SCHOOL OF LAW
CASE WESTERN RESERVE UNIVERSITY

Case Western Reserve Law Review

Volume 67 | Issue 1

2016

Privacy, Sharing, and Trust: The Facebook Study

Ari Ezra Waldman

PRIVACY, SHARING, AND TRUST: THE FACEBOOK STUDY

Ari Ezra Waldman†

ABSTRACT

Using sharing on Facebook as a case study, this Article presents empirical evidence suggesting that trust is a significant factor in individuals' willingness to share personal information on online social networks. I then make two arguments, one that explains why Facebook is designed the way it is and one that calls for legal protection against unfair manipulation of users. I argue that Facebook is built on trust: the trust that exists between friends and the trust that exists between users and the platform. In particular, I describe how Facebook designs its platform and interface to leverage the trust we have in our friends to nudge us to share. Sometimes, that helps create a dynamic social environment: knowing what our friends are doing helps us determine when it is safe to interact. Other times, Facebook leverages trust to manipulate us into sharing information with advertisers. This should give us pause. Because Facebook uses trust-based design, users may be confused about the privacy effects of their behavior. Federal and state consumer and privacy protection regulators should step in.

CONTENTS

† Associate Professor of Law; 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. Special thanks to Peter Bearman, Debbie Becher, Robert Blecker, Richard Chused, Danielle Keats Citron, Greg Eirich, Gil Eyal, Joshua Fairfield, Jonathan Frankle, Jeffrey Goldfarb, Woodrow Hartzog, Leslie John, Melanie Kim, Frank Pasquale, Rebecca Reinhardt, Neil Richards, and Matthew Sag. This Article is based, in part, on a chapter of the author's doctoral dissertation at Columbia University. A version of this Article was presented at the Internet Law Works-in-Progress Conference at New York Law School, at the Law and Society Conference in Minneapolis, Minnesota, at the University of Toronto, Faculty of Law Symposium, "The Future of Online Privacy Regulation," and at the Loyola University Chicago School of Law Consumer Law Review symposium, "Advertising in Digital Media: Disclosures and Transparency in Social Media." Thank you to all conference participants for their questions, comments, and important feedback. All errors are my own, and I trust you will forgive me for them.

INTRODUCTION

Online social networks present a privacy puzzle. Scholars have shown that between 2005 and 2011, both total sharing on Facebook and privacy-seeking behavior on the platform increased.[1] That means that Facebook users were sharing much 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.[2] This is a particularly jarring contradiction given that Facebook's voracious appetite for data is not sated by the information we actively disclose; it also sweeps in data from our clicks, third-party apps, internet browsing behavior, and our interactions with its partners and advertisers.

So how can we explain our sharing behavior? Several studies have suggested that people make their disclosure decisions based on a variety of factors, including whether others have disclosed,[3] the order of

1. Fred Stuntzman, Ralph Gross & Alessandro Acquisti, *Silent Listeners: The Evolution of Privacy and Disclosure on Facebook*, 4 J. PRIVACY & CONFIDENTIALITY 7, 8–9 (2012).

2. Professor James Grimmelmann noted the same mystery seven years ago. *See* James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1151 (2009) (suggesting that social motivations explain why Facebook users share personal information, regardless of its privacy risks).

3. *See* Alessandro Acquisti, Leslie K. John & George Loewenstein, *The Impact of Relative Standards on the Propensity to Disclose*, 49 J. MARKETING RES. 160, 172 (2012) ("[P]eople's decisions to disclose sensitive information are comparative in nature.").

questions,[4] website design and aesthetics,[5] and social motivations,[6] to name just a few. James Grimmelmann has argued that because social networking sites are platforms for executing essential human social needs, it is Facebook's design that nudges us to disclose.[7] This Article builds on this work, arguing that Facebook encourages us to share personal information by designing its platform to cue trust among its members.

In 2013, Facebook asked its users: "How trustworthy is Facebook overall?" A spokesperson explained that Facebook was just looking for feedback to improve service and enhance user experiences.[8] But there is likely much more to it. We know that Facebook is an inherently social tool designed to create, foster, and expand social interaction.[9] We also know that Facebook routinely tinkers with its user interface to inspire user trust and, in turn, sharing. Its committee of Trust Engineers, for example, plays with wording, multiple choice options, the order of questions, designs, and other tools to encourage users to honestly report what they do not like about posts they want taken down.[10] That may be an important goal, but it shows that Facebook is well aware that trust and sharing are linked.

This Article begins where Facebook left off, seeking to fill a gap in the legal and social science literature on what motivates people to share personal information online and when regulators should step in to protect individuals from manipulation. Based on previous studies on Facebook's design and using primary empirical research of Facebook users, this Article shows that we share when we trust. In particular, it is the trust we have in others—what sociologists call particular social trust—that encourages us to share on Facebook. Higher levels of trust in the platform and higher levels of trust in those individuals in our

4. *Id.*

5. Leslie K. John, Alessandro Acquisti & George Loewenstein, *Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information*, 37 J. Consumer Res. 858, 864 (2011).

6. Pedro Giovanni Leon et al., *What Matters to Users? Factors that Affect Users' Willingness to Share Information with Online Advertisers*, Symp. on Usable Privacy and Security 9 (2013).

7. Grimmelmann, *supra* note 2, at 1151.

8. Brian Fung, *Facebook Wants to Know If You Trust It. But It's Keeping All the Answers to Itself*, Wash. Post (Dec. 31, 2013), http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/31/facebook-wants-to-know-if-you-trust-it-but-its-keeping-all-the-answers-to-itself [https://perma.cc/F9WN-E74S].

9. Grimmelmann, *supra* note 2, at 1156.

10. *The Trust Engineers*, RadioLab (Feb. 09, 2015, 8:01 PM), http://www.radiolab.org/story/trust-engineers/ [https://perma.cc/NPZ5-BSRY].

networks are associated with a higher propensity to share personal information.

Facebook knows this and it has designed its platform to benefit from it.[11] Among many other tactics, Facebook prefaces both social posts and native advertisements with information on how one's friends and other users have interacted with the content. In doing so, it not only creates the circumstances for social interaction with those we trust, it exploits the trust we have in our friends and families for financial gain by manipulating us into sharing information with third party advertisers, as well. Given how frequently users already confuse native advertisements with other content,[12] Facebook's design strategy to leverage trust to manipulate us into clicking on those advertisements should give us pause. Regulators should step in.

This Article proceeds in four parts. Part I briefly summarizes the two literatures relevant to this study: users' propensity to share personal information online and the sociology of trust. This Part argues that, to date, trust has played an underappreciated role in our understanding of sharing. Part II defines the methodology used for the research. Part III presents the results and reports on the statistically significant correlation between trust and the willingness to disclose. The results suggest that individuals tend to share personal or sensitive information in contexts of trust, with the expectation that their privacy will be protected. Part IV describes how this research is already reflected in Facebook's News Feed and suggests that privacy lawyers and regulators have a role to play in protecting consumers from manipulation.

I. PRIVACY AND TRUST

There is a growing literature on the connection between privacy and trust.[13] Several scholars, including James Grimmelmann,

11. *See* Grimmelmann, *supra* note 2, at 1155 (describing Facebook's features—including adding contacts and "poking" other users—as mechanisms to build trust in the online platform).

12. *See, e.g.*, 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, 161 (2016) (finding, among other things, that only 17 of 242 subjects could distinguish between a native advertisement and a real news story).

13. *See, e.g.*, Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, STAN. TECH. L. REV. (forthcoming 2016) (manuscript at 37–40), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2655719 [https://perma.cc/P724-5W5Q] (connecting confidentiality and trust); Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 U. MIAMI L. REV. 559, 560 (2015) (arguing that disclosures in contexts of trust should be protected as private).

Alessandro Acquisti, and others, have conducted theoretical and empirical studies into our motivations and sharing behavior on Facebook.[14] This Article brings these otherwise isolated literatures together and provides quantitative evidence that trust is an important factor in Facebook users' decisions to share. The Article also shows that Facebook designs its platform to take advantage of this link.

This Part describes the current state of research on trust and sharing. I address what social scientists mean by trust, hypothesize its connection to individuals' propensity to disclose, briefly summarize the current social science literature on sharing, and show that trust in other people has been an underappreciated force in that research. I then bring together the social science and legal literatures to tease out the theoretical relationship between trust, sharing, and privacy.

A. What Is Trust?

Much of the work on trust,[15] sharing, and privacy online focuses either on how protecting privacy can build trust[16] or on how the perception that a website can be trusted to protect user privacy can assuage the privacy risks perceived by consumers.[17] Indeed, when the Federal Trade Commission (FTC) and the California Attorney General's office recommend that online platforms be transparent about their privacy and data practices so as to inspire consumer trust,[18] they

14. *See, e.g.*, Grimmelmann, *supra* note 2 (examining the social reasons people participate on social networking websites); Stuntzman, Gross & Acquisti, *supra* note 1 (documenting how social networking platforms have changed expectations of privacy and peoples' willingness to disclose information).

15. There are two types of trust in the social science literature: general and particular. Briefly, general social trust is the belief that most people can be trusted. For example, the question—"Generally speaking, would you say that most people can be trusted or that you can't be too careful in dealing with people?"—has been asked in the General Social Survey since 1972. Ken Newton & Sonja Zmerli, *Three Forms of Trust and Their Association*, 3 EUR. POL. SCI. REV. 169, 177 (2011). Particular social trust is the trust we have in specific other people. *Id.* at 170–72. This last form of trust is the subject of this research.

16. *See* Richards & Hartzog, *supra* note 13, at 37–44 (considering the effects of certain factors, including confidentiality, discretion, transparency, honesty, and security in building trust in social networking platforms).

17. *See, e.g.*, David Gefen & Paul A. Pavlou, *The Boundaries of Trust and Risk: The Quadratic Moderating Role of Institutional Structures*, 23 INFO. SYS. RES. 940 (2012) (discussing the impact that perceptions of confidentiality, security, and trust have on consumer practices).

18. KAMALA D. HARRIS, ATT'Y GEN., CAL. DEP'T. OF JUSTICE, MAKING YOUR PRIVACY PRACTICES PUBLIC: RECOMMENDATIONS ON DEVELOPING A MEANINGFUL PRIVACY POLICY 4 (2014); FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 3–4 (2013). *See also Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy: Hearing Before the Subcomm. for Privacy,*

are talking about the trust consumers have that those platforms will fulfill their data privacy promises and safeguard customer data.[19] But on what bases do we learn to trust these websites? This Article contends that it has a lot to do with *who else* uses them. That is particularly true for online social networks.

