "interested in," listing a significant other of the same gender, or using LGBT keywords in our posts—and love to travel

[39] *See* Ho, *supra* note 23. A petabyte's size is difficult to conceive. If I told you that a petabyte is one quadrillion bytes, that would still be pretty inscrutable. Put it this way: together, all United States academic libraries hold just 2 petabytes of data. Therefore, Facebook has about 150 times more data than every academic library in the United States. Julian Bunn, *How Big is a Petabyte, Exabyte, Zettabyte, or a Yottabyte*, High Scalability (Sept. 11, 2012, 9:15 AM), http://highscalability.com/blog/2012/9/11/how-big-is-a-petabyte-exabyte-zettabyte-or-a-yottabyte.html.

[40] Deepa Seetharaman, *Facebook Revenue Soars on Ad Growth*, WALL ST. J. (Apr. 28, 2016, 12:59 AM), http://www.wsj.com/articles/facebook-revenue-soars-on-ad-growth-1461787856.

[41] Tim Peterson, *Facebook's Ad Volume Has Grown for the First Time in Two Years*, ADVERTISING AGE (Jan. 27, 2016), http://adage.com/article/digital/facebook-q4-2016-earnings/302378/.

[42] *Social Network Ad Revenues Accelerate Worldwide*, eMARKETER (Sept. 23, 2015), http://www.emarketer.com/Article/Social-Network-Ad-Revenues-Accelerate-Worldwide/1013015. To put that in perspective, Facebook's $27 billion is larger than the GDP of 90 countries, according to the International Monetary Fund. *See* WORLD ECONOMIC OUTLOOK DATABASE, INT'L MONETARY FUND (2016), http://www.imf.org/external/pubs/ft/weo/2016/01/weodata/index.aspx.

may see advertisements from Atlantis Cruises or gay-friendly hotels and tourist destinations. Those who live in San Francisco, earned an advanced degree, "liked" a post supporting the DREAM Act,[43] and have visited *The Atlantic*'s website are more likely to see ads from *The New Yorker* or from the Democratic National Campaign Committee[44] than someone who "likes" Ted Nugent.[45] Therefore, Facebook has a strong financial interest in not only what we share, but in encouraging us to share as much personal information as possible:[46] the more data it has, the better it can target its ads, and the more revenue it can earn.

[43] The DREAM Act would give certain undocumented immigrants living in the United States a path to citizenship. It is overwhelmingly supported by progressives and overwhelmingly opposed by conservatives. *See* Brian Naylor, *Democrats Push DREAM Act; Critics Call It Amnesty*, NPR (Dec. 6, 2010, 12:01 AM), http://www.npr.org/2010/12/06/131796206/democrats-push-dream-act-critics-call-it-amnesty.

[44] *See, e.g.*, *A Deep Dive Into Party Affiliation*, PEW RESEARCH CENTER (Apr. 7, 2015), http://www.people-press.org/files/2015/04/4-7-2015-Party-ID-release.pdf.

[45] Ted Nugent is a rather vocal, and often controversial, conservative. *See, e.g.*, Tal Kopan, *Nugent Likens ACA to Nazi Germany*, POLITICO (Feb. 24, 2014, 3:36 PM), http://www.politico.com/story/2014/02/ted-nugent-affordable-care-act-obamacare-nazi-germany-103863.

[46] Not everything we share is so personal. Recently, I shared my displeasure with the creaky C train, a local subway that runs on Manhattan's West Side and is plagued by delays. *See* Nathan Tempey, *The Best & Worst Subway Lines in NYC, Ranked*, GOTHAMIST (Sept. 17, 2015, 3:42 PM), http://gothamist.com/2015/09/17/mta_subway_report_card.php. And we know, for example, that many people go on Facebook to share news. *See* Martha Barthel et al., *The Evolving Role of News on Twitter and Facebook*, PEW RESEARCH CENTER (July 14, 2015), http://www.journalism.org/files/2015/07/Twitter-and-News-Survey-Report-FINAL2.pdf. But much of the information we do share—sexual orientation and religious affiliation, for example—have been legally protected from disclosure. *See* Exec. No. 13672, 41 C.F.R. §§ 60-1, 60-2, 60-4, 60-50 (prohibiting federal contractors from discriminating on the basis of sexual orientation and gender identity); 42 U.S.C. §§ 3601-3609 (known as the Fair Housing Act, which prohibits discrimination on the basis of race, color, religion, sex, or national origin).

