William & Mary
Law Review

VOLUME 62 NO. 6, 2021

# A NEW COMPACT FOR SEXUAL PRIVACY

DANIELLE KEATS CITRON*

ABSTRACT

*Intimate life is under constant surveillance. Firms track people's periods, hot flashes, abortions, sexual assaults, sex toy use, sexual fantasies, and nude photos. Individuals hardly appreciate the extent of the monitoring, and even if they did, little could be done to curtail*

* Jefferson Scholars Foundation Schenck Distinguished Professor in Law, University of Virginia School of Law; Vice President, Cyber Civil Rights Initiative; 2019 MacArthur Fellow. I am grateful to William & Mary Law School for inviting me to give the George Wythe Lecture, to faculty and students for their thoughtful comments, and to the *Law Review* (especially Geoffrey Cannon and his fellow editors) for superb suggestions. Ryan Calo, Woodrow Hartzog, Mary Anne Franks, Neil Richards, Ari Waldman, Alan Butler, Sara Cable, Kris Collins, Jennifer Daskal, John Davisson, Hany Farid, Ahmed Ghappour, Rebecca Green, Debbie Hellman, Laura Heymann, Joe Jerome, Cameron Kerry, Ryan Kriger, Gary Lawson, Tiffany Li, Linda McClain, Mike Meuer, Luis Alberto Montezuma, Jeanine Morris-Rush, Nancy Moore, Nate Oman, David Rossman, Andrew Selbst, David Seipp, Kate Silbaugh, Jessica Silbey, Noah Stein, Peter Swire, and David Webber provided helpful advice. *Boston University Journal of Science & Technology Law* kindly asked me to present this paper as the keynote of its 2019 data privacy symposium. Matt Atha, Rebecca Gutterman, Caroline Hopland, and Julia Schur went above and beyond as research assistants. Tyler Gabrielski was a constant help. The MacArthur Foundation graciously supported this work. I am especially grateful to Dean Risa Goluboff and Vice Dean Leslie Kendrick of the University of Virginia School of Law for their encouragement and insights.

*it. What is big business for firms is a big risk for individuals. Corporate intimate surveillance undermines sexual privacy—the social norms that manage access to, and information about, human bodies, sex, sexuality, gender, and sexual and reproductive health. At stake is sexual autonomy, self-expression, dignity, intimacy, and equality. So are people's jobs, housing, insurance, and other life opportunities. Women and minorities shoulder a disproportionate amount of that burden.*

*Privacy law is failing us. Not only is the private sector's handling of intimate information largely unrestrained by American consumer protection law, but it is treated as inevitable and valuable. This Article offers a new compact for sexual privacy. Reform efforts should focus on stemming the tidal wave of collection, restricting uses of intimate data, and expanding the remedies available in court to include orders to stop processing intimate data.*

TABLE OF CONTENTS

## INTRODUCTION

Intimate life is under constant surveillance. Apps memorialize people's menstruation cycles, fertility, and sexually transmitted infections.[1] Advertisers and analytics firms track searches and browsing on adult sites.[2] Sex toys monitor the frequency and intensity of their owners' use.[3] Digital assistants record, transcribe, and store conversations in bedrooms and bathrooms.[4]

In some contexts, people enter into relationships with the firms tracking their intimate lives.[5] This is true when individuals subscribe to dating apps or purchase digital assistants.[6] In other contexts, people have no connection with the firms handling their intimate data. Data brokers, cyber stalking apps, and sites devoted to nonconsensual pornography and deep fake sex videos come to mind.[7]

---

1. *No Body's Business but Mine: How Menstruation Apps Are Sharing Your Data*, PRIV. INT'L (Oct. 7, 2020), https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data [https://perma.cc/6TMH-2CRU].

2. *See* Elena Maris, Timothy Libert & Jennifer R. Henrichsen, *Tracking Sex: The Implications of Widespread Sexual Data Leakage and Tracking on Porn Websites*, 22 NEW MEDIA & SOC'Y 2018, 2025-26 (2020).