The trust we have in specific other people is called particular social trust, or a resource of social capital between or among two or more persons concerning the expectations that others will behave according to accepted norms.[20] It is the "favourable expectation regarding other people's actions and intentions,"[21] or the belief that others will behave in a predictable manner. For example, if Alice asks Brady to hold her spare set of keys, she trusts that Brady will not break in and steal from her. 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 to grease the wheels of social activity.[22] If I never trusted, my social life would be paralyzed. As Niklas Luhmann

Technology and the Law of the S. Comm. on the Judiciary, 112th Cong. 90 (2011) (statement of Alan Davidson, Director of Public Policy, Google Inc.) ("If we fail to offer clear, usable privacy controls, transparency in our privacy practices, and strong security, our users will simply switch to another provider. This is as true for our services that are available on mobile devices as it is for those that are available on desktop computers.").

19. *See, e.g.*, Kirsten Martin, *Understanding Privacy Online: Development of a Social Contract Approach to Privacy*, 137 J. BUS. ETHICS 551 (2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2598963 [https://perma.cc/9CK6-QTKU] (examining online privacy under a social contract approach). *See also* Roger C. Mayer, James H. Davis & F. David Schoorman, *An Integrative Model of Organizational Trust*, 20 ACAD. MGMT. REV. 709 (1995) (proposing using a dyadic model of trust when studying trust in an organizational context); Michael Pirson, Kirsten Martin & Bidhan L. Parmar, *Public Trust in Business and Its Determinants*, *in* PUBLIC TRUST IN BUSINESS 116–53 (Jared D. Harris, Brian T. Moriarty & Andrew C. Wicks eds., 2014) (discussing the importance of trust in the business context).

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

21. Guido Möllering, *The Nature of Trust: From Georg Simmel to a Theory of Expectation, Interpretation and Suspension*, 35 SOCIOLOGY 403, 404 (2001). *See also* Newton and Zmerli, *supra* note 15, at 171 (noting that particular trust relates to trusting someone personally, as opposed to general trust which relates to generally trusting everyone); J. David Lewis & Andrew Weigert, *Trust as a Social Reality*, 63 SOC. FORCES 967, 968 (1985) (describing expectations from others as the basis for trust among people).

22. NIKLAS LUHMANN, TRUST AND POWER 4 (1979) (presenting trust as a "necessity" for proper social conduct).

stated, trust exists where knowledge ends.[23] It is the mutual "faithfulness" on which all social interaction depends.[24] 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.[25]

Lawyers should be familiar with particular social trust. It is, after all, at the core of the general notion of confidentiality and the more specific doctrines of privilege.[26] As Neil Richards and Woodrow Hartzog have noted, "perhaps the most basic assumption people make when disclosing personal information," whether to doctors, lovers, or ISPs, "is that the recipient will be discreet."[27] They note that we trust doctors "not to reveal information about our health and mental state" and trust lovers "not to kiss and tell."[28] Richards's 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 confidence because doing so conforms to presiding norms. These expectations also justify privilege doctrines. Mutual trust and confidentiality are essential for attorney-client, doctor-patient, and spousal privileges[29] because such norms encourage the kind of full and frank disclosure necessary for effective counsel, supportive care, and

23. *Id.* at 33–34. *See also* Patricia M. Doney, Joseph P. Cannon & Michael R. Mullen, *Understanding the Influence of National Culture on the Development of Trust*, 23 ACAD. MGMT. REV. 601, 603 (1998) (explaining knowledge-based trust).

24. *See* Waldman, *supra* note 13, at 602 ("[Trust is] essential to all social interaction, is at the heart of how we decide to share information about ourselves, and helps explain when we feel our privacy invaded.").

25. Trust helps us deal with uncertainty and complexity by allowing us to rely on the recommendations of others. *See* TALCOTT PARSONS, ACTION THEORY AND THE HUMAN CONDITION 45–47 (1978) (explaining that trust, in the professional context, builds from feelings of integrity and competence). 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.*, AARON T. BECK & BRAD A. ALFORD, DEPRESSION: CAUSES AND TREATMENT 292–324 (2d ed. 2009) (describing trust between a patient and therapist as integral to successful treatment). For a more in-depth discussion of the social benefits of particular social trust, see Waldman, *Privacy as Trust*, *supra* note 13, at 605.

26. Richards & Hartzog, *supra* note 13, at 37–41 (connecting confidentiality and trust).

27. *Id.* at 38.

28. *Id.*

29. RICHARD A. LORD, 23 WILLISTON ON CONTRACTS § 62:12 (4th ed. 2002).

love.[30] And, according to several studies, we are deeply concerned that information we share with one website may be shared with third parties.[31] Perhaps this concern stems from our inability, and lack of opportunity, to determine for ourselves whether we trust those third parties.

B. Particular Social Trust and the Propensity to Disclose

It makes sense, then, to turn to trust when thinking about what motivates us to share personal information online: Alice shares information with Brady because Alice trusts Brady with that information; the applicable norms—confidentiality and discretion—give Alice the confidence and comfort to share with Brady, trusting that Brady will be discreet. Despite the intuitive appeal of that mechanism, particular social trust has been, at best, a silent undercurrent in a growing literature on our propensity to disclose personal information.

For example, Alessandro Acquisti, Leslie John, and George Loewenstein have found that disclosure behavior is based on comparative judgments[32]: if we perceive that others are willing to disclose, we are more likely to disclose;[33] if we perceive that the information asked of us is particularly intrusive, we are less likely to disclose.[34] Acquisti and his colleagues asked individuals to respond to a series of ethics questions, some of which required them to admit to stigmatizing behavior. The individuals were more likely to respond that they had engaged in bad behaviors when told that previous respondents made similar admissions.[35] Based on research that established a link between how professional a website looks and its security,[36] Leslie John found

30. *See* Upjohn Co. v. United States, 449 U.S. 383, 389 (1981) (noting that the purpose of the attorney-client privilege "is to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice"). *See also* Trammel v. United States, 445 U.S. 40, 44 (1980) ("The modern justification for this privilege against adverse spousal testimony is its perceived role in fostering the harmony and sanctity of the marriage relationship.").

31. Mary Madden, Public Perceptions of Privacy and Security in the Post-Snowden Era, Pew Research Center 3, 29 (2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf [https://perma.cc/P2SM-AQPX].

32. *See* Acquisti, John & Loewenstein, *supra* note 3, at 172 ("[P]eople's decisions to disclose sensitive information are comparative in nature.").

33. *Id.* at 160, 165, 172.

34. *Id.* at 160, 171–73.

35. *Id.* at 165.

36. *See, e.g.*, Lorrie Faith Cranor, Web Privacy with P3P (2002) (discussing uniform internet code that will allow internet users to decide whether a website can collect information about the user's browsing

that individuals' are, perhaps counterintuitively, more willing to admit to bad behavior on unprofessional-looking websites.[37] In other words, contextual cues within an unprofessional website interface caused people to suppress privacy concerns and increase disclosure.[38] Other scholars have found that disclosure can be emotionally manipulated: positive emotional feelings about a website, inspired by website design, the type of information requested, and the presence of a privacy policy correlate with a higher willingness to disclose.[39] Still others have found that knowledge of a website's data use practices can influence disclosure behavior.[40]

This literature teaches us, among other things, that our propensity to share is contextual. That context is partly influenced by the other individuals around us.[41] That could mean that our propensity to disclose is subject to a herding effect: when we are around others who disclose, we disclose.[42] Another possible explanation is that knowledge that others have admitted to stigmatizing behavior inspires particular social trust: the admission creates vulnerability that links even strangers together and establishes a basis for social norms on the platform.

James Grimmelmann showed how social contexts are essential to our decisions to share information on online social networks. He identified several heuristics we use to evaluate the privacy risks associated with sharing on Facebook, some of which I will summarize here.[43] All

habits); Lorrie Faith Cranor et al., *P3P Deployment on Websites*, 7 Electronic Com. Res. & Applications 274, 274 (2008) (explaining the importance of privacy policies on websites); Eric C. Turner & Subhasish Dasgupta, *Privacy on the Web: An Examination of User Concerns, Technology, and Implications for Business Organizations and Individuals*, 20 Info. Sys. Mgmt. 8, 16–17 (2003) (explaining the use of privacy-enhancing technology to improve online trust among internet users).

37. John, Acquisti & Loewenstein, *supra* note 5, at 864.

38. *Id.*

39. Han Li, Rathindra Sarathy & Heng Xu, *The Role of Affect and Cognition on Online Consumers' Decision to Disclose Personal Information to Unfamiliar Online Vendors*, 51 Decision Support Sys. 434, 441–43 (2011).

40. *See, e.g.*, Leon et al., *supra* note 6, at 7 (noting participants were less willing to disclose information when they believed their information was collected on any website on the internet).

41. *See* Acquisti, John & Loewenstein, *supra* note 3, at 162 ("[W]hen people are surrounded by others who are revealing intimate details about their lives, they may conform to the prevailing norm of divulgence.").

42. *Id.*

43. *See* Grimmelmann, *supra* note 2, at 1160–64 (considering a user's conscious and subconscious reliance on proxies for privacy risks when using social media). Grimmelmann also noted that these heuristics do not always effectively or accurately assess privacy risks on Facebook. *Id.*

of them are proxies for trust.[44] First, *bigness*. Facebook's pride in being the largest social network on the planet is not rooted in a simple obsession with size. Rather, having lots of other people sharing is essential to encourage us to share with them. As Grimmelmann notes, millions of people can't be wrong. Our "Facebook-trusting friends" must know that the platform is safe; bigness shields us from the risk of being singled out for a privacy invasion.[45] In both of these ways, size is one way to identify a context of trust: more than one billion users actively sharing information on Facebook is like Alice safeguarding Brady's spare keys one billion times. 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 one after signing up lets us use 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 commented on a post above and below the content on our News Feeds. And, of course, Facebook brags about its size all the time.[46] It does so because platforms that are big are more trustworthy.

Second, *community*. Facebook's design makes us think that we're talking to specific other people in controlled spaces. We see others' faces and are taken to others' personal profile pages to interact with them. This creates a perception of safety.[47] The members of our social networks on Facebook also tend to be like us in some ways, so we

44. Although Grimmelmann used the word "trust" several times in *Saving Facebook*, he stops short of grouping these tools as proxies for understanding privacy and sharing decisions as based on particular social trust. *Id.*

45. Grimmelmann, *supra* note 2, at 1161–62.

46. 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 Come 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 [https://perma.cc/36HB-YB8U] (noting that Facebook and Google, two of the largest companies in web advertising, "have gone from a position of merely being two big, fast-growing players in mobile advertising to dominating it completely").