None of this is inherently bad. Behavioral targeting may be creepy[47] and perhaps even discriminatory,[48] but there are streamlining, efficiency, and relevance benefits to the user. For the purposes of this essay, however, I am more interested in how targeting works rather than its effects. My descriptive argument is that Facebook nudges us to share by leveraging the trust we have in our friends. As I have argued elsewhere, we share when we trust, and we use myriad social cues to identify contexts of trust.[49] Some of these cues, as James Grimmelmann has argued, do not always work effectively on online social networks.[50] But trust nevertheless forms the basis for our decisions to share. Facebook knows this; its platform is designed for it.

A. *What is Trust?*

Trust is a resource of social capital between or among two or more parties concerning the expectations that others will behave according to accepted norms.[51] It is the "favorable expectation regarding . . . the actions and intentions of others,"[52] or the belief that others will

[47] *See* Evan Selinger, *Why Do We Love To Call New Technologies "Creepy"?*, SLATE (Aug. 22, 2012, 3:30 AM), http://www.slate.com/articles/technology/future_tense/2012/08/facial_recognition_software_targeted_advertising_we_love_to_call_new_technologies_creepy_.html.

[48] Amit Datta, Michael Carl Tschantz, & Anupam Datta, *Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice, and Discrimination*, 2015 PROCEEDINGS ON PRIVACY ENHANCING TECHNOLOGIES 92 (2015), http://www.degruyter.com/view/j/popets.2015.1.issue-1/popets-2015-0007/popets-2015-0007.xml.

[49] *See* Waldman, *Privacy As Trust*, *supra* note 5; Waldman, *Privacy, Sharing, and Trust*, *supra* note 5.

[50] Grimmelmann, *supra* note 3.

[51] Alejandro Portes & Julia Sensenbrenner, *Embeddedness and Immigration: Notes on the Social Determinants of Economic Action*, 98 AM. J. SOC. 1320, 1332 (1993).

[52] J. David Lewis and Andrew Weigert, *Trust as Social Reality*, 62 SOCIAL FORCES 967, 968 (1985). *See also* Ken Newton and Sonja Zmerli, *Three Forms of Trust and Their Association*, 3 EUR. POL. SCI. REV. 169, 171 (2011); Guido Möllering, *The Nature of Trust: From*

behave in a predictable manner. For example, if I ask a friend to hold my spare set of keys, I trust she will not break in and steal from me. When an individual speaks with relative strangers in a support group like Alcoholics Anonymous, she trusts that they will not divulge her secrets. Trust, therefore, includes a willingness to accept some risk and vulnerability toward others and steps in to grease the wheels of social activity.[53] I cannot know for certain that my neighbor will not abuse her key privileges or that my fellow support group members will keep my confidences, so trust allows me to interact with and rely on them. And I earn all sorts of positive rewards as a result.[54] If I never trusted, my social life would be paralyzed. As Niklas Luhmann stated, trust exists where knowledge ends.[55] It is the mutual "faithfulness" on which all social interaction depends.[56]

Lawyers should be familiar with this kind of trust. It is, after all, at the core of the general notion of confidentiality and the more specific doctrines of privilege.[57] As Neil Richards and Woodrow Hartzog have noted, "perhaps the most basic assumption people make when disclosing personal information," whether

Georg Simmel to a Theory of Expectation, Interpretation and Suspension, 35 SOCIOLOGY 403, 404 (2001).

[53] NIKLAS LUHMANN, TRUST AND POWER 4 (1979).

