Trust: Privacy in the Digital Age

Ari Ezra Waldman[1]

Introduction

In May 2016, several Danish researchers released data on 70,000 users of the dating website, OKCupid. Those of us who have tried online dating know that profiles on OKCupid (or Match, JDate, or eHarmony) are rich in sensitive personal information. The researchers published much of it: usernames, age, gender, and location, as well as sexual orientation, fetishes, religious views, and more. Given the breadth of that information, it wouldn't take much to figure out the identities of those involved. And the researchers neither obtained consent nor anonymized the data.[2]

Mining personal data for scholarship is nothing new.[3] Online retailers do it all the time, as well, gathering everything from our browsing histories to Facebook "likes" to target us with advertisements they think we want to see.[4] Google tailors its search results based on what it learns from our behavior across platforms, sometimes discriminating against us in the

---

1 Associate Professor of Law and Director, Innovation Center for Law and Technology, New York Law School. Affiliate Scholar, Princeton University, Center for Information Technology Policy. Ph.D., Columbia University; J.D., Harvard Law School. Much of this essay is taken from the author's forthcoming book, *Privacy As Trust: Information Privacy in an Information Age*, scheduled to be published in 2018 by Cambridge University Press.

2 Woodrow Hartzog, *There Is No Such Thing as "Public" Data*, Slate (May 19, 2016, 9:15 AM), http://www.slate.com/articles/technology/future_tense/2016/05/okcupid_s_data_leak_shows_there_s_no_such_thing_as_public_data.html.

3 Taylor Hatmaker, *In 2006, Harvard Also Conducted a Facebook Study That Went Too Far*, The Daily Dot (July 12, 2014 6:55 AM), https://www.dailydot.com/debug/facebook-t3-study-tastes-ties-time/. *See also* Michael Zimmer, *"But the Data is Already Public": On the Ethics of Research in Facebook*, 12 Ethics Inf. Tech. 313 (2010).

4 Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. Times Mag. (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

process.[5] Data brokers amass vast collections of information about us gleaned from across the Web and sell it to the highest bidder. Facebook is steaming ahead with frighteningly accurate facial recognition technology based on the millions of photos we upload for our friends.[6] And marketers are using our buying patterns and GPS technology to send sale notifications directly to our phones when we pass a brick-and-mortar store.[7]

Under current law in the United States, almost anyone, whether they are over eager researchers or online advertisers, can use this data because, as a matter of law and social practice, the information is considered already public. We shared our data the moment we signed up for an account, browsed the Internet, or bought a book online.[8] We cannot put that genie back in the bottle, the argument goes, because we let it out a long time ago. Animating this approach is an outdated conception of privacy that is ill equipped to handle the disclosure demands of the digital age. We need

---

5 *See, e.g.*, Latanya Sweeney, *Discrimination in Online Ad Delivery*, Comm. ACM, May 2013, at 44.

6 Naomi Lachance, *Facebook's Facial Recognition Software Is Different from the FBI's. Here's Why*, NPR: All Tech Considered (May 18, 2016, 9:30 AM), http://www.npr.org/sections/alltechconsidered/2016/05/18/477819617/facebooks-facial-recognition-software-is-different-from-the-fbis-heres-why.

7 Chris Frey, *Revealed: How Facial Recognition Has Invaded Shops—and Your Privacy*, Guardian (Mar. 3, 2016, 07.01 EST), https://www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto.

8 The "it's already public" defense is remarkably common. For example, the FBI has argued that its agents do not need warrants to set up stingrays, or decoy cell towers, to capture our cellphone location because they are only collecting public information in public places. *See* David Kravets, *FBI Says Warrants Not Needed to Use "Stingrays" in Public Places*, Ars Technica (Jan. 5, 2015, 2:25 PM), http://arstechnica.com/tech-policy/2015/01/fbi-says-search-warrants-not-needed-to-use-stringrays-in-public-places; *see also* Smith v. Maryland, 442 U.S. 735 (1979). Perpetrators of so-called "revenge porn," or the publication of intimate or graphic photos of others without their consent, often justify their behavior by stating that the victim sent them the photos in the first place. *See* Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 Wake Forest L. Rev. 345, 346 (2014). Similar arguments are deployed in "up skirt" photo cases, too: snapping pictures of a woman's body underneath her skirt cannot be an invasion of privacy, the theory goes, because the pictures were taken in public places. *See* Justin Jouvenal & Miles Parks, *Voyeur Charges Dropped Against Photographer at Lincoln Memorial*, Wash. Post (Oct. 9, 2014), https://www.washingtonpost.com/local/crime/voyeur-charges-dropped-against-upskirt-photographer-at-lincoln-memorial/2014/10/09/7dc90eac-4ff5-11e4-aa5e-7153e466a02d_story.html.

to change the way we think about privacy so we can better leverage law to protect it in a modern world.