47. This type of rich social profile may be an effective design strategy to create safe online environments. As Danielle Citron has suggested, profiles that humanize internet users may stimulate interaction norms against online harassment. *See* DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 239–41 (2014) ("Just as the anonymity of networked interactions can influence our behavior, so can a site's environment.").

assume they are like us in a lot of ways.[48] The more familiar someone else appears to us, as Max Weber and Talcott Parsons noted, the more we are likely to bring her into our confidences.[49] Facebook also breeds a sense of familiarity by making all friends seem fungible: our closest friend and that guy we met at yoga are all defaulted as "friends." This makes us think we can share similar information with both of them.[50]

That these qualities of Facebook encourage us to share information with others, even when it is risky, is in line with much of the social science literature on the development of trust. Trust that individuals will behave according to norms of confidentiality and discretion could arise in a variety of contexts, all of them would seem to make sharing more likely. The most obvious sources of particular social trust are when the context includes explicit cues, like a confidentiality clause or prefacing a conversation with, "This is to be kept between us." Subtler indications of expectations of confidentiality are just as strong: two people sharing a secret at a party might physically turn their bodies away from the crowd, huddle down, and whisper.[51] Grimmelmann refers to this as the "I know how much this means to you" heuristic.[52] Furthermore, a friend in need may ask another friend for advice regarding a particularly sensitive, intimate, or personal problem. Trust and confidentiality also may be implied from certain professional

48. *See* CASS R. SUNSTEIN, REPUBLIC.COM 2.0 53–54 (2007) (arguing that uniformity of social networks creates echo chambers of views).

49. *See* MAX WEBER, *The Protestant Sects and the Spirit of Capitalism*, *in* FROM MAX WEBER: ESSAYS IN SOCIOLOGY 303, 312 (H. H. Gerth & C. Wright Mills eds., 1948) (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.'").

50. *See* Grimmelmann, *supra* note 2, at 1162 ("We don't say private things to people we don't know. Facebook is great at making us feel like we know lots of people.").

51. These implicit cues of confidentiality are discussed at length in ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE 112–32 (1959) (discussing the "backstage" of social interaction). *See also* ERVING GOFFMAN, STRATEGIC INTERACTION (Erving Goffman & Dell Hymes eds., 1969) (analyzing interpersonal dealings at the intersection of emotional expression and human intelligence).

52. Grimmelmann, *supra* note 2, at 1163.

contexts[53] and from a long history of interaction[54]: if Brady kept Alice's spare keys and never broke into her home, Alice is likely to continue trusting Brady with her home's security. These explicit and implicit indicia of information security allow the disclosing party to trust that the recipient of her information will continue to respect prevailing norms of confidentiality, thus encouraging sharing in the first place.

But the way trust works most often is through transference from knowns to unknowns—namely, from those we do know to strangers, or from people we know to websites we do not. For example, we may trust experts and other professionals based on their degrees, transferring the trust we have in a school's reputation, which we know, to one of its graduates, whom we do not.[55] There is some evidence that we trust lawyers and doctors based on firm or hospital affiliations, respectively,[56] and even office location in prime real estate[57] and office design.[58] The transference process does not end there. Many of us do not choose doctors based solely on their degrees. Rather, we rely on the

53. *See, e.g.*, Alberts v. Devine, 479 N.E.2d 113, 120 (Mass. 1985) ("We hold today that a duty of confidentiality arises from the physician-patient relationship . . . ."); Peterson v. Idaho First Nat'l Bank, 367 P.2d 284, 290 (Idaho 1961) (holding a bank manager liable for breach of bank's duty of confidence when he divulged details of the plaintiff's unsteady finances to the plaintiff's employer).

54. *See, e.g.*, PETER M. BLAU, EXCHANGE AND POWER IN SOCIAL LIFE 98–99 (1964) ("Since social exchange requires trusting others to reciprocate, the initial problem is to prove oneself trustworthy . . . . As individuals regularly discharge their obligations, they prove themselves trustworthy of further credit."); John K. Rempel et al., *Trust in Close Relationships*, 49 J. PERSONALITY & SOC. PSYCHOL. 95, 96 (1985); Doney et al., *supra* note 23, at 605 ("[T]he greater the variety of shared experiences, the greater the generated knowledge base and the more a target's behavior becomes predictable.") (citation omitted).

55. *See* Doney et al., *supra* note 23, at 606 ("[T]rust may develop through a transference process, during which the trustor transfers trust from a known entity to an unknown one.").

56. Mark A. Hall et al., *Trust in Physicians and Medical Institutions: What Is It, Can It Be Measured, and Does It Matter?*, 79 MILBANK Q. 613, 619–20 (2001).

57. *See* Shawn G. Kennedy, *About Real Estate: Law Firms Actively Leasing Office Space in Midtown*, N.Y. TIMES (Feb. 18, 1987), http://www.nytimes.com/1987/02/18/business/about-real-estate-law-firms-actively-leasing-office-space-in-midtown.html [https://perma.cc/8X2Y-P8YD] (describing the importance of elaborate office spaces in centralized locations for law firms to project success and promote confidence in their services).

58. *See* David Lat, *The Best Law Firm Offices in America: The Finalists!*, ABOVE THE LAW (Aug. 30, 2012, 6:19 PM), http://abovethelaw.com/2012/08/the-best-law-firm-offices-in-america-the-finalists/2/ [https://perma.cc/82VU-LVNE] (naming the "best law firm offices in America" based on architectural aesthetics, elaborate furnishings, and refined décor).

recommendations of others and, in particular, those that we respect.[59] This transference of trust from those we know to those we do not operates in the lay context as well. Mark Granovetter has shown that economic actors transfer trust to an unknown party based on how embedded the unknown actor is in a familiar and trusted social network.[60] And several studies have shown that social actors tend to trust strangers if they share the same important, perhaps stigmatizing, in-group identity.[61] This transference mechanism may be at play when the individuals in Acquisti's study shared stigmatizing information more readily after learning that others had already done the same. Transference of trust is also at the heart of Grimmelmann's heuristics: we transfer the trust we put in herds, familiar intimates, and confidential situations, generally, to specific cases of interaction on Facebook.

C. Trust, Sharing, and Privacy

Therefore, there may be a correlation between particular social trust and an individual's propensity to disclose personal information on online social networks. If there is, our understanding of privacy risks must evolve as well. When recognized at all, the relationship between privacy and trust is usually functional—namely, trust builds privacy, or privacy builds trust. Such a view may make privacy good for business, but it does not adequately protect personal privacy in the age of Facebook.

Implicit in laws like the California Online Privacy Protection Act, which requires that any website collecting personally identifiable information from a California resident post a privacy policy,[62] and explicit in recommendations from the FTC that encourage websites to be

59. *See* Roni Caryn Rabin, *You Can Find Dr. Right, with Some Effort*, N.Y. TIMES (Sept. 29, 2008), http://www.nytimes.com/2008/09/30/health/30find.html [https://perma.cc/GW8B-MYJH] (noting the difficulty of objectively measuring physician qualifications as the basis for people having to rely on recommendations from friends and family when choosing a doctor).

60. *See* Mark Granovetter, *Economic Action and Social Structure: The Problem of Embeddedness*, 91 AM. J. SOC. 481, 490 (1985) (discussing the "role of concrete personal relations and structures (or 'networks') of [embedded] relations in generating trust and discouraging malfeasance").

61. *See* Michele Williams, *In Whom We Trust: Group Membership as an Affective Context for Trust Development*, 26 ACAD. MGMT. REV. 377, 381, 385 (2001) ("People tend to associate positive beliefs and feelings with the groups to which they belong.").

62. CAL. BUS. & PROF. CODE §§ 22575–22579 (West 2014). Delaware recently passed a similar statute. *See* DEL. CODE ANN. tit. 6, §§ 1201C–1206C (West 2016).

transparent about their data use practices,[63] is the notion that protecting privacy builds trust. These policies require and encourage web platforms to both be honest with users about data uses and aggressively protect users' personally identifiable information. Scholars are taking note of these policies. Kirsten Martin argues that, all else being equal, a website's failure to meet the privacy expectations of users will negatively impact the trust those users have in the website.[64] Neil Richards and Woodrow Hartzog, furthermore, have argued that privacy should be conceptualized as a builder of trust rather than as a shield against invasions. Part rhetorical, part substantive, Richards's and Hartzog's argument is that privacy laws should be the tools that build trust in information sharing relationships.[65]

These are important first steps in reminding online platforms that privacy is good business. But if sharing occurs in contexts of particular social trust, it is not clear that these understandings of privacy are sufficient to adapt privacy to the digital age. In a world where petabytes of our data are in the hands of third parties[66] and at risk of further disclosure to private as well as government actors, saying that privacy builds trust does not provide a clear doctrinal path for continued privacy protection for information known to some others.[67] Merely

63. *See* FED. TRADE COMM'N., *supra* note 18, at 3 (emphasizing the importance of short, effective, and accessible privacy disclosures as a means to build trust with online users).

64. Kirsten Martin, *Formal Versus Informal Privacy Contracts: Comparing the Impact of Privacy Notices and Norms on Consumer Trust Online* 1 (Oct. 5, 2015) (unpublished manuscript), http://www.law.uchicago.edu/files/file/martin_formal_versus_informal_privacy_contracts.pdf [https://perma.cc/KKP7-RSJB].

65. Richards & Hartzog, *supra* note 13, at 34.

66. 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 two petabytes of data. Facebook, consequently, 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 [https://perma.cc/H5TD-4G3J].

67. Many scholars have addressed this problem in different ways. *See, e.g.*, Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1427–28 (2000) (arguing for a "constitutive" relationship between the flow of information and self-development); Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 856–57 (2000) (relying on "bandwagon effects" in which the government serves as a model infrastructure for limiting the transmission of falsified information online). *See generally* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004) (arguing that the collection and aggregation of personal information disrupts our expectations of what will happen to our information); Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV.

requiring notice of data use practices under the governing notice-and-choice approach to privacy ignores the myriad ways in which web platforms can manipulate our propensity to share through leveraging, among other tools, website design and the information they collect about our social networks. And seeing trust as a byproduct of a functioning privacy regime misses the fact that sharers tend to expect privacy protection where trust exists already.