[54] Trust helps us deal with uncertainty and complexity by allowing us rely on the recommendations of others. *See* TALCOTT PARSONS, ACTION THEORY AND THE HUMAN CONDITION 45-47 (1978). Plus, it encourages therapeutic sharing by giving all individuals, from alcoholics and those suffering from depression to close friends, the confidence they need to disclose personal and perhaps stigmatizing information. *See, e.g.*, ANTON T. BECK & BRAD A. ALFORD, DEPRESSION: CAUSES AND TREATMENT 292-324 (2009).

[55] *Id.* at 32-38. *See also* Patricia M. Doney, Joseph P. Cannon, & Michael R. Mullen, *Understanding the Influence of National Culture on the Development of Trust*, 23 ACADEMY OF MGMT. REV. 601, 603 (1998).

[56] GEORG SIMMEL, THE PHILOSOPHY OF MONEY 379 (1978).

[57] Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, __ STANFORD TECH. L. REV. __, at 37-41 (forthcoming 2016), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2655719 (connecting confidentiality and trust).

to doctors, lovers, or ISPs, "is that the recipient will be discreet."[58] They note that we trust doctors "not to reveal information about our health and mental state" and trust lovers "not to kiss and tell."[59] Richards' and Hartzog's formulation of discretion, therefore, is based on trust, or the expectation that individuals will continue to behave according to accepted social norms. We expect doctors to keep our medical confidences and our lovers to keep our sexual confidences because doing so conforms to presiding norms. And, according to several studies, we are deeply concerned that information we share with one website may be shared with third parties.[60] Perhaps this concern stems from our inability, and lack of opportunity, to determine for ourselves whether we trust those third parties.

B. Trust and Facebook's Design

Yet, we continue to disclose information on Facebook knowing that it is collecting, analyzing, sharing, and making money off of our data. We do that, I argue, because Facebook is designed with trust in mind, nudging us to disclose. In his article, *Saving Facebook*, Grimmelmann noticed this, but not in so many words. He suggested that "Facebook systematically delivers signals suggesting an intimate, confidential, and safe setting."[61] In that context, Grimmelmann argued, we rely on potentially incomplete heuristics about privacy risks to determine when to share our information.[62] I will discuss several of those heuristics here. I will then show how each of them is both bound up with the concept of trust and activated by Facebook's design, encouraging us to share our information.

Bigness. Grimmelmann suggests that Facebook's

[58] *Id.* at 38.

[59] *Id.*

[60] Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, at 3, 29, PEW RESEARCH CENTER (Nov. 12, 2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf.

[61] Grimmelmann, *supra* note 3, at 1160.

[62] *Id.* at 1161.

size makes it seem safe in three ways.[63] First, there is a herding effect: we tend to adapt our behavior to conform to those around us and infer that because other people are doing something, we should be doing it, as well.[64] Bigness also reduces risk for the same reason. As Andrea Devenow and Ivo Welch have shown in the economic context, the risk to one among millions is far smaller than the risk to one among ten.[65] And bigness allows us to rely on the "wisdom of crowds," or the idea that groups aggregate information and can, as a result, make better decisions than any one member.[66] As Grimmelman notes, 1.65 billion Facebook users sharing all the time cannot all be wrong about the relative safety of the platform.[67]

Herding and the wisdom of crowds are essentially about trust. Facebook's size and growth make it more predictable as a safe place for sharing. We see massive crowds posting information, and rarely, if ever, hear about anything going wrong. And Facebook is designed to emphasize its bigness. Step 1 after signing up lets us mine our email contacts to see which of our friends are already members and which we can invite, thus making the community bigger. Whenever another member sends us a "friend request," or a request to be added to our network, Facebook lists her network size and the number of mutual friends we have in common. And it includes the number of people who have "liked" or

[63] *Id.*

[64] *See* CHRISTINA BICCHIERI, THE GRAMMAR OF SOCIETY: THE NATURE AND DYNAMICS OF SOCIAL NORMS 216-17 (2006). *See also* Erin L. Krupka & Roberto A. Weber, *Identifying Social Norms Using Coordination Games: Why Does Dictator Game Sharing Vary?*, Research Showcase @ Carnegie Melon University Working Paper, *available at* http://repository.cmu.edu/cgi/viewcontent.cgi?article=1096&context=sds.