3. Steven Musil, *Internet-Connected Vibrator Connects with Privacy Lawsuit*, CNET (Sept. 13, 2016, 4:15 PM), https://www.cnet.com/news/internet-connected-vibrator-we-vibe-lawsuit-privacy-data/ [https://perma.cc/XK9Y-H4X9].

4. Jennings Brown, *The Amazon Alexa Eavesdropping Nightmare Came True*, GIZMODO (Dec. 20, 2018, 11:24 AM), https://gizmodo.com/the-amazon-alexa-eavesdropping-nightmare-came-true-1831231490 [https://perma.cc/J6T7-ZXTT].

5. *See, e.g.*, Thomas Germain, *How Private Is Your Online Dating Data?*, CONSUMER REPS. (Sept. 21, 2019), https://www.consumerreports.org/privacy/how-private-is-your-online-dating-data/ [https://perma.cc/MF52-4ENF]. They use online services that facilitate testing for sexually transmitted infections and share the results with prospective partners. Kimberly M. Aquiliana, *STD Testing? Yeah, There Is an App for That*, METRO (June 5, 2017), https://www.metro.us/std-testing-yeah-theres-an-app-for-that/ [https://perma.cc/9UUM-DVPA].

6. For instance, people subscribe to dating apps that record their sexual preferences and favorite positions, interest in threesomes, HIV status, and hookups. *See* Azeen Ghorayshi & Sri Ray, *Grindr Is Letting Other Companies See User HIV Status and Location Data*, BUZZFEED NEWS (Apr. 2, 2018, 11:13 PM), https://www.buzzfeednews.com/article/azeenghorayshi/grindr-hiv-status-privacy [https://perma.cc/3PHU-5UH2]; Makena Kelly & Nick Statt, *Amazon Confirms It Holds on to Alexa Data Even if You Delete Audio Files*, VERGE (July 3, 2019, 4:14 PM), https://www.theverge.com/2019/7/3/20681423/amazon-alexa-echo-chris-coons-data-transcripts-recording-privacy [https://perma.cc/C6VQ-YWUR].

7. *See* Kashmir Hill, *Data Broker Was Selling Lists of Rape Victims, Alcoholics, and*

Whether anticipated and expected or unknown and unwanted by individuals, the tracking of intimate information is poised for explosive growth. Profits drive what I have previously described as the "collection imperative."[8] For instance, analysts predict that within five years, the "femtech market"—menstruation, fertility, and sexual wellness apps—will be a $50 billion industry.[9]

Personal data is the coin of the realm for our everyday products and services.[10] At some level, people understand that online services are not actually free.[11] But the firms intentionally structure the deal in a manner that obscures its lopsided nature. Individual consumers cannot fully grasp the potential risks, and few options exist for those who do (beyond not using the service).[12] Firms have every incentive to reinforce the status quo, from which they earn considerable profits.[13]

The surveillance of intimate life garners significant returns with little risk for businesses.[14] The opposite is true for individuals.[15] The

---

*'Erectile Dysfunction Sufferers*,' FORBES (Dec. 19, 2013, 3:40 PM), https://www.forbes.com/sites/kashmirhill/2013/12/19/data-broker-was-selling-lists-of-rape-alcoholism-and-erectile-dysfunction-sufferers/#42acebdb1d53 [https://perma.cc/9HWM-FED4]; Lorenzo Franceschi-Bicchierai & Joseph Cox, *Inside the 'Stalkerware' Surveillance Market, Where Ordinary People Tap Each Other's Phones*, VICE: MOTHERBOARD (Apr. 18, 2017, 8:01 AM), https://www.vice.com/en/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x[https://perma.cc/JPB3-QYXH]; Danielle Keats Citron, *Spying Inc.*, 72 WASH. & LEE L. REV. 1243, 1244-47 (2015) [hereinafter Citron, *Spying Inc.*]; Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1917-18 (2019) [hereinafter Citron, *Sexual Privacy*].

8. Danielle Keats Citron, *A Poor Mother's Right to Privacy*: *A Review*, 98 B.U. L. REV. 1139, 1141 (2018) [hereinafter Citron, *A Poor Mother's Right to Privacy*].