Seeing trust as antecedent to privacy judgments is a step in the right direction. This is the idea that users will only make privacy-related decisions based on perceptions of trust, and it is implicit in opt-in clauses and "just-in-time" notifications. For example, the FTC recommends that before mobile apps access sensitive information, they should provide concurrent disclosures of the impending data use and "obtain affirmative express consent" from users.[68] Per the FTC, "[p]roviding such a disclosure at the point in time when it matters to consumers, just prior to the collection of such information by apps, will allow users to make informed choices about whether to allow the collection of such information."[69]

But these may not be the only ways websites build trust with their users. This Article argues that our trust in websites, or our expectations that they will use our data according to prevailing social norms of discretion, may also come from specific determinations about who among our friends also uses the website, clicks on a link, buys a product, or shares information. Privacy scholars have been inching closer to this trust-building, information-sharing mechanism. Meanwhile, social networks like Facebook are far ahead.[70]

1087 (2002) (contending that different information privacy invasions, including the collection of digital dossiers on individuals, implicate a variety of overlapping interests rather than one single common denominator). *See also* Waldman, *supra* note 13 (arguing that information privacy should be understood as protecting relationships of trust in order to protect as private information known to some others).

68. FED. TRADE COMM'N., *supra* note 18, at 15. *See also* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 60 (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf [https://perma.cc/2HVK-5P2Y] (suggesting that companies "make privacy statements clearer, shorter, and more standardized; give consumers reasonable access to their data; and undertake consumer education efforts to improve consumers' understanding of how companies collect, use, and share their data").

69. FED. TRADE COMM'N., *supra* note 18, at 15.

70. *See* Grimmelmann, *supra* note 2, at 1151–60 (detailing the ways Facebook "drives users to release personal information").

II. RESEARCH DESIGN, METHODOLOGY, AND DATA

I designed an empirical study to test the link between trust and sharing, asking: What effect, if any, does particular social trust have on internet users' willingness to share personal information on online social networks? This study included survey questions to identify what information respondents shared on Facebook, why they share it, and for what reasons, if at all, they would share information with strangers.[71] Based on this survey, this Article concludes that among participants in online social networks like Facebook, particular social trust contributes to individuals' propensity to share: sharing increases when trust increases and trust in Facebook is correlated with having friends on Facebook that users trust. Facebook has known this trust-sharing link for some time, and has been exploiting it to encourage us to cede even more control over our information. The policy and regulatory implications of that conclusion are discussed after this Section.

A. Facebook

Facebook was chosen as the platform for this research because of its size and its massive data collection practices. It is the largest and most popular online social network. As of March, 2016, it had more than 1.65 billion monthly active users, 1.09 billion daily active users, 989 million mobile daily active users, and 1.51 billion mobile monthly active users.[72] Given its size, it is a voracious gatherer of information,

71. Respondents were recruited through Amazon Mechanical Turk, an online marketplace that pays individuals to crowd source the completion of various tasks, including research surveys. Responses were collected at several points during 2015. Workers were not permitted to complete the survey more than once. Several studies have shown that Amazon Turk offers researchers a random sample of respondents with a demographic distribution roughly comparable to the United States population. *See, e.g.*, Tara S. Behrend et al., *The Viability of Crowdsourcing for Survey Research*, 43 BEHAV. RES. METHODS 800, 800–13 (2011) (concluding that crowdsourcing platforms, such as Amazon Mechanical Turk, are "efficient and appropriate alternative[s] to a university participant pool"); Gabriele Paolacci et al., *Running Experiments on Amazon Mechanical Turk*, 5 JUDGMENT & DECISION MAKING 416 (2010) (confirming that Mechanical Turk is a "reliable source of experimental data in judgment and decision-making"). Turkers were paid for their time: on average, the survey took nineteen minutes and twenty-eight seconds to complete, resulting in a $4.62 hourly rate. To be eligible to participate, Turkers were required to have at least a 95% approval rating for 1000 completed tasks on the platforms. This relatively high pay and high approval rating and experience, plus screening checks that determined, as best as possible, whether workers had made a good faith effort to complete the survey, were meant to ensure honest and accurate responses.

72. *Newsroom*, FACEBOOK (June 26, 2016), https://web.archive.org/web/20160626012315/http://newsroom.fb.com/company-info/ [https://perma.cc/2S8D-KV6A]. For the current statistics, see FACEBOOK NEWSROOM, http://newsroom.fb.com/company-info/ (last visited June 26, 2016).

some which we hand over directly and some of which is gathered without our knowledge. It is worth summarizing both processes.

To sign up for an account we have to provide our names, email addresses or mobile numbers,[73] dates of birth, and 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.[74] 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." Facebook is designed to make image management easy.[75]

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. 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.[76]

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 identify them with a link to their profile.[77] 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"

73. If you do not provide your mobile number upon registration, 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?*, Facebook, https://www.facebook.com/help/1137953062904148 [https://perma.cc/HT55-AJW5] (last visited June 22, 2016).

74. *Step 1: Find Your Friends*, Facebook, https://www.facebook.com/gettingstarted/?step=contact_importer (last visited October 21, 2016).

75. *See* Goffman, *supra* note 51, at 25 (using an extended metaphor of the back-stage and front-stage of a play to argue that we present ourselves to others in ways that may be different from the reality of who we are).

76. 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.

77. *How Tagging Works*, Facebook https://www.facebook.com/about/tagging [https://perma.cc/C47H-3EJN] (last visited June 22, 2016).

someone to flirt.[78] We can play any of the multitude of apps and games on the Facebook platform, including FarmVille.[79] We can post comments to a friend's "timeline" or tag them in posts on our own.[80] We can also tag a location for those posts, so the Facebook universe knows where we are.[81] And unless a we restrict certain posts from appearing in our timelines, most of those posts will appear in a "News Feed," or the running list of stories, interactions, and contributions that we see when we log in.[82] 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 six reactions: Love, Laugh, Wow, Sad, Angry, and, of course, Like.[83]

The Facebook "like" button, a right-handed, white thumbs up on the Facebook blue background,[84] 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

78. *See* Jackie Cohen, *5 Rules of Facebook Flirting*, SOCIAL TIMES (Apr. 14, 2009, 11:11 AM), http://www.adweek.com/socialtimes/facebook-flirting/308415 [https://perma.cc/4HER-M8N6] ("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?").

79. *FarmVille Page*, FACEBOOK, https://www.facebook.com/FarmVille/ [https://perma.cc/QV6Y-8CM3] (last visited June 22, 2016). *But see* Saqib Khan, *How to Block Annoying Game Requests from Your Facebook Friends*, VALUEWALK (Mar. 4, 2013, 3:17 PM), http://www.valuewalk.com/2014/03/block-game-requests-on-facebook/ [https://perma.cc/5VL7-LHFU].

80. *How Do I Post to My Timeline*, FACEBOOK, https://www.facebook.com/help/1462219934017791 [https://perma.cc/ST7W-BBQ8] (last visited June 22, 2016).

81. According to some sources, there are seventeen billion location-tagged posts per day on Facebook. Kevin Ho, *41 Up-to-Date Facebook Facts and Stats*, WISHPOND (2015), http://blog.wishpond.com/post/115675435109/40-up-to-date-facebook-facts-and-stats [https://perma.cc/8U97-DXMT].

82. *How News Feed Works*, FACEBOOK, https://www.facebook.com/help/327131014036297/ [https://perma.cc/GFR9-AX3B] (last visited June 22, 2016).

83. Sammi Krug, *Reactions Now Available Globally*, FACEBOOK (Feb. 24, 2016), http://newsroom.fb.com/news/2016/02/reactions-now-available-globally/ [https://perma.cc/9N7X-EEA3].

84. *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 [https://perma.cc/6K3J-K455] (explaining the use of various colors in marketing and the effects they have on viewers).

million per minute.[85] 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;[86] 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.[87]

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.[88]

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 memory capsules. Thanks to Amazon's cookie, for example, I can put a plush Judy Hopps (from the Disney movie, *Zootopia*)[89] in my Cart, close the window, and have the

85. Ho, *supra* note 81.

86. *See* Veikko Eranti & Markku Lonkila, *The Social Significance of the Facebook Like Button*, FIRST MONDAY (June 1, 2015), http://firstmonday.org/ojs/index.php/fm/article/view/5505/4581#3a [https://perma.cc/2LQM-M6DB] (detailing how Facebook tracks a user's interests and hobbies via that user's use of the "Like" button).

87. *See* Robinson Meyer, *How Facebook Could Tilt the 2016 Election*, THE ATLANTIC (Apr. 18, 2016), http://www.theatlantic.com/technology/archive/2016/04/how-facebook-could-tilt-the-2016-election-donald-trump/478764/ [https://perma.cc/DB4C-KGNM] (analyzing the effects Facebook could have on voter turnout).

88. Much of the following discussion is based on Franziska Roesner, Tadayoshi Kohno & David Wetherall, *Detecting and Defending Against Third-Party Tracking on the Web*, 9TH USENIX SYMP. 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*, FACEBOOK, https://www.facebook.com/policy.php [https://perma.cc/DPP5-CPRS] (last visited June 23, 2016) (explaining how Facebook does and does not use the data it collects).

89. It's adorable. *See Zootopia Large Plush Office Judy Hopps*, AMAZON.COM, https://www.amazon.com/Zootopia-Large-Plush-Office-Hopps/dp/B016LBYL42/ref=sr_1_4?s=toys-and-games&ie=UTF8&qid=

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.[90]

It is also central to information flows and tracking. Consider the New York Times website, www.nytimes.com. Nytimes.com runs several ads on its homepage. When I last visited the site, 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.[91] These ads sit within "iframes," or pages within the main nytimes.com page.[92] It has to be this way; otherwise, nytimes.com would have to grant these companies access to its code to insert their ad language. As a page within a page, these ads also drop cookies onto our computers, allowing them to track us wherever we go. If you have ever wanted to know why similar advertisements from the same company tend to follow us around the web, that is why.

"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.[93] When we visit these pages, Facebook may be receiving 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.[94] And Facebook channels that information into user-targeted advertisements.[95] When we "like" a post

---

1466705009&sr=1-4&keywords=judy+hopps+plush [https://perma.cc/PJ9P-5LV4].

90. *See* Roesner, Kohno & Wetherall, *supra* note 88, at 2 (describing cookies and their storage and tracking usages).

91. *See* N.Y. TIMES, http://www.nytimes.com/ (last visited June 21, 2016).

92. *See* Roesner, Kohno & Wetherall, *supra* note 88, at 2 (explaining how websites can embed content from different domains). *See also* E-mail from Jonathan Frankle, Staff Technologist, Center for Privacy and Technology, Georgetown University Law Center, to Author (June 23, 2016, 8:27 AM) (on file with author).

93. Any developer can visit Facebook to get the code for the "Like" button and drop it into their page. *Like Button for the Web*, FACEBOOK FOR DEVELOPERS, https://developers.facebook.com/docs/plugins/like-button [https://perma.cc/NV9X-YZTF].