[65] *See* Andrea Devenow & Ivo Welch, *Rational Herding in Financial Economics*, 30 EURO. ECON. REV. 603, 604 (1996).

[66] *See* JAMES SUROWICKI, THE WISDOM OF CROWDS (2004) (*cited in* Grimmelmann, *supra* note 3, at 1161).

[67] Grimmelmann said "50 million," but he published his article in 2009, when there were far fewer Facebook users than there are today. That means that Facebook is 33 times bigger in June, 2016, than it was in 2009.

commented on a post above and below the content on our Newsfeeds. And, of course, Facebook brags about its size all the time.[68] It does so because platforms that are big are more trustworthy.

Community. Grimmelmann notes that we tend to share private things only when the right people are listening in.[69] The "right" people are, of course, the ones we trust to behave with discretion and confidentiality toward our information. And Facebook does a good job making us think that only trustworthy people are around. In the aggregate, our networks tend to look like us: we often agree on politics, have similar backgrounds, and enjoy some of the same hobbies. It creates an echo chamber of sorts, as Cass Sunstein noted.[70] But it also creates a feeling of familiarity, something that Max Weber and Talcott Parsons argued was essential to building trust.[71] Facebook is also designed to create community on an individual level: Members' pictures pop up when we hover our cursor over their names, attempting to simulate the closeness we feel when we look someone in the eye in the physical world.[72] And yet we never see any evidence of Facebook

[68] And size matters when it comes to ad revenue on the web. *See, e.g.*, Jim Edwards, *In Just 2 Years, Google and Facebook Have Control to Control 75% of All Mobile Advertising*, BUSINESS INSIDER (Mar. 20, 2014, 5:29 PM), http://www.businessinsider.com/google-and-facebook-dominate-mobile-advertising-2014-3.

[69] Grimmelmann, *supra* note 3, at 1162.

[70] *See* CASS SUNSTEIN, REPUBLIC.COM 2.0 (2009).

[71] *See* Max Weber, *The Protestant Sects and the Spirit of Capitalism*, in FROM MAX WEBER: ESSAYS IN SOCIOLOGY 302, 312 (H. H. Gerth & C. Wright Mills eds., 1946) (arguing that common membership in the Protestant sect in early America allowed people who did not really know each other to trust that they would be competent contractual partners); TALCOTT PARSONS, ACTION THEORY AND THE HUMAN CONDITION 47 (1978) ("People defined as sharing one's values or concrete goals and in whose competence and integrity one has 'confidence' come to be thought of as 'trustworthy individuals' or 'types.'").

[72] *See, e.g.*, Michael Argyle & Janet Dean, *Eye Contact, Distance, and Affiliation*, 28 SOCIOMETRY 289, 289-99 (1965) (presenting evidence that eye contact is an expression of intimacy). There is a Seinfeld episode about this very concept. Kramer wants to create a better society in his and Jerry's Manhattan apartment building, so

listening in. Our Newsfeeds, like our lists of friends, prioritize our closest friends, or those with whom we have had more online interactions. Facebook lets us join Causes and helps us get invited to friends' housewarming and holiday parties. This has the effect of making the platform seem like a friendly, welcoming, and trustworthy community in which it safe to share.