As I have argued elsewhere, trust between social actors is a primary factor in our decision to share personal information with others.[9] Because we share when we trust, I argue that we should start talking about, thinking through, and operationalizing information privacy as a social norm based on trust. In the context of information sharing, trust gives us the ability to live with, yet minimize vulnerability by relying on expectations of confidentiality and discretion. So, when we share information with others in contexts of trust, that information should be protected as private. I call this argument privacy-as-trust, and it helps to adapt privacy to the digital age.

I. A New Way of Looking at Privacy

Privacy is an inherently social concept. The very idea of privacy presumes that we exist in both formal and informal relationships with others: privacy only matters after we share within those relationships. When making sharing decisions, we rely on and develop expectations about what should happen to our information, thus integrating privacy into our lives relative to other people.[10] As the law professor Robert Post described, privacy norms "rest[] not upon a perceived opposition between persons and social life, but rather upon their interdependence."[11] Privacy, then, is socially situated. It is not a way to withdraw or to limit our connection to others. It is, at its core, about the social relationships governing disclosure between and among individuals and between users and the platforms that collect, analyze, and manipulate their information for some purpose.[12]

For example, when we share the fact that we are HIV-positive with the 100 members of an HIV support community, we may expect a far greater degree of confidentiality and discretion from them than from just two ac-

9 Ari Ezra Waldman, *Privacy, Sharing, and Trust: The Facebook Study*, 67 Case W. Res. L. Rev. 193 (2016).

10 Sandra Petronio, Boundaries of Privacy 3 (2002).

11 Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 Cal. L. Rev. 957, 959 (1989).

12 Ferdinand David Schoeman, Privacy and Social Freedom 8 (1992) (Privacy is a social norm that gives people the confidence to share and the ability to develop relationships in the process.).

quaintances at work. When we whisper secrets to a good friend, we expect confidentiality even without a written agreement. We share our bank account numbers with Bank of America's website and expect that it won't be shared with online marketers. And although we may recognize that using the Internet or joining a discount loyalty program requires some disclosure, we share our information with the expectation that it will be used for the specific purpose for which we shared it. What we share, with whom we share it, and how we share it matter. In other words, something about the social context of disclosure is the key to determining what is private and what is not.[13]

That key is trust. Trust is a resource of social capital between or among two or more persons concerning the expectations that others will behave according to accepted norms.[14] Trust is the "favourable expectation regarding other people's actions and intentions,"[15] or the belief that others will behave in a predictable manner according to accepted contextual norms. For example, if Alice asks her friend Brady to hold her spare set of keys, she trusts Brady will not break in and steal from her; friends do not break in to friends' homes. When an individual speaks with relative strangers in a support group like Alcoholics Anonymous (AA), she trusts that they will not divulge her secrets; AA members are bound to keep confidences. Trust, therefore, includes a willingness to accept some risk and vulnerability toward others to grease the wheels of social activity.[16] And if I never trusted, my social life would be paralyzed. As Niklas Luhmann stated, trust begins where knowledge ends.[17] I cannot know for certain that my neighbor will not abuse her key privileges or that my fellow support

13 Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 Wash. L. Rev. 119 (2004). *See also* Helen Nissenbaum, Privacy in Context: Technology, Privacy, and the Integrity of Social Life (2010).

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

15 Guido Möllering, *The Nature of Trust: From Georg Simmel to a Theory of Expectation, Interpretation and Suspension*, 35 Sociology 403, 404 (2001); *see also* J. David Lewis & Andrew Weigert, *Trust as a Social Reality*, 63 Soc. Forces 967, 968 (1985).

16 Niklas Luhmann, Trust and Power 4 (1979).

17 *Id*. at 33–34; *see also* Patricia M. Doney et al., *Understanding the Influence of National Culture on the Development of Trust*, 23 Acad. Mgmt. Rev. 601, 603 (1998).

group members will keep my confidences, but the norms of those contexts tell me that they will.

Trust is the expectation that people will continue to behave according to those norms. Therefore, trust allows us to interact with and rely on others. It mitigates the vulnerability and power imbalance inherent in disclosure, allowing sharing to occur in the first place. Put another way, disclosures happen in contexts of trust, and trust is what's broken when data collection and use go too far.