94. *See* Tom Simonite, *What Facebook Knows*, MIT TECH. REV. (June 13, 2012), https://www.technologyreview.com/s/428150/what-facebook-knows/ [https://perma.cc/CFF2-7DVN] (detailing the enormous amount of information that Facebook collects from its users, even when users do not use the "Like" button).

95. Tom Simonite, *Facebook's Like Buttons Will Soon Track Your Web Browsing to Target Ads*, MIT TECH. REV. (Sept. 16, 2015),

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 collected more than 300 petabytes of data on us.[96] It is truly a data behemoth.

In 2012, Facebook revealed that it sweeps in 2.5 billion pieces of content and more than 500 terabytes of data each day. With "2.7 billion Like actions and 300 million photos per day," Facebook analyzes nearly "105 terabytes of data each half hour,"[97] including the personal data we provide to the real-time location of our smartphones. The company, along with third-party and partner websites, tracks users' web-browsing history, purchases, and other web content.[98] It has teamed up with corporate data brokers Datalogix, Epsilon, Acxiom, and BlueKai to allow companies to display targeted ads on Facebook based on the data those brokers have on individual users.[99] All of this information is essential to the success of Facebook's business model, relying as it does on behavioral advertising, targeting content, and tailoring users' online experiences. Knowing what might make users more or less willing to share personal information with Facebook, therefore, matters to both privacy advocates and information gatherers.

B. The Survey

Part I of the survey asked for basic demographic data: respondents selected age categories, gender, education level, sexual orientation, and race or ethnicity. Respondents were then asked how much time they spend online each day and to select from a list all the social networking websites on which they maintain active profiles, where "active" referred to any website that respondents viewed or updated regularly. These

---

https://www.technologyreview.com/s/541351/facebooks-like-buttons-will-soon-track-your-web-browsing-to-target-ads/ [https://perma.cc/KB76-XSA2].

96. Ho, *supra* note 81.

97. Josh Constine, *How Big Is Facebook's Data? 2.5 Billion Pieces Of Content And 500+ Terabytes Ingested Every Day*, TECHCRUNCH (Aug. 22, 2012), http://techcrunch.com/2012/08/22/how-big-is-facebooks-data-2-5-billion-pieces-of-content-and-500-terabytes-ingested-every-day/ [https://perma.cc/UGA4-GGFQ].

98. *Data Policy*, FACEBOOK, https://www.facebook.com/about/privacy/update/ [https://perma.cc/V8HP-EKW9]. *See also* Will Oremus, *There Are Two Kinds of Online Privacy. Facebook Only Likes to Talk About One.*, SLATE (Nov. 13, 2014, 4:37 PM), http://www.slate.com/blogs/future_tense/2014/11/13/facebook_privacy_basics_page_what_it_won_t_tell_you_about_personal_data.html [https://perma.cc/X576-K4X3] (detailing all the ways Facebook tracks its users).

99. *New Ways to Reach the Right Audience*, FACEBOOK (Feb. 27, 2013), https://www.facebook-studio.com/news/item/new-ways-to-reach-the right-audience [https://perma.cc/D2L6-B5S6].

two questions are commonly used by social science researchers to assess how "networked" an individual is; a high number of active profiles or many hours spent online may be correlated with increased sharing of personal information.

Part II of the survey concerned what type of information users share on Facebook. Twenty-seven different items were selected based on Pew's research, my own observations of sharing on Facebook, and advice from research assistants. Respondents were asked Yes/No questions about whether they shared the given information. The questions ranged from, "*Do you share jokes or funny videos?*" to "*Do you share your personal email address?*" When coding the responses for analysis, I created a "Total Sharing" column that aggregated all "Yes" answers and a separate "Total Intimate Sharing" column that aggregated all "Yes" answers for items shared that could be consider more personal. The questions for which answers constituted the "Total Intimate Sharing" data set were selected based on personal value judgments. The relative position on the scale itself was not considered relevant; for the purposes of this research, it did not matter whether "personal telephone number" was more or less intimate than "information about illnesses or medication." Both qualified as "intimate."[100]

Part III of the survey included the standard trust question: *Generally speaking, would you say that most people can be trusted or that you can't be too careful in dealing with strangers?* This question was asked to obtain baseline information on respondents' general feelings about trust and trust in others. This section also asked respondents how many "friends" they had on Facebook, how many of their close friends used the platform, and how much they trusted Facebook to protect their privacy. Respondents rated their trust in Facebook on a scale of 1 (no trust) to 10 (absolute trust).

Part IV of the survey asked respondents a series of Likert scale questions about their motivations to share information on Facebook. The diverse list captured potential emotional, rational, and social motivations. For example, respondents were asked if they felt compelled to share on Facebook because "*everyone [they] know does.*" Other questions asked if they only "*share with certain people on Facebook*

100. The information included in the Total Intimate Sharing data set were as follows: personal email address, location data, personal phone number, information about the respondent's romantic life, intimate or suggestive pictures, sexual orientation, first and last name of the respondent's partner, information about any children, admissions about doing something illegal or stigmatized, pictures of the respondent kissing someone else, pictures showing the respondent drunk or drinking to excess, names of family members, home address, admission of depression or sadness, birth date and year, and medical information. This information is more intimate or personal than, for example, funny videos, news items, college attended, professional accomplishments, non-intimate selfies, hobbies and interests, place of employment, and political views on current affairs or issues.

[where the information] will stay with those people and not reach a wider audience" or if they share because they "*have set up privacy preferences that protect [their] information from outsiders.*" Other options sought to determine if people share based on their perception of how well Facebook protects their privacy or based on the fact that "*nothing bad has ever happened*" to anyone they knew that shared information. The goal of this section was to elicit different possible motivations for sharing personal information. This data can be compared with the revelation data of the previous section.

Section V of the survey also included Likert scale questions. These questions sought to determine whether certain contextual factors would make respondents more or less likely to accept a "friend request" from a stranger. This was used as an admittedly imperfect proxy for a willingness to share information with strangers to avoid a response bias.

C. Data Report

This Section reports on the data collected, including the background demographics of the sample and the survey responses.

1. Background Demographics

Although the entire survey was anonymous, respondents were required to identify their age bracket, gender, education level, sexual orientation, race or ethnicity, the number of active online social networking profiles, and the amount of time they spend online per day. There were 629 valid responses ($n = 629$), of which 46% (287) were female and 54% (342) were male. This differs from the wider Facebook community, which remains majority female.[101] The gender gap has been shrinking for some time, however, and women and men now use social media platforms at comparable rates.[102] It is, therefore, unsurprising that some samples of Facebook users would deviate slightly from the average gender distribution.

Users ages 18–24 constituted 14.4% of the sample; 25–34 year-olds made up just over 51%. The first group is slightly underrepresented, while the second group is overrepresented, when compared with the most recent available data.[103] Because of this significant deviation from

101. Monica Anderson, *Men Catch Up with Women on Overall Social Media Use*, PEW RES. CTR. (Aug. 28, 2015), http://www.pewresearch.org/fact-tank/2015/08/28/men-catch-up-with-women-on-overall-social-media-use/ [https://perma.cc/3XNV-YZ4S].

102. Andrew Perrin, *Social Media Usage: 2005–2015*, PEW RES. CTR. 3 (Oct. 8, 2015), http://www.pewinternet.org/files/2015/10/PI_2015-10-08_Social-Networking-Usage-2005-2015_FINAL.pdf [https://perma.cc/B68Q-NG5D].

103. Keith N. Hampton et al., *Social Networking Sites and Our Lives*, PEW RES. CTR. 9 (June 16, 2011), http://www.pewinternet.org/files/old-media//Files/Reports/2011/PIP%20-%20Social%20networking%20sites%

the distribution of Facebook users by age, any correlations involving age should be questioned and retested with another sample.

The sample is highly educated, with 85% of respondents reporting that they completed at least some college. Several surveys also suggest that the Facebook population is highly educated,[104] which suggests that the sample may resemble the Facebook population, generally, but differs from the overall population of Internet users or consumers. The sample is also relatively networked. Approximately 71% of respondents maintain active profiles on 1, 2, or 3 social networking sites. All respondents, by definition, have a Facebook profile; the next most popular platforms were LinkedIn and Twitter.

2. Quantitative Data Analysis

This Section presents the quantitative analysis of the data collected.[105] The Article's hypotheses are that (1) higher levels of trust that Facebook will protect our privacy and higher levels of trust in those individuals in our networks are both associated with a higher propensity to share personal information, and (2) having a network with high levels of trust is associated with trusting that Facebook will protect our privacy. The data collected lend credibility to both hypotheses.

Social scientists have not used online social network participants to test the relationship between trust and the propensity to share. Although several pieces of data included in the survey could correlate with a willingness to share information on Facebook—age, gender, education, sexual orientation, race or ethnicity, networked level, time spent online, general social trust, trust that Facebook will protect user privacy, how many friends one has on Facebook, and how many close friends use Facebook—only those factors speaking to trust were found to have any statistically significant association.[106] With respect to sharing, generally,

20and%20our%20lives.pdf [https://perma.cc/64HG-NTM4]; *Number of Facebook Users in the United States as of February 2016, by Age Group (in Millions)*, STATISTA (Feb. 2016), http://www.statista.com/statistics/398136/us-facebook-user-age-groups/ [https://perma.cc/C9R7-SK7A].

104. *See* Hampton et al., *supra* note 103, at 12.

105. The raw data is available at New York Law School's Innovation Center for Law and Technology's Data Privacy Project.

106. I used bivariate correlation to test relationships and then partial correlation to determine if the relationship stood while controlling for other variables. Correlation generally refers to the degree and direction of association of variable phenomena: how well one can be predicted from the other. Bivariate correlations analyze the relationship between two variables and mainly serve to test hypotheses for further research. Partial correlations analyze the relationship between two or more variables while controlling, or removing, one or more variables from the relationship. For example, a data set may include: information, gender, highest degree level obtained, and annual income. A partial correlation could test the relationship between degree

and sharing personal information, a greater propensity to share on Facebook is positively associated with the number of Facebook friends one has,[107] the number of close friends that use Facebook,[108] and the extent to which one trusts Facebook to protect user privacy.[109] This means that having more friends, more close friends who use Facebook, and greater institutional trust in Facebook are all associated with greater sharing of personal information. When controlling for the other variables, these associations remained significant.

Regression analysis confirms a relationship.[110] Regression is a form of predictive analysis that tries to explain the relationship, if any exists, between one dependent variable and one or more independent variables. We use regression techniques to answer questions like: Are people who are left-hand dominant (independent variable) more or less likely than the general population to have high SAT scores (dependent variable)? Are redheads more or less likely to be architects? Are those who identify as religious more or less likely to vote Republican? We want to know if any of a series of independent variables—age, gender, education level, and proxies for trust, for example—have an impact on a single dependent variable—the willingness to share more information, and more personal information, on Facebook.[111]

---

obtained and income, controlling for gender, or the relationship between annual income and gender, controlling for degree.