Discretion. In the physical world, we tend to share information along with cues for our audience on how to deal with it. We lean in, speak in hushed voices, and turn away from a crowd to indicate confidentiality. Grimmelmann called this the "I know how much this means to you" cue.[73] Richards and Hartzog called this "discretion," noting that "perhaps the most basic assumption people make when disclosing personal information," whether to doctors, lovers, or ISPs, "is that the recipient will be discreet."[74] They note that we trust doctors "not to reveal information about our health and mental state" and trust lovers "not to kiss and tell."[75] This understanding of sharing is based on trust, or the expectation that individuals will continue to behave according to accepted social norms. And Facebook's design comes into play here, too. Although we may not be able to put our arm around someone and share secrets with them in a huddle, we can send them direct messages (emails) and fiddle with Facebook's "privacy controls" to determine, as best we can, who will see what.[76] Facebook designs its Privacy Settings

he takes Polaroid pictures of everyone's faces and posts them on a lobby wall. This way, instead of passing by someone in the hall, neighbors can greet each other with a smile, a handshake, and a name. It didn't work out too well for Jerry, of course. *Seinfeld: The Kiss Hello* (NBC television broadcast Feb. 16, 1995).

[73] Grimmelmann, *supra* note 3, at 1163.

[74] Richards & Hartzog, *supra* note 57.

[75] *Id.*

[76] *See* Gordon Gottsegen, *Here's How to Use Facebook's Mystifying Privacy Settings*, WIRED (Aug. 11, 2015, 5:55 AM), http://www.wired.com/2015/08/how-to-use-facebook-privacy-settings-step-by-step. *See also* Mary Madden, *Privacy Management on Social Media Sites*, PEW RESEARCH CENTER (Feb. 24, 2012), http://www.pewinternet.org/files/old-media/Files/Reports/2012/PIP_Privacy_management_on_social_m

page[77] to make us feel like we have control over the entire universe of privacy on the platform even though we don't.[78]

The key takeaways are as follows: there are several cues that we use in the physical world that help us determine if a given context is safe for disclosure. In other words, they are proxies for trust. Facebook has designed its interface to trigger some of those proxies, encouraging us to share more and more personal information even though the platform may not be as safe and trustworthy as we think. As Grimmelmann argued, this alone does not make Facebook culpable. The puzzle—that we seem to care more about privacy yet are sharing more personal information—is not so puzzling when Facebook is understood from a social perspective:

> [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.[79]

That is not entirely Facebook's fault. We cannot blame the platform for identifying "primal, human desires" and allowing us to realize some basic elements of human happiness. But Facebook does more than that. Helping us interact with others—friends, families, and our communities—is only a portion of Facebook's model. It also wants us to interact with its advertisers

edia_sites_022412.pdf.

[77] *See* Privacy Settings and Tools, https://www.facebook.com/settings?tab=privacy (last visited June 24, 2016).

[78] A quick review of Facebook's Data Policy, however, proves that control is severely limited. *See* Data Policy, https://www.facebook.com/policy.php (last visited June 24, 2016).

[79] Grimmelmann, *supra* note 3, at 1151.

and other third parties that generate its revenue. When Facebook leverages the trust we have in our friends to nudge us to share with businesses we've never heard of, Facebook steps over the line from dynamic social space to manipulative force.

III. MANIPULATING TRUST

As we have discussed, Facebook already leverages design to encourage users to share with each other, or as Grimmelmann has argued, to "scratch its users' social itches."[80] More specifically, part of Facebook's design is dedicated to using trust to encourage sharing. When we receive "Friend Requests" from another Facebook user, the number of friends we have in common appears immediately below the user's name. Hovering over the number tells us who sits in both networks. This information gives us clues as to the requester's trustworthiness, which is particularly important for someone we have never met offline.[81] Member posts from inside and outside our networks also notify us if a friend has recently added a comment—"Lisa Simpson replied to a comment on this post"—or is simply mentioned in the post—"Charlie Brown and Peppermint Patty were mentioned in a post." Furthermore, rather than just listing the number of "likes" for a given post, Facebook goes further and tells us that "Abbi Jacobson, Ilana Glazer and 76 others like this." When none of our friends have liked a post, the note reads, "9 people like this." This design strategy, when applied to social posts, helps grease the wheels of social interaction by indicating that the post is real, engaging, and trustworthy. These are social nudges helping to create a social space.