Trust is what defines private contexts. Trust also mitigates the vulnerabilities inherent in disclosure. We are vulnerable to data collectors because we share a lot with all of them. They know a lot about us, down to the number of seconds our cursor hovers over a button, and releasing what they know could harm us. Furthermore, they have the money and manpower to aggregate information about our wants and needs, but we know nothing about the algorithms they use to analyze that data and predict our behavior. Data sharing, therefore, creates vulnerability and an imbalance of power. Elsewhere, as in doctor-patient or attorney-client relationships, where significant disclosures create similar power imbalances, we manage those risks with strong trust norms and powerful legal tools that protect and repair disclosure relationships. Reinvigorating information privacy in the digital age requires similar norms and legal weapons, as well. Privacy-as-trust matches the way we think about privacy with the power relationships that data sharing create.

Information privacy, I argue, is really a social construct based on trust between social sharers, between individuals and Internet intermediaries, between groups of people interacting online and offline, broadly understood. And because trust both encourages the sharing and openness we need in society and because breaches of privacy are experienced as breaches of trust, privacy law—the collective judicial decisions, legislative enactments, and supporting policy arguments regulating disclosures, searches and seizures, data aggregation, and other aspects of informational knowledge about us—should be focused on protecting and repairing relationships of trust. In short, the only way to reestablish the balance of power between sharers and data collectors is to leverage law to enforce disclosure's trust norms: one can be held liable for invasion of privacy if he further disseminates information that was originally shared in a context that manifests trust.

II. Applying Privacy-As-Trust: A Case Study

United States privacy law today is, for the most part, structured around concepts of autonomy, choice, and individual rights.[18] Judges deny recovery even when data collectors misuse our information because we supposedly made the free and voluntary choice to share our data in the first place.[19] Therefore, we assumed the risk that our information could be further disseminated and shared.[20] Previously disclosed information is, in this view, no longer private. And on the assumption that we make rational privacy and disclosure decisions, federal and state privacy laws focus much of their energy on requiring data collectors to draft and publish privacy policies that list, in tortuous detail, the companies' data use practices.[21] Were it not for the Federal Trade Commission's robust privacy enforcement, data collectors would have few, if any other responsibilities with respect to our data after disclosure.

Privacy-as-trust would reorient privacy law away from a narrow focus on individual choice to disclosure relationships. In this section, I briefly discuss one example of what that means. Privacy law is a multifaceted animal; it is, among others things, a collection of common law responsibilities, court decisions, federal and states statutes, and regulatory enforcement actions that manages the rights and responsibilities of citizens and data collectors alike. This section uses one case study—the legal obligations data collectors have to consumers—to tease out some of the effects of privacy-as-trust on one facet of privacy and information law. Overall, the result of approaching privacy law as a protector of trusted relationships is to more effectively protect privacy in an information age where data sharing is inevitable, ongoing, and extensive.

---

18 Ari Ezra Waldman, *Privacy As Trust: Sharing Personal Information in a Networked World*, 69 U. Miami. L. Rev. 559, 565-85 (2015).

19 There are too many examples of this to list here. *See, e.g.*, Dwyer v. American Express Co., 652 NE.2 d 1351 (Ill. App. Ct. 1995); Gill v. Hearst Pub., Co., 253 P. 2 d 441 (Cal. 1953); *In re* Nw. Airlines Privacy Litig., No. Civ. 04-126, 2004 WL 1278459 (D. Minn. June 6, 2004).

20 Smith v. Maryland, 442 U.S. 735, 744 (1979).

21 *See* Ari Ezra Waldman, *Privacy, Notice, and Design*, 20 Stanford Tech. L. Rev. 129 (2018).

A. The Current Approach: Notice and Choice

Companies that collect, aggregate, analyze, and share our information have considerable power over us. But under current United States law, their responsibilities are minimal, their power essentially unlimited. That is because our relationship to data collectors is based on principles of privacy-as-autonomy. Although the rules vary to some extent by industry,[22] the general approach is the same: on the theory that we have the right to decide for ourselves how and when to disclose our information, data collectors are required to provide us with both a comprehensive list of their data use practices and the opportunity to opt out and use another platform. This regime is called "notice and choice," and it is woefully inadequate.

