

Consent (Still) Won't Save Us

Jasmine McNealy

A PROVOCATION AND AN ANALOGY

In late January 2016, the internet came abuzz with news of how one woman was dealing with unwanted attention on social media. Australian model Emily Sears, who at the time had more than 2 million followers on Instagram, had found a solution to men sending unsolicited “dick pics”¹ to her direct messages (DMs).² Instead of deleting the photos and simply blocking the accounts sending the DMs, Sears would alert the dick pic sender’s romantic partner, after finding their name or account information by searching through the sender’s Instagram account. In the alternative, Sears would reply to the sender with a photo of him with his girlfriend.³ Both contacting their partners and demonstrating that she knew their relationship status would prompt apologies.⁴ Sears and her friend Laura Lux, herself with more than six-hundred thousand followers, claimed that they send messages to the romantic partners of these men to fulfill their obligations under “girl code.”⁵ Lux explained to BuzzFeed:

So I sent her a message with a screenshot of our conversation telling her that I was really sorry, but I thought she deserved to know how her boyfriend was behaving towards other women. I know if the roles were reversed and it was my boyfriend sending that shit out, I would want to know.⁶

The perils of being a woman online has and continues to receive much needed attention as scholars across many disciplines and the mainstream media examine the impact and implications of internet misogyny.⁷ That the sending of dick pics, for example, is not at all abnormal, is deserving of further investigation.

But, although the study of the sending of unsolicited not-safe-for-work (NSFW) photos and other harassment is important, this chapter is not an examination of online sexual harassment or misogyny. Instead, it focuses on the issue of consent.

Both Sears and Lux claim that when they told the men that they would be informing their partners or other listed relatives about the sending of the dick pics, they would quickly receive an apology and sometimes a plea that they not go through with their plan to contact.⁸ A question, then, arises as to the expectations these men had for the information, in the form of a photo, sent to these strangers. Even if Sears and Lux had not forwarded the photos, could the men have expected that the shots of their penis would remain between them and the women? Surely, the men had consented to their bits being seen, at least by Sears and Lux. Where does that consent, then, end? On the other hand, by just existing online, or having amassed a following and a touch of celebrity, did Sears and Lux consent to being contacted? Even if they had consented to, perhaps, initial contact, how does one make the inference that they had consented to receiving unwanted or unsolicited photos (data). Finally, have the loved ones of the photo senders consented to being contacted and perhaps embarrassed by the disclosures?

The Sears and Lux anecdote demonstrates an ongoing issue with current data protection and data privacy regimes that focus on individual information control. The usual mechanism for this in data protection is notice and choice,⁹ which requires that organizations provide users with information about how their private data might be used and then to choose whether to accept the conditions.¹⁰ Individuals, using their limited understanding of the data ecosystem—what is collected, how it is used, who has access—decide whether to consent. This consent mechanism has proved insufficient for informing us and ensuring that organizations are clear about the expectations users have for their data. This chapter considers the boundaries of consent and the limitations on the continued use of information control as the grounding for data protection regulation, especially with the accelerated use of artificial intelligence and algorithmic decision systems.

ON INDIVIDUAL CONTROL: CONSENT AND ITS BOUNDARIES

In the West, many trace the foundations of privacy as individual control to Alan Westin's 1967 book *Privacy and Freedom*, in which he defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." This definition is used as a basis for many data protection regulations.¹¹ Data, information, however, is leaky; "it escapes in unexpected ways, be it through errors, hacks, or whistleblowing."¹² Data is also shared beyond the bounds of what an individual agrees or can possibly imagine. When the government can access this data from third parties like banks or utility companies, it is able to point to the "third-party

doctrine,” which in general states that law enforcement does not need a warrant to get information about an individual if that information is held by a third-party, as an excuse for why this kind of data access does not violate the 4th Amendment. When private organizations share information commercially, their activities are usually upheld as having been disclosed in the organization’s privacy policy or terms of service, to which the individual agreed.