107. For total sharing, $r = .197$, Sig. = .000. For total intimate sharing, $r = .200$, Sig. = .000. Spearman's rho correlation—a correlation for variables that are at least ordinal—was used because almost all variables in the data set were ordinal, i.e., ranked categories: age was reported in categories, as was education level, number of Facebook friends, and number of close friends on Facebook. All r coefficients were significant at the 0.01 level (2-tailed), indicating statistical significance.

108. For total sharing, $r = .235$, Sig. = .000. For total intimate sharing, $r = .201$, Sig. = .000.

109. For total sharing, $r = .311$, Sig. = .000. For total intimate sharing, $r = .301$, Sig. = .000.

110. Regression is a statistical tool used when we want to predict the value of a variable based on the value of two or more other variables. Correlations merely tell us if there is a relationship. Regression is a much more powerful way of explaining what that relationship is.

111. Using all the independent variables in the survey, the model would have violated the multicollinearity assumption of multiple regression. Multicollinearity happens when two or more independent variables are highly correlated with each other, which makes it difficult to decipher which variable is actually causing the dependent variable to differ from the mean. As an example, when one football player sacks the quarterback, we have a good idea who did what. But when three football players tackle him at the same time, it is hard to identify which man made the biggest contribution to the sack. In the model, age and education are highly correlated with each other: older people tend to be more educated. To fix this problem, I eliminated age and education level from the regression analysis.

Table 1: Regression Results for Sharing, Generally

	Coefficient	Std. Error
Constant	6.599	1.534
Gender	.287	.385
Sexual Orientation	.489	.568
Race	-1.059	.460
Networked	.275	.122
Time Online	.657	.409
General Trust	.465	.395
Trust in Facebook	**.551***	.081
# Facebook Friends	**.969***	.363
# Close Friends on Facebook	**1.997***	.475
* indicates statistical significance at 99% level		
R-squared: .184		
n=629		

As evident from Table 1, proxies for trust—trust that Facebook will protect our privacy, the number of "Facebook friends" we have, and the number of close friends we have on the platform—are the only statistically significant predictors of a willingness to share, generally. More specifically, for every two notches up on the trust scale ("Trust in Facebook," where "1" refers to "no trust" and 10 refers to "complete trust") users are likely to share an additional piece of personal information. Similarly, respondents with more than 1000 "Facebook friends" shared, on average 1 more piece of information on the platform than those with 501-1000 friends. And those with "many" close friends on the website share, on average, two more pieces of information than those with "some" close friends on the platform. Although these factors may only account for just under 20% of sharing behavior (r^2=.184), factors related to trust must be included in the conversation about our propensity to disclose information. What's more, Table 2 shows that the effect of trust is also strong when we focus on sharing particularly intimate or personal information.

Table 2: Regression Results for Sharing Personal Information

	Coefficient	Std. Error
Constant	2.646	.936
Gender	.158	.235
Sexual Orientation	.167	.346
Race	-.439	.280
Networked	.060	.075
Time Online	.316	.249
General Trust	.291	.241
Trust in Facebook	**.315***	.049
# Facebook Friends	**.675***	.221
# Close Friends on Facebook	**.743***	.290
* indicates statistical significance at 99% level		
R-squared: .157		
n=629		

Other data that can also speak to the relationship between particular social trust and the decision to share are motivations for accepting Facebook "friend requests" from strangers. As discussed above, overlapping networks and sharing an important or in-group social identity have been found to be strong indicators of trustworthiness in strangers.[112] The survey asked respondents several questions about whether a given piece of information about a stranger, defined as an individual they had never met offline in person before, would make it more or less likely that they would accept the stranger's "friend request." They covered a wide range of possible reasons for accepting a "friend request" from a stranger, from "large number of mutual friends" and "the stranger is friends with your close friends" to "physical attractiveness" and "you will never see the stranger in real life." Answers to the first and second questions would speak to the strength of overlapping networks and the presence of particular social trust in that network. Respondents were also asked if they are more likely to accept a "friend request" from a stranger who shares their minority status. This last question was used as a proxy for determining the role of an important in-group identity in developing a connection with a stranger. These factors could then be tested for any relationship with expecting Facebook to protect user privacy, thus suggesting that particular social trust plays a role in the development of institutional trust.

Many of the factors that received an overwhelming concentration of "more likely" and "much more likely" answers are proxies for particular social trust. For example, 85% of users would accept a "friend request" from a stranger if they shared a large number of mutual friends. More than 81% of respondents would accept a request if the stranger was friends with their close friends. And although only 18.3% would be more likely to accept a "friend request" from a stranger that

112. *See supra* notes 60–61 and accompanying text.

shared their same sexual orientation, approximately half of those respondents also identified as members of the LGBT community. These are cues of trustworthiness based on strong overlapping networks and in-group identity: as discussed above, individuals routinely transfer the trust they have in known entities (friends and close friends) to unknown entities (strangers).[113] The next most important factor was evidence of active participation on Facebook (63.3%), which is another social cue of trustworthiness: active participation suggests that the account is real, mitigating the risks associated with bringing a stranger inside a network. This is, of course, precisely the role of particular social trust.[114]

Given the amount of information someone can learn about us if they are among our Facebook "friends," accepting "friend requests" from strangers based on transferring trust indicates the power of particular social trust in the propensity to share information. Attractiveness or sharing similar names, genders, hometowns, locations, or hobbies and interests were not considered important or, in only a few cases, made respondents less likely to accept the "friend request." These factors are unrelated to particular social trust: none of them are strong indicators of predictable behavior according to accepted social norms. Notably, 27% of respondents stated that they were less likely to add a stranger to their network if they knew they would never meet the stranger in person, suggesting that, at least on Facebook, anonymity is not an invitation to share.

The Article's second hypothesis is that having trusted friends on Facebook is associated with trusting that Facebook will protect our privacy. This can sound strange: trust in others has little to do with how well Facebook protects user privacy. If this relationship exists, however, social networks can gain our trust not only by actually protecting privacy. They can also manipulate us into sharing more information with them by exploiting our relationships with our friends. The data suggests that general social trust is strongly predictive of institutional trust in Facebook, but particular social trust is weakly predictive. Responding that we do generally trust other people is associated with a more than one step increase on the 1–10 Facebook trust scale compared to those who respond that generally do not trust others.[115] This is in line with current research, as well.[116] With respect to particular social trust, survey data on network size and the presence of

113. *See supra* notes 55–61 and accompanying text.

114. *See supra* notes 20–25 and accompanying text.

115. Using a multiple regression model: Coefficient = 1.263, Sig. = .000.

116. *See* D. Harrison McKnight, Vivek Choudhury & Charles Kacmar, *Developing and Validating Trust Measures for e-Commerce: An Integrative Typology*, 13 Info. Sys. Res. 334, 337–40 (2002) (finding that in terms of institutional trust, users who have had successful internet experiences in the past will continue to trust that institution in the future).

close friends on Facebook could serve as proxies. These factors are weaker predictors of trust in Facebook, but the relationship is still statistically significant: having a larger network was associated with a 0.62 increase in trust that Facebook would protect one's privacy; having more close friends on the platform predicted an even smaller increase.[117] Admittedly, the indicators of particular social trust are weak predictors of trust that Facebook will protect user privacy. But even a weak, yet statistically significant, relationship is notable.

III. Significance of Findings

This Article presents data suggesting that (a) an individual's expectation that an online social network will protect his or her privacy is predictive of the propensity to share personal information on that website, (b) having a large network of many close friends on the website is another predictor of a willingness to share, and (c) although being a trusting person is a stronger predictor of expecting an online social network to protect user privacy than having many close friends on the network, the presence of many close friends on Facebook was also predictive of trust in the platform. This data lends further support for the argument that self-disclosure is contextual, and, in particular, that the propensity to share is based on trust. The implications of this research fall into two categories. Online social networks like Facebook already know about the connection between particular social trust and sharing; it explains various facets of Facebook's design. But some elements of that design may manipulate us into sharing more than we intend. Privacy lawyers, scholars, and regulators should also recognize that information tends to be shared in contexts characterized by particular social trust. Regulators should ensure that web platforms are not manipulating trust to deceitfully encourage users to share personal information.

A. How Facebook Exploits Trust

For online platforms, establishing trust with users is critical if they want us to share our personal information. This study suggests that the relationship holds for social networking sites, as well. The data also suggest that indicators of particular social trust, including having many close friends on Facebook, are also important in predicting a users' willingness to share. Therefore, platforms may be able to encourage sharing by letting users know that their friends have also shared.[118]

117. Network size: Coefficient = .627, Sig. = .000. Number of close friends on Facebook: Coefficient = .204; Sig. = .002.

118. This is also in line with the current literature on e-commerce websites. *See* Acquisti, John & Loewenstein, *supra* note 3, at 160.

Facebook already designs its platform to encourage users to share with each other, or as James Grimmelmann has argued, to "scratch its users' social itches."[119] It lets us craft and maintain public profiles, which allow us to articulate a particular message about who we are.[120] It also lets us join affinity groups and causes and publicizes what we post on others' Timelines.[121] Facebook deepens our connections to friends and helps establish new ones: we add people as contacts or "friends," send notes or messages or pictures of birthday cakes with our friends' names on them, and "tag" people in our own content.[122] And it does all of this publicly to encourage reciprocal sharing.[123] Facebook also helps us find community and establishes our value in that community. We add connections, make comments, and share our passions because doing so helps us find other, similarly situated potential friends and mates. And adding connections increases our social capital.[124]

Facebook leverages trust, thereby encouraging us to share, by telling us what our friends are up to. When we join, it tells us who else has joined and lets us invite friendly faces along with us. When we seek to join affinity groups or causes, those pages immediately tell us who among our friends are also members of the community. When we log on, our friends' likes, viewpoints, and interests are on the home page, visible to us by a default organizational algorithm that privileges the social interactions of those closest to us. 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 our mutual friends, or who sits in both networks. This information gives us clues as to the requester's trustworthiness, allowing us to transfer the trust we have in our friends to an unknown, which is particularly important for someone we have never met offline.[125]

119. Grimmelmann, *supra* note 2, at 1151.

120. *Id.* at 1152–53.

121. *Id.* at 1153.

122. *How Tagging Works*, FACEBOOK, https://www.facebook.com/about/tagging [https://perma.cc/Z92V-G6DQ] (last visited June 21, 2016).

123. *See* Grimmelmann, *supra* note 2, at 1156 ("Facebook's design encourages reciprocal behavior by making the gesture-and-return cycle visible and salient.").