As a governing legal regime, notice-and-choice is self-explanatory. Companies that collect our data are supposed to tell us what information they collect, how and for what purpose they collect it, and with whom they share it. That's the notice part. We then have the opportunity to opt out.[23] That, or the option to use another platform, is the choice.

Notice-and-choice makes sense as the limits of platform responsibility if we understand privacy through a lens of autonomy and choice. At its core, notice-and-choice is a doctrine of informed consent premised on autonomous decision-making: provide us with all the information we need in a privacy policy and allow us the freedom to make our own informed decisions. If companies disclose the details of their data use practices, the argument goes, disclosure decisions will be rational exercises of our power to exercise control over our information.[24]

---

22 The Health Insurance Portability and Accountability Act (HIPAA), for example, governs the collection, storage, and sharing of certain types of health and medical information. The Children's Online Privacy Protection Act (COPPA) applies to platforms that collect information about children 13-years-old or younger. And the Gramm-Leach-Bliley Act sets out rules for information management for some financial institutions. These statutes have somewhat different rules, with each imposing additional restrictions on data sharing in certain contexts.

23 Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 592 (2014).

24 *See* Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 Notre Dame L. Rev. 1027, 1049 (2012).

But notice-and-choice doesn't work. We do not make perfectly rational disclosure decisions regardless of what notice-and-choice may presume.[25] The law ignores our embodied experience and the contextual nature of privacy expectations.[26] What's more, notice-and-choice is meaningless in a world on ongoing data collection. As several chief privacy officers have said, concepts like "notice" and "consent" play "limited role[s]" in the ways their companies approach privacy questions because users cannot be expected to continuously evaluate their disclosure preferences over time.[27]

Notice-and-choice is also hopelessly underinclusive. It reflects an arbitrary and selective approach to the Fair Information Privacy Principles, which also included limitations on data collection, security requirements, a rejection of black boxes, user rights to data, and robust accountability policies.[28] There are administrative critiques, as well: it is difficult for companies to comply with a patchwork of laws, including the innumerable state laws governing data privacy, that apply to some information in the hands of some entities some of the time.

B. A New Approach: Trust

If we understood privacy as protecting relationships of trust, the obligations of data collectors would be different. Rather than limiting corporate responsibility to giving us a list of data use practices for rational privacy decision-making, privacy-as-trust recognizes that data collectors are being

---

25 *See* Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy?*, *in* Digital Privacy 363, 363–64 (Alessandro Acquisti et al. eds., 2008); Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, 3 IEEE Security & Privacy 26 (2005).

26 "Embodied" experience refers to the phenomenological and pragmatic idea that things like comprehension, understanding, and truth are only possible through lived experience as mediated by the social structures around us. *See, e.g.*, Maurice Merleau-Ponty, Phenomenology of Perception xi (Ted Honderich ed., Colin Smith trans. 1962). It was applied to the context of cyberspace by Julie Cohen. *See, e.g.*, Julie E. Cohen, Configuring the Networked Self: Law, Code, and the Play of Everyday Practice 34-31 (2012); Julie E. Cohen, *Cyberspace As/And Space*, 107 Columb. L. Rev. 210, 226-35 (2007).

27 Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 Stan. L. Rev. 247, 266–267 (2011).

28 Org. for Econ. Co-operation & Dev., OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 14–16 (2001).

entrusted with our information. Therefore, they should be held to a higher standard than mere notice. They are, in fact, fiduciaries with respect to our data, and should be obligated to act in a trustworthy manner. This argument, developed most recently and comprehensively by Yale Law School Professor Jack Balkin, follows directly from reorienting privacy law toward relationships of trust.

Fiduciary law is a common law construct, which means that judges developed it over time to respond to changing realities on the ground. Whereas contract law sets out the obligations of parties formally bound in voluntary agreements and tort law establishes the background rules of social interaction, fiduciary law focuses on a few special relationships that are based on trust and confidence. In short, a fiduciary has special obligations of loyalty and trustworthiness. A client puts his trust in a fiduciary, and the fiduciary has an obligation not to betray that trust. She must act in her client's interests, not in a way that harms him.[29] Estate managers, investment advisers, lawyers, and doctors are classic examples of fiduciaries: They handle their clients' money, secrets, and livelihoods under duties of loyalty and care.[30]

As Balkin explains, fiduciary duties are "duties of trust." Even the word "fiduciary" comes from the Latin word for "trust." And, as I argued in Chapter 5, "trust and confidence are centrally concerned with the collection, analysis, use, and disclosure of information."[31] Therefore, those that handle our personal information, whether doctors, lawyers, or an online social network, have "special duties with respect" to our information. These parties are "information fiduciaries."[32] Several other leading privacy law scholars agree. In *The Digital Person*, Daniel Solove argued that businesses that are collecting personal information from us should "stand in a fiduciary relationship with us."[33] And in a blog post at Concurring Opinions, the law professor Danielle Keats Citron suggested that a fidu-

---

29 Deborah A. DeMott, *Beyond Metaphor: An Analysis of Fiduciary Obligation*, 1988 Duke L.J. 879, 882.

30 Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U. C. Davis L. Rev. 1183, 1207-08 (2016).