Scholars have written much about the insufficiency of transparency and notice-and-choice architecture online. While transparency is a prerequisite for holding organizations accountable for data collection, usage, and sharing, it places the onus on users to be aware of all the possible ways that organizations might interact with data, of policing those interactions, and to understand the meaning of the organizational disclosures. These requirements are virtually impossible for even the savviest of technology users. Individuals do not have the time or bandwidth to make all the possible choice decisions that might arise in the use of web and app technology.

As further evidence of the reliance of the individual control theory of data protection, a familiar refrain is that those who do not want their information shared should simply not use the technology. This ignores that many technologies are deployed on individuals without their knowledge or consent. Schwartz identified three major problems with the continued use of individual control as privacy: the autonomy trap, the data seclusion deception, and the commodification illusion.¹³ In sum, these major problems with individual control illustrate that the individual can never be in total control of their data at all times based on power imbalances between the individual, organizations, and government agencies. Therefore, although choice is looked at as offering power to the individual about how their data might be used, choice does not offer complete control nor supervisory powers.

What does this mean for data interactions in the social media context? The Sears and Lux opening anecdote provides an illustration. Sears and Lux use Instagram, like many others, as a social media platform, a space for garnering attention for their personal brands. With this platform use, they accept interactions with other users. They have “consented” to these social interactions, along with the platform terms. That does not mean, however, that they have consented to all forms of contact, as demonstrated by their responses to receiving unsolicited photos. The problem is that they had no way of proactively controlling the kinds of interactions they would encounter. Consent, then, is both contextual and sociotechnical.

CONSENT AS CONTEXTUAL

The boundaries of consent, whether in personal or business relationships, are based on expectations for disclosure and use of information. This can be demonstrated in the personal realm in cases of invasion of privacy by public disclosure and revenge porn. Some courts have recognized an expectation of privacy in information shared with other people in certain instances in which a special rela-

tionship exists.¹⁴ *Miller v. Motorola, Inc.* offers an example of an invasion of privacy case decided based upon the relationship between individuals.¹⁵ Joy Miller sued her employer, Motorola, after the company's resident nurse disclosed her mastectomy surgery to her coworkers. In reversing the lower court's dismissal of the Miller's public disclosure claim, the Illinois appellate court found that Miller had an expectation of privacy in speaking with the medical professional.¹⁶

No exact calculus exists for determining when courts will find the kind relationship in which an expectation of privacy is present. At least one scholar, however, has called for a consideration of social network theory when examining if a plaintiff had a privacy in information disclosed to others.¹⁷ This would examine not the number of people in a particular group that the information has the potential to reach, but the possibility of the information reaching individuals outside of that group. Therefore, information would be considered private—the person sharing would have an expectation of privacy—even if the group is large, so long as the information remains confined to that group.¹⁸ Lior Strahilevitz enumerates three factors that predict whether information will remain among a particular group: the level of interest the information generates, the group's information sharing norms, and group structure and information flows.¹⁹ Although not expressly decided based upon a social network theory, *Multimedia WMAZ, Inc. v. Kubach* offers an opportunity to consider how a court will consider in group relationships and the impact on the reasonable expectation of privacy.²⁰

Kubach was an HIV-positive man who shared his status with around sixty people, including family members, friends, his doctor, and members of a support group. He also appeared on a television show after obtaining assurances from the producers that his identity would be hidden.²¹ The show's producers, however, failed to adequately hide his identity and he was recognizable to those in his community who became aware of his HIV-positive status. The court found that despite his having told his status to several people, an expectation of privacy in that information remained because his disclosure was to people who cared about him.²²

As Helen Nissenbaum argues, expectations related to consent, whether online or off, differ from how consent mechanisms actually behave.²³ The implications of this failure in the data context are particularly significant. Current notice and choices schemes seek to present a measure of control to users. At the same time, to have perfect transparency or notice, organizations would have to inform users of all the ways data are and might be collected, as well as all the ways that data are and might be used, and by whom. Even if this were possible, Nissenbaum points to the transparency paradox or, "transparency of textual meaning and transparency of practice conflict in all but rare instances."²⁴ Therefore, if organizations make finely detailed disclosures, users may not understand all the ways data are collected and used; if organizations instead choose to make disclosures understandable, the disclosures might not offer enough details so that the user might be adequately

informed to consent. Instead, she offers the system of contextual integrity as an alternative.