9. Drew Harwell, *Is Your Pregnancy App Sharing Your Intimate Data with Your Boss?*, WASH. POST (Apr. 10, 2019, 3:11 PM) (internal quotation marks omitted), https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/ [https://perma.cc/G5B9-9NKQ].

10. Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606, 608-10 (2014).

11. *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 10-11 (2019); JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 44-46 (2019).

12. *See* Hoofnagle & Whittington, *supra* note 10, at 635-36, 640-41.

13. *See* Neil Richards & Woodrow Hartzog, A Duty of Loyalty for Privacy Law 9 (July 28, 2020) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217 [https://perma.cc/ACL8-GD5E].

14. This pattern happens across the economy but is particularly problematic when it comes to sexual privacy, as I explore throughout this Article.

15. *See* STIGLER COMM. ON DIGIT. PLATFORMS, STIGLER CTR. STUDY OF ECON. & STATE, FINAL REPORT 11-12 (2019), https://www.chicagobooth.edu/research/stigler/news-and-media/

private sector's collection, use, storage, and disclosure of intimate information undermines what I have elsewhere called "sexual privacy" and "intimate privacy"—the ways people manage the boundaries around intimate life.[16] Sexual (or intimate) privacy concerns information about, and access to, the body, particularly the parts of the body associated with sex, gender, sexuality, and reproduction.[17] It concerns information about, and access to, people's sex and gender; their sexual activities and interactions; their innermost thoughts, desires, and fantasies; and their sexual and reproductive health.[18] This includes on- and offline activities, interactions, communications, thoughts, and searches.[19] It concerns information about the decisions that people make about their intimate lives.[20]

This Article focuses on the collection, use, storage, and disclosure of information about sexual privacy, a crucial subset of sexual privacy. I will use the terms "intimate information" and "intimate data" interchangeably to refer to the subject matter of this piece: information about our bodies and health; our sexuality, gender, and sex; and our close relationships.

Maintaining and protecting the privacy of intimate information is foundational for interlocking interests, all of which are essential for us to flourish as human beings.[21] Privacy-afforded intimate information enables identity- and self-development. It frees us to let our guards down and engage in sexual and gender experimentation and expression, alone or with trusted others (including companies).[22] It gives us sexual autonomy. Intimate or sexual privacy also protects our dignity, enabling us to enjoy self-esteem and social respect. Then, too, it frees us to form close intimate relationships

committee-on-digital-platforms-final-report [https://perma.cc/V6BM-JJM7] ("Firms that collect and process private information do not internalize the harms associated with consumer privacy and security breaches. Nor do they internalize negative externalities, or potential misuses of data that impact people who are not their own consumers.").

16. *See* Citron, *Sexual Privacy*, *supra* note 7, at 1874-75, 1880-81.

17. *Id.* at 1874.

18. *Id.*

19. *See id.*

20. *Id.*

21. *See id.* at 1883-85.

22. *See id.* Sexual privacy protects the ability of people to be sexual on their own terms, including being asexual. *See id.*

with friends, lovers, and family members.[23] As Charles Fried said long ago, privacy is the precondition for love and intimacy.[24] And, lastly, it secures equal opportunity.[25]

Our digital services and products could be built to protect our sexual privacy and the experimentation, expression, and intimacy that it makes possible. They could, but they are not. Why? Simply put, privacy is not profitable. For individuals, the costs are significant, though we do not have a real chance to understand the extent of the damage. Private-sector surveillance of intimate information strips individuals of the ability to decide who learns about their miscarriages, breakups, HIV infections, and sexual assaults, now and long into the future. It undermines people's self-esteem as they see themselves as intimate parts and not as whole selves.[26] When companies categorize and rate people as rape sufferers or escort users and nothing more, they give those individuals fractured identities.[27] People's self-expression and association are chilled.[28] Fearful of unwanted surveillance, people stop using dating apps, fertility trackers, or digital assistants.[29] They refrain from browsing sites devoted to gender experimentation, sexuality, and reproductive health.[30]

The damage may be hard for us to grasp as it is happening, but it is no less profound or real. Intimate data reveals people's physical and emotional vulnerabilities, which firms exploit to their advantage.[31] When intimate data is leaked or disclosed to hackers and criminals, individuals have an increased risk of reputational ruin, blackmail, and extortion.[32] When commercial hiring companies use

---

23. *See id. See generally* DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 193-95 (2014) [hereinafter CITRON, HATE CRIMES IN CYBERSPACE].