When applied to native advertisements in the

[80] *See id.*

[81] Research from the Pew Research Center suggests that 31% of young people have reported accepting "Friend Requests" from strangers, i.e., persons they have never met offline. Amanda Lenhart & Mary Madden, *Friendship, Strangers, and Safety in Online Social Networks*, PEW RESEARCH CENTER (Apr. 18, 2007), http://www.pewinternet.org/2007/04/18/friendship-strangers-and-safety-in-online-social-networks/.

Newsfeed, however, this tactic confuses and obscures, manipulating us into clicking on a third party's post. This isn't "scratch[ing] our social itches."[82] We have no innate human desire to interact with Spirit Airlines or Arby's. Rather, this is Facebook's attempt to transmogrify what makes its social platform so enticing into a misleading money-making scheme.

Native advertisements, or third-party links that are designed to look like social posts, also appear on our Newsfeeds. Like the social posts of our friends, these ads are often preceded by the names of our friends who have "liked" the advertiser's page. For example, a statement like, "Clara Oswald, Sarah Jane Smith, Martha Jones and 7 others like JCrew," might appear at the top of a JCrew ad about the new Spring line. And "Alice, Barry, Catherine, and 22 others like Adidas" may appear above an ad for the newest Adidas running shoe. The information about our friends, not the ad, is the first thing we see. The only thing that distinguishes these ads from our friends' social posts is the word "Sponsored," written in light grey text under the name of the company and sandwiched between the ad's much larger graphic content and Facebook's note about our friends.

Facebook, then, obscures the difference between social and commercial posts and between social interaction and endorsement, exploiting the trust-sharing link. This can be deceitful and coercive. We could respond in one of two ways: changing design or regulatory enforcement. Since platforms like Facebook may lack the incentives to change these design tactics,[83] regulators, particularly the Federal Trade Commission (FTC) and state attorneys-general,[84] may need to start paying attention to how social platforms that collect user data deploy information they know about us and our friends.

Facebook should design its Newsfeed to be more

[82] Grimmelmann, *supra* note 3, at 1151.

[83] Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH L.J. 1409 (2011).

[84] *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. __ (forthcoming 2016).

transparent about native advertising. The word "sponsored", which is confusing to many users,[85] should be changed to "From Our Advertisers." It should be larger and more obvious, not obscured by a light-colored font and other, richer content. The Associated Press mobile application is a good model. Standard news articles on the interface are in white text on a black background. A picture associated with the article is on the right; the headline is on the left. Sponsored posts not only reverse the positioning of the picture and headline; they are prefaced by a bright yellow bar that reads "Paid for by. . . ". Furthermore, a "just in time" pop up privacy notification could notify users that a click on sponsored links will release some information to third parties.

It is unlikely that Facebook would either adopt these mitigating design strategies or voluntarily drop the practice of using trust cues on native ads. Instead, the FTC[86] and the more active state attorneys-general[87] could step in.[88] By taking users' names and placing them

[85] Bartosz W. Wojdynski & Nathaniel J. Evans, *Going Native: Effects of Disclosure Position and Language on the Recognition and Evaluation of Online Native Advertising*, 45 J. ADVERTISING 157 (2016), *available at* http://www.tandfonline.com/doi/pdf/10.1080/00913367.2015.1115380 (finding, among other things, that only 17 of 242 subjects could distinguish between a native advertisement and a real news story).

[86] 15 U.S.C. § 45(a)(1) ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."). The FTC was given the authority to prevent such practices in subsection (a)(2). *See* 15 U.S.C. § 45(a)(2).

[87] Citron, *supra* note 84.

[88] As Daniel Solove and Woodrow Hartzog have shown, the FTC's authority to regulate unfair and deceptive practices is broad. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014). As the authors point out, the FTC has developed a broader view of unfair or deceptive practices, including, for example, "deception by omission," *id.* at 631, "inducement" to share personal information, *id.* at 632-33, and "pretexting," *id.* at 633, to name just a few. Their persuasive argument is that "through a common law-like process, the FTC's actions have developed into a rich jurisprudence that is effectively

on top of an advertisement in others' Newsfeeds, Facebook takes advantage of everyday social interactions among persons. It then reframes these interactions as commercial endorsements in the same way and with the same design as trust cues on social posts. In so doing, Facebook is obscuring the difference between advertising and social spaces and manipulating users into sharing information with third parties.[89] Regulating such tactics is well within the scope of the state's authority to protect the public from predatory and manipulative business practices.[90]