CONSENT AS SOCIOTECHNICAL

The system of contextual integrity recognizes that consent and privacy are intertwined with human social networks and patterns of communication.²⁵ Because of the humanity of data disclosure, traditional consent via notice and choice architecture fails to adequately deliver the kind of “control” that is necessary for consent to be at all meaningful. Further, human relationships, depending on the context, can add duties for the recipients of information disclosures. These duties can be related to confidentiality. Both the *Miller* and *Kubach* cases previously mentioned have elements of a less asserted, but related tort claim of breach of confidentiality. Breach of confidentiality, or breach of confidence, arises when the plaintiff can prove that the defendant owed her a duty of keeping information secret, and breached that duty.²⁶ Such a duty arises between a doctor and her patient,²⁷ and a lawyer and her client.²⁸ For such a duty to arise there must be “the assurance of secrecy and the reliance that it evokes,” which creates a special relationship between the parties.²⁹

Breach of confidence has been asserted outside of the patient/client–specialist, and familial realms. Andrew McClurg argues that intimate partner relationships evoke a similar duty of confidentiality.³⁰ The basis of such a right can be found in the culture, customs, and laws related to intimate relationships. The legal cases of *Griswold v. Connecticut*,³¹ *Eisenstadt v. Baird*,³² and *Lawrence v. Texas*,³³ according to McClurg, are foundational for the protection of the privacy in intimate relationships.³⁴

Breach of confidence has been proposed as a remedy in revenge porn cases.³⁵ The argument is that, as with privacy, expectations exist about the kind of information that will be kept confidential.³⁶ This information—including sexual photographs, information about past relationships, kinks, and the like—may be shared with partners based on trust that it will not be revealed to third parties. This trust, according to Ari Waldman, is embedded in the idea of social capital, and relies on the belief that individuals will conform to societal norms.³⁷ This provides support for the claim that consent has boundaries, and because of this, current consent mechanisms, including notice and choice, do not adequately recognize the limitations and expectations that human information disclosure carry.

BOUNDARIES OF CONSENT

Though perhaps not stated expressly at the time, both Sears and Lux had boundaries about how they would interact with data on Instagram. Although using the social media for their own personal purposes, and thereby consenting to how other users might communicate with them, they did not *de facto* consent to all kinds of communications. Instead, they had limitations on the content of the

communications they would accept. In this case, it seems that one boundary was set against other users sharing photos of their genitals. This would seem like a recognizable boundary. Yet, the women reported contacting the loved ones of multiple men who had sent dick pics, demonstrating how boundaries are often ignored and/or how some individuals lack awareness of those boundaries.

Until now, both the opening anecdote and the cases in support of my argument about the insufficiency of the notice and choice consent mechanism have been based on human-to-human information disclosure. Sears and Lux involved social media user interactions; both *Miller* and *Kubach* were cases involving the sharing of sensitive information within close networks. But data disclosure in human-to-organization or human-to-machine schemes follow much the same pattern and are replete with same dangers, if only amplified. Therefore, the current consent schemes in these areas, too, need to be changed. Current controversies in facial recognition technology illustrate the issues with continued reliance on consent.

In June 2022, Google settled a class action lawsuit brought under the Illinois Biometric Information Privacy Act (BIPA) for its use of facial recognition software in connection to its Google Photos product.³⁸ According to the original claim, Google's facial grouping tool automatically identified users' faces in photos and videos uploaded to Google Photos. The plaintiffs had brought the claim under BIPA, which prohibits the collection and storage of biometric data without informing the user, because the product did not ask for consent in violation of the law. Google agreed to settle the lawsuit for \$100 million and to provide notice about the facial grouping tool as required under the law.