31 *Id*.

32 *Id*. at 1208-09.

33 Daniel J. Solove, The Digital Person 102-03 (2004).

ciary relationship between data brokers and users would help fight the massive power imbalance online.[34]

All fiduciary relationships have two overarching similarities—namely, asymmetry and vulnerability. Doctors, lawyers, and investment managers have special skills that their clients do not. As much as we might fear hospitals, we can neither diagnose nor perform surgery on ourselves. Instead, we rely on physicians to perform these tasks. We also lack the ability to effectively monitor or evaluate our doctors' job performances. Because of these asymmetries, we are in a position of vulnerability vis-à-vis our fiduciaries: We put our information, our money, our health, and our fate in their hands.[35]

Companies like Facebook, Google, Uber, and Match.com should be considered information fiduciaries for the same reasons that doctors, estate managers, and investment analysts are considered fiduciaries. First, our relationship to these companies "involve[s] significant vulnerability." Traditional fiduciaries have special skills unavailable to their clients, just many Internet and technology companies. They know everything about us; trade secrecy keeps their algorithms hidden from us. They monitor every step we take online; we know little about how they process our information. Second, we are absolutely dependent on these companies. We cannot engage in modern life without the Internet, and our movements online are tracked as a matter of course.[36] Third, many Internet companies market themselves as experts in what they do: Facebook is the best and largest social connector,[37] Match.com calls itself "#1 in dates, relationships, and marriages,"[38] and Google is the dominant search engine and primary avenue to the World Wide Web for most Internet users.[39] And, fourth, these companies hold themselves out as trustworthy. As Kenneth Bamberger

34 Danielle Keats Citron, *Big Data Brokers as Fiduciaries*, Concurring Opinions (June 19, 2012), http://www.concurringopinions.com/archives/2012/06/big-data-brokers-as-fiduciaries.html.

35 Balkin, *supra* note 30, at 1216-17.

36 *Id*. at 1222.

37 Mark Zuckerberg, Facebook (Aug. 20, 2013), https://www.facebook.com/zuck/posts/10100933624710391.

38 Match, http://www.match.com/cpx/en-us/match/IndexPage (last visited Mar. 29, 2017).

39 Dan Frommer, *Google Has Run Away with the Web Search Market and Almost No One Is Chasing*, Quartz (July 25, 2014), http://qz.com/239332/google-has-run-away-with-the-web-search-market-and-almost-no-one-is-chasing.

and Deirdre Mulligan found during their groundbreaking research on privacy professionals, many leading chief privacy officers around the world felt that corporate privacy strategy was about maintaining user trust and being sufficiently flexible, adaptive, and forward looking to meet consumer expectations whatever they may be.[40] It was not about doing the least they could to prevent a lawsuit. Rather, they had to engage in ongoing management of risk and keep up with consumers' changing expectations.[41] Several CPOs talked about their jobs in fiduciary terms: they were "steward[s]" of data and "responsibl[e]" to consumers.[42] In short, several privacy leads saw their primary objective as creating and maintaining "the company's trusted relationship" with customers, employees, and society.[43]

Given this asymmetrical relationship, posting an obscure, inscrutable, and vague privacy policy is not enough to meet the fiduciary duties of care and loyalty. On top of the duty to inform, Balkin and the cyberlaw scholar Jonathan Zittrain propose "to adapt old legal ideas to create a new kind of law—one that clearly states the kinds of duties that online firms owe their end users and customers." The most basic of those duties is to "look out for the interests of the people whose data businesses regularly harvest and profit from." In other words, information fiduciaries should never act like "con men," inducing trust and then actively working against their users' interests. Balkin and Zittrain give the perfect example: Google Maps should not hold itself out as providing the "best" or "fastest" route from Logan International Airport to the Westin Copley and then deliver a route that drives passes an IHOP simply because IHOP paid Google $20.[44] Even if it never explicitly promised to offer users the fastest route on Google Maps, Google and other information fiduciaries should be held accountable when they induce trust in any way and then break it.