Facebook is not the only trust manipulator. Consider, for example, the case of Groupon, a social e-commerce company that sells vouchers, or "Deals," for discounts at participating businesses, restaurants, and other establishments. Each Deal has its own webpage, which includes the name, location, and description of the participating business, the terms of the offer, and several photographs of the establishment provided by the business.[91] At times, Groupon has also included pictures of consumers who were ostensibly at the location.[92] But rather than asking consumers or the participating business for these photos, Groupon allegedly scraped them from Instagram's application programming interface (API) by making a request for

the law of the land for businesses that deal in personal information. . . . By clarifying its standards and looking beyond a company's privacy promises, the FTC is poised to enforce a holistic and robust privacy regulatory regime that draws upon industry standards and consumer expectations of privacy . . . ." *Id.* at 589.

[89] The plaintiffs made a similar argument, albeit without a full understanding of the role of trust in manipulating disclosure, in *Fraley v. Facebook. See* Second Amended Class Action Compl. for Damages at 8-13, Fraley v. Facebook, No. CV 11-01726 LHK PSG (N.D. Cal. June 6, 2011), *available at* http://www.dmlp.org/sites/citmedialaw.org/files/2011-06-06-2ndAmendedComplaint.pdf

[90] *See* Solove & Hartzog, *supra* note 88, at 630-633; Citron, *supra* note 84.

[91] Class Action Complaint and Demand for Jury Trial at 3-4, Dancel v. Groupon, No. 2016CH01716 (Cir. Ct. Cook County Feb. 5, 2016) (hereinafter, "Groupon Complaint").

[92] *Id.* at 5.

Instagram photos "tagged" with the name of the business in the Deal.[93] In other words, Groupon asked Instagram for all photos that were taken at the business's location and included them on its Deal page. Setting aside the fact that, if true, Groupon violated Instagram's Platform Policy,[94] it is likely that Groupon included the photos to suggest to consumers that all of the individuals had already purchased the Deal, enjoyed themselves, and now endorse the business or product.[95] Groupon also placed the photos next to the Deal's "Tips" section, where actual Groupon users who had purchased the Deal provided feedback, thus suggesting that the individuals in the Instagram photos did, as well. If these allegations prove true, Groupon would appear to be taking advantage of the fact that individuals tend to share personal information online based on indicia of trust. Its tactics deceive and manipulate users into thinking the Deal is trustworthy when, in fact, it might not be.

Facebook's manipulation may be more subtle, but it is no less deceptive. Both Groupon and Facebook know that we share when we trust. That may not be a bad thing when we are talking about creating dynamic social spaces. But it raises significant privacy concerns when our information is being shared with third parties that are both strangers to us and our privacy settings.

CONCLUSION

That our propensity to share can be nudged by creating a community of sharers that we trust explains several elements of Facebook's design. These nudges may enhance our experiences because they are roughly

[93] *Id.* at 5-6.

[94] Platform Policy, https://www.instagram.com/about/legal/terms/api/ (last visited Apr. 4, 2016) stating that API users must "[o]btain a person's consent before including their User Content in any ad."). *See also Does Instagram Let Advertisers Use My Photos or Videos?*, Instagram Help Center, https://help.instagram.com/206875879493855 (last visited Apr. 4, 2016) ("No. You own your own photos and videos. Advertising on Instagram doesn't change this.").

[95] Groupon Complaint, *supra* note 90, at 6.

equivalent to personal recommendations from trusted sources. But they can also be used to coerce, mislead, and deceive, especially when a platform is designed to leverage the trust we have in each other to manipulate us into sharing with advertisers and third parties. Therefore, this essay suggests that the FTC and state attorneys-general should investigate social networks' design strategies to ensure fair and transparent business practices.