24. *See* Charles Fried, *Privacy*, 77 YALE L.J. 475, 477-78 (1968).

25. Citron, *Sexual Privacy*, *supra* note 7, at 1883-85.

26. *See id.* at 1886.

27. *See id.*

28. *See* CITRON, HATE CRIMES IN CYBERSPACE, *supra* note 23, at 193-95.

29. *See* Jonathon W. Penney, *Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study*, INTERNET POL'Y REV., May 26, 2017, at 13 [hereinafter Penney, *Case Study*].

30. *See id.* at 8-13.

31. *See infra* Part II.A.

32. Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 744-45 (2018); Kate Fazzini, *Ashley Madison Cyber-Breach: 5 Years Later, Users Are Being Targeted with 'Sextortion' Scams*, CNBC (Jan. 31, 2020, 9:25

intimate data to mine, rank, and rate candidates, people may be unfairly excluded from employment opportunities.[33] People's insurance rates may rise because algorithms predict their need for expensive fertility treatments or gender confirmation surgeries.[34]

These risks are not evenly distributed across society. Women and marginalized communities disproportionately bear the burden of private-sector surveillance of intimate life.[35] Given the way that demeaning stereotypes work, intimate data will more often be used to disadvantage women, sexual minorities, and racial minorities rather than heterosexual white men.[36] The femtech market will surely have a disproportionate impact on women in healthcare, employment, and insurance decisions.[37] The majority of people appearing on sites devoted to revenge porn and deep fake sex videos are women and minorities.[38] For people with intersecting marginalized identities, the harm is compounded.[39] The denial of equal opportunity in the wake of sexual privacy invasions is why I called for the recognition of "cyber civil rights" more than a decade ago.[40]

---

AM), https://www.cnbc.com/2020/01/31/ashley-madison-breach-from-2015-being-used-in-sextortion-scams.html [https://perma.cc/WLN2-J7F2].

33. *See* Ifeoma Ajunwa & Daniel Greene, *Platforms at Work: Automated Hiring Platforms and Other New Intermediaries in the Organization of Work*, *in* 33 RESEARCH IN THE SOCIOLOGY OF WORK, WORK AND LABOR IN THE DIGITAL AGE 61, 79 (Steven P. Vallas & Anne Kovalainen eds., 2019). *See generally* Marie Hicks, *Hacking the Cis-tem: Transgender Citizens and the Early Digital State*, 41 IEEE ANNALS HIST. COMPUTING 20, 28 (2019); SAFIYA UMOJA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM 123-25 (2018).

34. Jaden Urbi, *Some Transgender Drivers Are Being Kicked Off Uber's App*, CNBC (Aug. 13, 2018, 9:21 AM), https://www.cnbc.com/2018/08/08/transgender-uber-driver-suspended-tech-oversight-facial-recognition.html [https://perma.cc/4X59-3T3W]; SARAH MYERS WEST, MEREDITH WHITTAKER & KATE CRAWFORD, AI NOW INSTITUTE, DISCRIMINATING SYSTEMS: GENDER, RACE, AND POWER IN AI 17-18 (2019), https://ainowinstitute.org/discriminatingsystems.pdf [https://perma.cc/5JD9-VS57].

35. *See* Citron, *Sexual Privacy*, *supra* note 7, at 1928.

36. *Id.*; CITRON, HATE CRIMES IN CYBERSPACE, *supra* note 23, at 9-17.

37. As suggested above, this is the direct result of the data collection campaigns of femtech companies.

38. *See* Citron, *Sexual Privacy*, *supra* note 7, at 1919-20, 1924.

39. *See* Mary Anne Franks, *Democratic Surveillance*, 30 HARV. J.L. & TECH. 425, 464 (2017); *see also* Citron, *Sexual Privacy*, *supra* note 7, at 1892-93; Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RSCH. 77, 88 (2018).