124. *Id.* at 1157–58.

125. 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 RES. CTR. (Apr. 18, 2007), http://www.pewinternet.org/2007/04/18/friendship-strangers-and-safety-in-online-social-networks/ [https://perma.cc/RVR8-28HT].

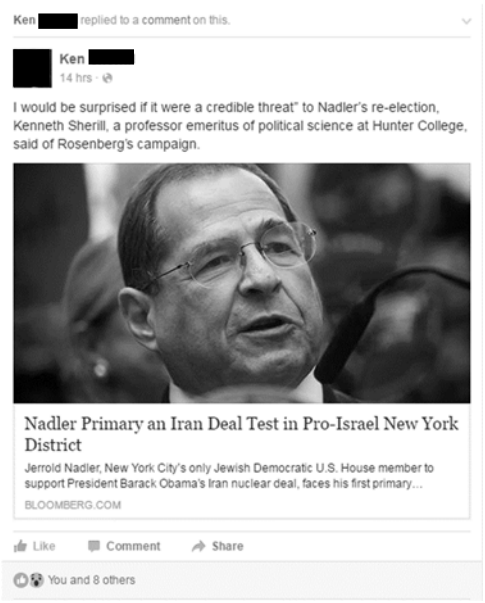
In a series of updates from April, 2015, through July, 2016, Facebook stepped up its strategy of leveraging trust to encourage us to share. More specifically, the News Feed algorithm was tweaked to give greater preference to posts and interactions from friends and family, pushing them to the top of Feed.[126] Facebook sold this change as a way to realize the platform's founding "idea of connecting people with their friends and family" and to keep us "connected to the people, places and things [we] want to be connected to."[127] That may be true, but no Facebook design change can be understood independent of the platform's insatiable appetite for user data. Privileging the posts of friends and family over the posts of third party publishers themselves may limit the reach of a naked post from Vocativ or Upworthy, but not when one of their videos is shared by a friend.[128] That is ideal for Facebook for two reasons. First, users tend to dislike seeing posts from third parties; second, under the new design, most third party content that users see will come through their trusted social networks of friends. This cues the trustworthiness of the post far better than any naked post from a publisher ever could.

126. Lars Backstrom, *News Feed FYI: Helping Make Sure You Don't Miss Stories from Friends*, FACEBOOK (June 29, 2016), http://newsroom.fb.com/news/2016/06/news-feed-fyi-helping-make-sure-you-dont-miss-stories-from-friends/ [https://perma.cc/2GZ4-T35C]. Max Eulenstein & Lauren Scissors, *News Feed FYI: Balancing Content from Friends and Pages*, FACEBOOK (Apr. 21, 2015), http://newsroom.fb.com/news/2015/04/news-feed-fyi-balancing-content-from-friends-and-pages/ [https://perma.cc/5VMK-Z8UL] (describing how Facebook's updates prioritize content posted by friends that the user cares about the most).

127. Backstrom, *supra* note 126.

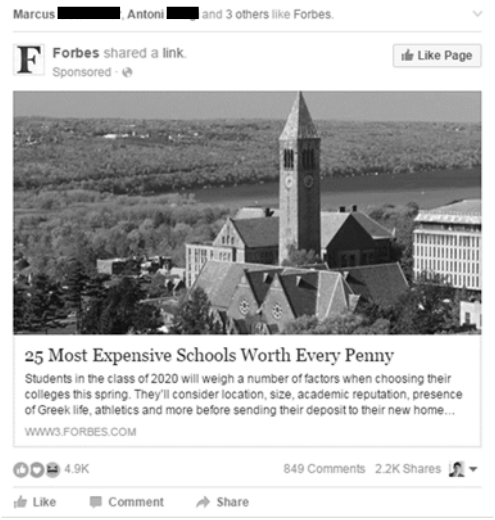
128. *See* Mike Isaac & Sydney Ember, *Facebook to Change News Feed to Focus on Friends and Family*, N.Y. TIMES (June 29, 2016), http://www.nytimes.com/2016/06/30/technology/facebook-to-change-news-feed-to-focus-on-friends-and-family.html [https://perma.cc/PHG2-HLLM] ("[C]ontent posted by publishers will show up less prominently in news feeds, resulting in significantly less traffic to the hundreds of news media sites that have come to rely on Facebook.").

Figure 1



As seen in Figure 1, member posts from inside and outside our networks 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 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." After an update to its design in July, 2016, Instagram does this, too. 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.

Figure 2



When applied to native advertisements in the News Feed, this tactic confuses and obscures, manipulating us into clicking on a third party's post. Native advertisements, or third-party links that are designed to look like social posts, also appear on our News Feeds. Like the social posts of our friends, these advertisements, like the one in Figure 2, 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 advertisement about the new Spring line. And "Alice, Barry, Catherine, and 22 others like Adidas" may appear above an advertisement for the newest Adidas running shoe. The information about our friends, not the advertisement, is the first thing we see. The only thing that distinguishes these advertisements from our friends' social posts is the word "Sponsored," written in light grey text under the name of the company and sandwiched between the advertisement's much larger graphic content and Facebook's bolded trust cue.

These tactics exploit the relationship between particular social trust and the propensity to share: we are more likely to accept a "Friend Request" from someone with whom we share mutual friends, just like we are more likely to click on a link that our friends, especially our close friends, have also clicked. And when we do click on the link, we send data about our preferences to Facebook and its third party partners.

B. Steps Forward

If they are accurate portrayals of our friends' behavior, Facebook's notifications on social posts can cue trust and help us keep on top of social interaction. But when used to obscure the difference between social and commercial posts and between social interaction and

endorsement, exploiting the trust-sharing link can be deceitful and coercive. This problem can be solved in two different ways: changes in design or regulatory enforcement. Since platforms like Facebook may lack the incentives to change these design tactics,[129] regulators, particularly the Federal Trade Commission (FTC) and state attorneys general,[130] may need to start paying attention to how social platforms that collect user data deploy information they know about us and our friends.

1. Privacy by Design

Privacy by design is the notion that we should engineer our online platforms from the ground up with privacy in mind.[131] As FTC Commissioner Julie Brill once noted, it involves "baking" user control over personal data into the underlying structure of a built online environment.[132] This could include building databases with internal cybersecurity measures, incorporating privacy into everyday corporate practice, placing limits on data collection, and everything in between.[133] Facebook has a long way to go before it could be seen as a privacy-by-design adopter. But it could start by designing its News Feed to be more transparent about native advertising. The word "sponsored," which is confusing to many users,[134] should be larger and more obvious, not obscured by a light-colored font and other, richer content. The Associated Press mobile application (Figure 3) 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 reserve the positioning of the picture and headline, they are also prefaced by a bright yellow bar that reads "Paid for by . . .". Furthermore, a "just in time" pop up

129. Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1436 (2011).

130. *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, NOTRE DAME L. REV. (forthcoming 2017) (manuscript at 7–8), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2733297 (proposing that attorneys general should encourage laws that ban deceptive commercial acts).

131. ANN CAVOUKIAN, PRIVACY BY DESIGN 1 (2013), https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-primer.pdf [https://perma.cc/6RAF-G5YG] ("[Privacy by design] anticipates and prevents privacy invasive events before they happen.").

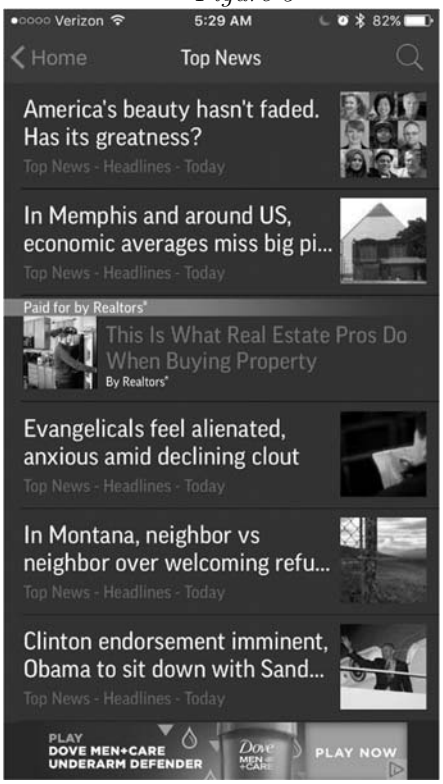
132. Julie Brill, Commissioner, Fed. Trade Comm'n, Opening Remarks at W3C Meeting at 1 (Apr. 11, 2012), http:// www.ftc.gov/speeches/brill/120411w3cremarks.pdf [https://perma.cc/F7CA-QP69].

133. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 44 (2010) (proposing a framework for how companies can protect consumer privacy).

134. Wojdynski & Evans, *supra* note 12, at 162, 164–65.

privacy notification could notify users that a click on sponsored links will release some information to third parties.

Figure 3



2. Federal Regulatory Responses

Ultimately, privacy by design would require a change in culture at Facebook. The social network will likely neither adopt these mitigating design strategies nor voluntarily drop the practice of using trust cues on native advertisements. This leaves an opening for regulators. The FTC, which stepped into the role of de facto privacy regulator in the late 1990s pursuant to its authority in Section 5 of the FTC Act,[135] and state attorneys general, arguably more active and more effective privacy

135. 15 U.S.C. § 45(a)(1) (2012) ("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) (2012) ("The Commission is hereby empowered and directed to prevent [others] . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.").

regulators than the FTC,[136] could step in.[137] By taking users' names and placing them on top of an advertisement in others' News Feeds, 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.[138]

This type of behavior is similar to unfair and deceitful design tactics that have previously been subject to FTC enforcement. As a threshold matter, it is clear that manipulative design can be regulated. In *In re Sony BMG Music Entertainment*,[139] for example, Sony had designed its CDs to install digital rights management, or DRM,[140] software on its users' computers in such a way as to make it unreasonably difficult for users to remove or even know about it.[141] Sony also designed its bundled media player to automatically send user information to Sony's servers

136. Citron, *supra* note 130 (manuscript at 37).

137. 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, 585–86, 588 (2014). As the authors point out, the FTC has developed a broader view of unfair or deceptive practices, including, for example, "deception by omission," "inducement" to share personal information, and "pretexting," to name just a few. *Id.* at 630–33. Their persuasive argument is that "through a common law-like process, the FTC's actions have developed into a rich jurisprudence that is effectively 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.

138. 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 Complaint for Damages at ¶¶ 32–35, Fraley v. Facebook, 830 F. Supp. 2d 785 (N.D. Cal. Dec. 16, 2011) (No. 11–CV–01726–LHK) (arguing that Facebook misleads its users regarding sharing information with companies).