Google is not, of course, the only organization that has run afoul of BIPA. Meta—Facebook—has had to field at least two state level lawsuits over its use of facial recognition software. In February 2021, Facebook settled a class action suit claiming its facial recognitions system violated BIPA by not complying with the law's notice and consent requirements.³⁹ In the settlement, Facebook agreed to pay \$650 million. In 2022, the state of Texas sued Meta, Facebook's parent company, for violating the state's privacy law through its repeated use of facial recognition technology.⁴⁰ The Texas suit centers Facebook's "tag suggestions" tool that encouraged users to affirm the suggested identity of people in a photo, which would then be connected to the identified person's profile. Facebook ended the use of the tool in 2021, but the lawsuit claims that the company collected data without consent, shared data with third parties, and did not destroy the data in a timely manner.

Perhaps the most recognizable facial recognition lawsuit settlement was that of Clearview AI, another class action lawsuit brought under BIPA. Unlike the Google and Facebook cases in which site users actively use a facial recognition tool, although without notice, in the case of Clearview, the organization was accused of scraping social media data, including photos, in violation of platform rules and without the permission of the data subjects.⁴¹ More than solely collecting

and storing this data, Clearview sold access to it voluminous database to many government, corporate, and other organizations.

These cases with “big tech” companies hinge on whether the organizations obtained adequate consent from users, while at the same time failing to recognize that simply consenting to use a site or a site’s tools is not blanket permission for the use of personal data for uses beyond the boundaries of the user’s imagination or realization. The Google and Facebook settlements leave little to analyze about how courts will consider bounds of consent in these facial recognition cases. The Clearview case demonstrates that even accepted bounds of consent in agreeing to the terms of use for a social media site are not enough to prevent the use and access of personal data by third parties. This should provide further evidence that consent or notice and choice are normative legal constructs that do not provide the kinds of data protection that individuals need against ever emerging ways of collecting, using, and exploiting personal data.

State laws like BIPA and state actions like that of Texas against Facebook may offer a small amount of relief to those in affected classes. But these suits again reflect a focus on individual choice—control of information. Although individual choice is important as a general matter, it does not stop organizations and organizational tools from interacting with personal data in ways that cross personal boundaries. What’s needed, instead, is the institution of a regulatory framework that prohibits certain data collection and sharing at the outset of any human–organization or human–machine interaction. Such a framework would assist individuals from being left without recourse if they had offered a measure of consent. Instead, this kind of framework would preclude certain business models and shut off certain kinds of data interactions.

NOTES

1. “Dick pics” are photographs of a human penis. See, e.g., “Dick Pic,” UrbanDictionary.com, <http://www.urbandictionary.com/define.php?term=dick+pic> (accessed, March 20, 2016).

2. Joyce Chen, *Australian Model Emily Sears Is Warning Girls about Guys Who Send Her Penis Pics*, US WEEKLY (Jan. 29, 2016), <http://www.usmagazine.com/celebrity-news/news/australian-model-emily-sears-is-warning-girls-about-guys-who-send-her-penis-pics-w162926>; Jay Hathaway, *This Model Deals with Unwanted Dick Pics by Contacting the Dicks’ Girlfriends*, NYMAG.COM (Jan. 29, 2016), <http://nymag.com/following/2016/01/how-a-model-deals-with-the-unwanted-dick-pics.html>; Madeleine Davies, *Model Responds to Unwelcome Dick Pics By Contacting Senders’ Girlfriends*, JEZEBEL (Jan. 29, 2016), <http://jezebel.com/model-responds-to-unwelcome-dick-pics-by-contacting-sen-1756022915>; Rossalyn Warren, *A Model Is Alerting Girlfriends of the Men Who Send Her Dick Pics*, BUZZFEED (Jan. 29, 2016), <http://www.buzzfeed.com/rossalynwarren/a-model-is-alerting-girlfriends-of-the-men-who-send-her-dick>.