Balkin and Zittrain add several other obligations on top of not acting like con men. Companies "would agree to a set of fair information practices, including security and privacy guarantees, and disclosure of

40 Kenneth A. Bamberger & Deirdre K. Mulligan, Privacy on the Ground 59, 65, 67 (2015).
41 *Id*. 67, 68.
42 *Id*. at 66.
43 *Id*. at 67.
44 Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, Atlantic (Oct. 3, 2016), http://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346.

breaches. They would promise not to leverage personal data to unfairly discriminate against or abuse the trust of end users." And here's the kicker: "And they would not sell or distribute consumer information except to those who agreed to similar rules."[45] Or, as Balkin wrote, "[w]hat information fiduciaries may not do is use the data in unexpected ways to the disadvantage of people who use their services or in ways that violate some other important social norm." This is the essence of privacy-as-trust. As we discussed above, trust is a resource of social capital between two or more parties concerning the expectations that others will behave according to accepted norms.[46] We share information with others, including online data collectors, with the expectation that those companies will treat our data according to prevailing norms and promises. We experience the further sale or dissemination of our data to unknown third parties as violations of our privacy precisely because such dissemination breaches the trust that allowed us to share in the first place. We know nothing about those third parties, particularly their data use practices. Under the law of information fiduciaries, online data collectors would not be allowed to share the data they collect with third parties that do not comply with the same data privacy obligations.

Conclusion

Pundits have been writing privacy's obituary for years.[47] We have been told privacy is dying for so long that the average person on the street can be excused for thinking it died years ago, alone, gasping for breath.

Privacy is only dead if we think about it narrowly. We tend to confuse privacy with secrecy, or limit the private world to the constellation of inti-

---

45 *Id*.

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

47 Thomas Friedman, *Four Words Going Bye-Bye*, New York Times (May 21, 2014), https://www.nytimes.com/2014/05/21/opinion/friedman-four-words-going-bye-bye.html; Marshall Kirkpatrick, *Facebook's Zuckerberg Says The Age of Privacy is Over*, Readwrite (Jan. 9, 2010), https://readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_ov/; Polly Sprenger, *Sun on Privacy: 'Get Over It'*, Wired (Jan. 26, 1999 12:00 PM), https://www.wired.com/1999/01/sun-on-privacy-get-over-it/.

mate, sexual, or familial facets of our lives. Courts frequently (though not exclusively) do the same. We also tend to think about privacy spatially ("behind closed doors") or as the ability to exclude others from something by closing a window, locking a door, or stepping inside our homes.

In some ways, new technologies and the mandates of modern life have made this kind of privacy antiquated. It's hard to keep anything secret these days, especially since browsing the Internet is an information sharing event; our credit cards numbers, likes and dislikes, browsing histories, and purchasing patterns are collected, analyzed, and sold by websites, technology companies, and advertisers. This makes it difficult to control the flow of our information. What's more, disclosure is often a necessary prerequisite of modern social life and, for some, for access to legal rights and entitlements.

Even if we think that privacy ends at disclosure, the privacy-is-dead meme still doesn't make much sense. We still keep many things private. We wear clothes. We lock dairies. We warn others: "This stays between us." Social life functions with privacy. And yet, even these habits fail to tell the whole story. We do wear clothes, but not always in front of our romantic partners. We do write secrets down in diaries, but sometimes share them with our best friends, therapists, or relative strangers at support group meetings. We do make explicit requests for confidentiality, but often not when sharing with those with whom confidentiality is implied. In other words, we manage the flow of our information with selective disclosures based on contextual norms of trust.

So understood, privacy is very much alive. It is a fact of life so engrained in the social structure that we couldn't live without it. In my work, I try to show that privacy, at least in the information-sharing context, is not about separating from society, but rather about engaging with it on terms based on trust. We share when we trust, and we do so expecting that even though we shared information with others, it is not up for grabs for just anyone to hear, see, or use. We feel our privacy is violated when our trust is breached, like when we are induced to share or when our information is taken from one place and given to people or companies about which we know nothing. And we use trust to contextually manage our personae and the flow of our information in order to engage in social life. Information privacy, therefore, is really a trust-based social construct between social sharers, between individuals and Internet intermediaries, between groups of people interacting online and offline, broadly understood. As such, pri-

vacy law should be focused on protecting and repairing the relationships of trust that are necessary for disclosure.