139. Complaint, Sony BMG Music Entm't, F.T.C. File No. 062 3019, No. C-4195, 2007 WL 1942983 (F.T.C. June 28, 2007) [hereinafter Sony Complaint].

140. DRM is a catch-all term for technological measures copyright owners use to control how their content is used and distributed. *See* Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575, 575 (2003) ("In an effort to control the proliferation of unauthorized copies, and to maximize profit from information goods distributed over the Internet, copyright owners and their technology partners are designing digital rights management ('DRM') technologies that will allow more perfect control over access to and use of digital files.").

141. Sony Complaint, *supra* note 139, at ¶ 20.

to be used to targeted advertisements.[142] Per the FTC's complaint against Sony, these tactics constituted unfair design practices that misled, deceived, and constrained users.[143] The FTC made a similar case for misleading design against Frostwire. Frostwire developed peer-to-peer file sharing software that when downloaded onto a computer, automatically enabled other users on the network to search for files on that computer.[144] But the interface included a "Frostwire Setup Wizard" that was designed to give users the impression that they could control which files could and could not be searchable.[145] In reality, users had limited control. As the FTC noted, Frostwire had designed its software to, among other things, designate pre-existing files for sharing and make it extraordinarily difficult to opt out.[146]

The FTC has also moved against companies that used design to deceive their users into handing over personal information. In *FTC v. Hill*,[147] a particularly egregious case, the FTC argued that Hill engaged in a manipulative phishing scheme by designing fake websites to masquerade as AOL to trick people into disclosing log in and credit card information.[148] Hill used AOL marks and logos and made the website look like an AOL-affiliated page in all respects.[149]

The elements of Facebook's design that use trust to manipulate us into sharing information with advertisers suffer from the same faults underlying the *Sony*, *Frostwire*, and *Hill* actions. At the heart of the complaints were the FTC's objections to designing a platform to not only to erode user privacy, but also to make it difficult for users to recapture control over the use of their data. *Sony* focused on manipulative default settings. In addition to deceptive defaults, *Frostwire* challenged the design of an entire interface that made it seem like users

142. *Id.* at ¶ 11.

143. *Id.* at ¶ 21. *See also* Solove & Hartzog, *supra* note 137, at 642 (explaining instances where the FTC found website and software designs unfair).

144. Complaint for Permanent Injunction and Other Equitable Relief at 3, FTC v. Frostwire, LLC. (S.D. Fla. Oct. 12, 2011) (No. 1:11-cv-23643), http://www.ftc.gov/enforcement/cases-proceedings/112-3041/frostwire-llc-angel-leon [https://perma.cc/HS2F-7VAZ] [hereinafter Frostwire Complaint].

145. *Id.* at 5–11.

146. *Id.* at 13–14.

147. FTC v. Hill (S.D. Tex. Mar. 22, 2004) (No. 03-5537), http://www.ftc.gov/sites/default/files/documents/cases/2004/03/040322cmp0323102.pdf [https://perma.cc/EQ54-CBMS].

148. Complaint for Permanent Injunction and Other Equitable Relief at 10–11, FTC v. Hill (S.D. Tex. Mar. 22, 2004) (No. 03-5537), http://www.ftc.gov/sites/default/files/documents/cases/2004/03/040322cmp0323102.pdf [https://perma.cc/EQ54-CBMS].

149. *Id.* at 5.

were erecting privacy controls when, in fact, they were being misled into a false sense of security. *Hill* involved using design to evoke trust and manipulate sharing. Facebook's manipulative behavior may not be as overt as Hill's, but the platform uses default settings and design to turn social interaction into endorsements and elicit sharing of personal information while keeping users in the dark. By leveraging trust among users to make advertisements look like social posts, Facebook leads its users into a false sense of trust and security when none exists. Its News Feed design, perhaps more subtly than the designs of Sony's DRM, Frostwire's P2P software, and Hill's fake websites, still wrests control over personal data in a coercive, hidden way.

3. State Attorneys General

Attorneys at the FTC are not the only ones who could maneuver Facebook into redesigning its News Feed to remove trust cues from advertisements. As Danielle Citron argues, state attorneys general may actually be better equipped to protect personal privacy, in general.[150] They have cemented and changed privacy norms throughout the spectrum of privacy matters, including transparency of data use practices, data breach notification, giving consumers real choice, restricting what companies can do with data, and protecting and respecting youth and sexual privacy.[151] And they have considerable power and flexibility to limit Facebook's and other platforms' manipulation of trust to coerce users to share.

Citron notes that state attorneys general are more nimble privacy enforcers: they are free of Byzantine federal bureaucracies, have large teams of lawyers with privacy expertise, and have a wider array of state privacy laws at their disposal.[152] In particular, state attorneys general have several regulatory tools that may make them more effective privacy protectors than federal regulators. First, because they play a significant role in drafting state privacy legislation,[153] state attorneys general could lead the charge to either apply existing laws to online platforms' manipulation of trust or write new ones.

150. Citron, *supra* note 130 (manuscript at 3–4).

151. *Id.* (manuscript at 18–34).

152. *Id.* (manuscript at 4).

153. Citron notes that Delaware has adopted four privacy laws proposed by its attorney general, Matt Denn. *Id.* (manuscript at 12 n.54). And many state attorneys general have testified before federal committees concerning the adoption of federal privacy laws. *See id.* (manuscript at 12–13, 55 n.322) (stating that state attorneys general routinely testify before congressional committees).

Illinois, for example, already has a right of publicity statute that prohibits the use of a person's name or photograph for the sale or advertisement of goods or services without consent.[154] It is that statute that encouraged a group of users of Groupon, a social e-commerce company that sells vouchers, or "Deals," for discounts at participating businesses, restaurants, and other establishments, to challenge that company's manipulation of trust. According to the complaint in the putative Groupon class action, 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.[155] At times, Groupon has also included pictures of consumers who were ostensibly at the location.[156] But rather than asking consumers or the participating business for these photos, Groupon allegedly scraped them from Instagram's application programming interface by making a request for Instagram photos "tagged" with the name of the business in the Deal.[157] 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,[158] 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.[159] 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 particular social trust. Its tactics deceive and manipulate users into thinking the Deal is trustworthy when, in fact, it might not be.

154. 765 ILL. COMP. STAT. § 1075/30(a) (West 2016).

155. Class Action Complaint and Demand for Jury Trial at 3, Dancel v. Groupon, (Ill. Cir. Ct. Cook Cnty. Feb. 5, 2016) (No. 2016CH01716), 2016 WL 464011 (hereinafter, "Groupon Complaint").

156. *Id.* at 5.

157. *Id.* at 5–6.

158. *Platform Policy*, INSTAGRAM https://www.instagram.com/about/legal/terms/api/ [https://perma.cc/Z3CV-XQN3] (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, https://help.instagram.com/206875879493855 [https://perma.cc/2FWY-K4FF] (last visited Apr. 4, 2016) ("No. You own your own photos and videos. Advertising on Instagram doesn't change this.").

159. Groupon Complaint, *supra* note 155, at 6–7.

Facebook's manipulation may be subtler, 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. State attorneys general may be able to address those concerns through legislation and associated litigation.[160]

Another weapon in the hands of state attorneys general is persuasion, a tool used most effectively to protect privacy by California Attorney General Kamala Harris.[161] AG Harris has convened task forces with business leaders, come to informal business agreements with technology companies from Google to Yahoo to Facebook, and issued extensive best practice guides to help flesh out state statutory requirements.[162] And industries often have significant incentives to comply: adherence to agreements negotiated in good faith stave off expensive lawsuits that destroy good will with policymakers and damage user confidence.[163] Similar guidance on appropriate and inappropriate uses of trust cues on social networks—social posts versus native advertisements—and on how to design native advertisements to sufficiently contrast with the balance of the platform could help nudge Facebook to change its ways.[164]

---

160. *See* Citron, *supra* note 130 (manuscript at 15) (identifying "litigation" as another weapon for state attorneys general to use to protect privacy).

161. Citron reports on several other state attorneys general, including those in Vermont, Massachusetts, and Connecticut, who have used task forces and best practice guides to cajole companies into protecting privacy, but Attorney General Harris has been a pioneering leader. *Id.* (manuscript at 13–14).

162. *Id.* (manuscript at 30–31). AG Harris's *Privacy on the Go: Recommendations for the Mobile Ecosystem*, a guide for app developers and platform providers to provide mobile app users with adequate privacy protections, and *Making Your Privacy Practices Public*, a practice guide on California's Online Privacy Protection Act, are particularly notable examples. KAMALA D. HARRIS, ATT'Y GEN., CAL. DEP'T OF JUSTICE, PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM (2013), http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf [https://perma.cc/8BHK-WVS2]; KAMALA D. HARRIS, ATT'Y GEN., CAL. DEP'T OF JUSTICE, MAKING YOUR PRIVACY PRACTICES PUBLIC (2014), https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf [https://perma.cc/J6HW-F45H].

163. *See* Citron, *supra* note 130 (manuscript at 16) (explaining the incentives companies have to follow relevant regulatory standards).

164. Notably, the FTC has already issued native advertising guidance. *E.g.*, *Native Advertising: A Guide for Businesses*, FED. TRADE COMM'N (2015), https://www.ftc.gov/tips-advice/business-center/guidance/native-advertising-guide-businesses [https://perma.cc/UN3U-894A]. Evidence of their success is mixed, at best. State attorneys general, given their strong

Conclusion

This Article has presented data suggesting that we share when we trust. In particular, we tend to be more willing to share information online when we know that our friends have also shared similar information. This confirms and extends the current social science research on the propensity to share. Scholars have shown that, with respect to e-commerce websites, higher levels of trust in the website translate into a greater willingness to share. Previous studies have also shown that sharing decisions are contextual and, in particular, heavily influenced by the knowledge that other users have shared. This research suggests that sharing is indeed contextual and is particularly influenced by users' trust in others they know well. It adds to our understanding of trust and sharing by suggesting that the relationship holds for social networking websites and by highlighting the importance of trusted users in our decisions to share.

That a user's propensity to share can be nudged by creating a community of sharers that a user trusts explains why Facebook notifies its users about their friends' likes, dislikes, and online activity. These nudges may enhance user experiences online because they are roughly equivalent to personal recommendations from trusted sources. But they can be used to coerce, mislead, and deceive users, as well. Given that the connection between particular social trust and the propensity to share has been underappreciated to date, misuse of social network data has escaped privacy regulation. This research, then, opens up a new path for the FTC and state attorneys general to protect consumers from the online misuse of their information.

history in setting privacy norms, need to step in to ensure compliance with substantive and design requirements over native advertisements.