3. Warren, *supra* note 2; Hathaway, *supra* note 2.

4. *Id.*

5. UrbanDictionary.com defines “Girl Code” as the guidelines that “girls most obey in order not to get kicked out of the community,” UrbanDictionary.com, <http://www.urbandictionary.com/define.php?term=Girl+Code> (accessed, June 17, 2022).

6. Warren, *supra* note 2.
7. Sarah Banet-Weiser & Kate M. Miltner, *#MasculinitySoFragile: Culture, Structure, and Networked Misogyny*, 16 FEM. MEDIA STUD. 171 (2016); Gender Stereotypes, Aggression, and Computer Games: An Online Survey of Women (Feb. 1, 2005), <http://online.liebertpub.com/doi/abs/10.1089/cpb.2004.7.714>; Jessica Megarry, *Online Incivility or Sexual Harassment? Conceptualising Women's Experiences in the Digital Age*, 47, Part A, WOMEN'S STUD. INT. FORUM 46 (2014); *Sexual Harassment in Online Gaming Stirs Anger*, NEW YORK TIMES, <https://www.nytimes.com/2012/08/02/us/sexual-harassment-in-online-gaming-stirs-anger.html>; Jerry Finn & Mary Banach, *Victimization Online: The Downside of Seeking Human Services for Women on the Internet*, 3 CYBERPSYCHOL. BEHAV. 785 (2000); *Women and the Internet: Promise and Perils* (July 5 2004), <http://online.liebertpub.com/doi/pdf/10.1089/10949310050191683>.
8. Warren, *supra* note 2; Davies, *supra* note 2.
9. See Robert H. Sloan & Richard Warner, *Beyond Notice and Choice: Privacy, Norms, and Consent*, SSRN ELECTRON. J. (Mar. 27, 2013), <http://www.ssrn.com/abstract=2239099>.
10. Lorrie Faith Cranor, *Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, J. TELECOMM. AND HIGH TECH. L., 10.
11. *Id.*, at 277.
12. Kate Crawford, Kate Miltner & Mary L. Gray, *Critiquing Big Data: Politics, Ethics, Epistemology*, INTL. J. OF COMMUN., *Special Section Introduction*, 10, 1666 (2014).
13. See Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN REV 821 (2000).
14. See e.g., *Y.G. v. Jewish Hospital*, 795 S.W.2d 488 (Mo. Ct. App. 1990) (finding an expectation of privacy for a couple receiving in vitro fertility treatments); *Multimedia WMAZ, Inc. v. Kubach*, 443 S.E.2d 491 (Ga. 1994) (finding an expectation of privacy for a man who had disclosed his HIV-positive status to sixty people).
15. 560 N.E.2d 900 (Ill. App. 1990).
16. *Id.*, at 903–4.
17. See Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919 (2005).
18. Strahilevitz, *supra* note 34, at 973–980.
19. *Id.* at 970–971.
20. 443 S.E.2d 491 (Ga. 1994).
21. *Id.* at
22. *Id.* at
23. Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DAEDALUS 32, 35 (2011).
24. *Id.*, at 36.
25. See generally, Helen Nissenbaum, *PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE* (2009), <https://www.degruyter.com/document/doi/10.1515/9780804772891/html?lang=en>.
26. See Alan B. Vickery, *Breach of Confidence: An Emerging Tort*, 82 COLUM. L. REV. 1426 (1982); G. Michael Harvey, *Confidentiality: A Measured Response to the Failure of Privacy*, 140 U. PA. L. REV. 2385 (1992); Susan M. Gilles, *Promises Betrayed, Breach of Confidence as a Remedy for Invasion of Privacy*, 43 BUFF. L. REV. 1 (1995); Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123 (2007).
27. See e.g., *Alsip v. Johnson City Medical Center*, 197 S.W.3d 722 (2006); *Berger v. Sonneland*, M.D., 1 P.3d 1187 (2000).
28. See e.g., *Waite, Schneider, Bayless & Chesley Co., LPA v. Davis*, 2012 U.S. Dist. Lexis 117634 (S.D. Ohio, Aug. 21, 2012).
29. Vickery, *supra* note 26, at 1428.
30. Andrew J. McClurg, *Kiss and Tell: Protecting Intimate Relationship Privacy through Implied Contracts of Confidentiality*, 74 U. CIN. L. REV. 887 (2006).
31. 381 U.S. 479 (1965) (finding unconstitutional a ban on the use of contraceptives).

32. 405 U.S. 438 (1971) (holding that the constitutional right to use contraceptives extended to both married and unmarried people).

33. 539 U.S. 558 (2003) (finding unconstitutional a criminal prohibition against homosexual acts).

34. McClurg, *supra* note 30, at 915.

35. See e.g. Justine Mitchell, *Censorship in Cyberspace: Closing the Net on "Revenge Porn,"* 25 ENT. L. REV. 283 (2014); Janice Richardson, *The Changing Meaning of Privacy, Identity, and Contemporary Feminist Philosophy*, 21 MINDS & MACH. 517 (2011); Ari Ezra Waldman, *Breach of Trust: Fighting "Revenge Porn,"* 102 IOWA L. REV. 709 (2017).

36. Waldman, *supra* note 35, at 713.

37. *Id.*, at 716.

38. Dan Avery, *Last Day to File a Claim for Google's \$100 Million Privacy Settlement*, CNET (Sept. 24, 2022), <https://www.cnet.com/personal-finance/googles-100-million-facial-recognition-lawsuit-who-can-claim-money-from-the-settlement/>; Jim Hagerty, *Google Settles Lawsuit with Illinois Residents for \$100M after Photo App Privacy Concerns*, USA TODAY (June 3, 2022), <https://www.usatoday.com/story/tech/2022/06/03/google-pay-illinois-settlement-photo-privacy/7495827001/>; Emma Roth, *Google to Pay \$100 Million to Illinois Residents for Photos' Face Grouping Feature*, THE VERGE (June 6, 2022), <https://www.theverge.com/2022/6/6/23156198/google-class-action-face-grouping-biometric-information-illinois-privacy-act>.

39. Torsten Kracht, Lisa Sotto & Bennett Sooy, *Facebook Pivots from Facial Recognition System Following Biometric Privacy Suit*, REUTERS (Jan. 26, 2022), <https://www.reuters.com/legal/legalindustry/facebook-pivots-facial-recognition-system-following-biometric-privacy-suit-2022-01-26/>.

40. Peter Granitz, *Texas Sues Meta, Saying It Misused Facial Recognition Data*, NPR (Feb. 15, 2022), <https://www.npr.org/2022/02/15/1080769555/texas-sues-meta-for-misusing-facial-recognition-data>; Cecilia Kang, *Texas Sues Facebook's Parent, Saying It Collected Facial Recognition Data without Consent*, NEW YORK TIMES (Feb. 14, 2022), <https://www.nytimes.com/2022/02/14/technology/texas-facebook-facial-recognition-lawsuit.html>.

41. Adi Robertson, *Clearview AI Agrees to Permanent Ban on Selling Facial Recognition to Private Companies*, THE VERGE (May 9, 2022), <https://www.theverge.com/2022/5/9/23063952/clearview-ai-aclu-settlement-illinois-bipa-injunction-private-companies>; Nick Statt, *ACLU Sues Facial Recognition Firm Clearview AI, Calling It a "Nightmare Scenario" for Privacy*, THE VERGE (May 28, 2020), <https://www.theverge.com/2020/5/28/21273388/aclu-clearview-ai-lawsuit-facial-recognition-database-illinois-biometric-laws>.