40. *See* Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 84-85 (2009) [hereinafter Citron, *Cyber Civil Rights*].

Despite the enormity of these potential harms, intimate information lacks meaningful legal protection. American law generally treats privacy as a consumer protection matter. It focuses on policing firms' notice to consumers about their data practices and any deception associated with those practices.[41] For the most part, the collection, use, storage, and sharing of intimate data are enabled by this approach rather than restricted by it.[42] Tracking intimate data is not just permissible. It is viewed as beneficial.[43] But the truth of the matter is that human flourishing is being impaired, not secured.

This Article offers a new compact for the protection of intimate information. As a start, we need to revise our understanding of the privacy afforded to intimate life. Treating sexual privacy as a consumer protection problem underestimates the interests at stake. The surveillance of intimate life matters—not just because firms fail to provide notice or engage in deceptive practices but also because they undermine autonomy, dignity, intimacy, and equality. It matters because people's crucial life opportunities, including employment, education, housing, insurance, professional certification, and self-expression, are on the line. It matters because our core capabilities hang in the balance.

All personal data needs protection, but even more so for intimate information.[44] Intimate information should not be collected or processed without meaningful consent—knowing, voluntary, and exceptional. Firms should not use intimate information to manipulate people to act against their interests. Firms should have robust obligations of confidentiality, discretion, and loyalty when handling intimate data. Available remedies should include injunctive relief ordering firms to stop processing intimate data until legal commitments are satisfied. Repeated violations can and should result in the

---

41. *See, e.g.*, Richards & Hartzog, *supra* note 13, at 38, 40-41.

42. *See id.*

43. Julie E. Cohen, *Turning Privacy Inside Out*, 20 THEORETICAL INQUIRIES L. 1, 11 (2019) (explaining that the collection and processing of personal data are "position[ed] ... as virtuous and productive, and therefore ideally exempted from state control").

44. *See* Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1128-29 (2015); Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 244-45 (2007) [hereinafter Citron, *Reservoirs of Danger*].

"data death penalty"—forbidding a firm's handling of personal data now and in the future.[45] Given that with enough personal data we can infer intimate information, all personal data deserves strong protection.[46]

This Article has three parts. Part I provides a snapshot into the corporate surveillance of intimate life. It categorizes the surveillance into first- and third-party data collection. Part II highlights the damage that corporate intimate surveillance causes to the values that sexual privacy secures and the harm to human well-being that it inflicts. It provides an overview of the legal landscape and the extent to which law is failing us. Part III offers a plan of action for the protection of intimate information. It provides guideposts for regulating the private sector's surveillance of intimate information, and it suggests affirmative obligations for firms and additional remedies.

---

45. *See infra* Part III.A.3. Thanks to Woodrow Hartzog for suggesting the concept of the "data death penalty" to describe stop processing orders.

46. There is terrific scholarship on the contours of strong baseline privacy protections. *See generally* Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461 (2019) [hereinafter Richards & Hartzog, *Pathologies of Digital Consent*]; Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952 (2017) [hereinafter Hartzog, *Inadequate, Invaluable Fair Information Practices*]; Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016); Woodrow Hartzog, *The Case Against Idealising Control*, 4 EUR. DATA PROT. L. REV. 423 (2018) [hereinafter Hartzog, *The Case Against Idealising Control*]; Richards & Hartzog, *supra* note 13. Cameron Kerry has been thoughtfully exploring the various proposals for data privacy reform at the federal level. *See, e.g.*, Cameron F. Kerry, *Protecting Privacy in an AI-Driven World*, BROOKINGS (Feb. 10, 2020), https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/ [https://perma.cc/8J4T-VU8K]; Cameron Kerry, *Data Collection Standards in Privacy Legislation: Proposed Language*, LAWFARE (Apr. 10, 2019, 11:20 AM), https://www.lawfareblog.com/data-collection-standards-privacy-legislation-proposed-language [https://perma.cc/6K7W-YL6X] [hereinafter Kerry, *Proposed Language*]; Cameron F. Kerry, *Op-Ed: A Federal Privacy Law Could Do Better than California's*, L.A. TIMES (Apr. 25, 2019, 3:05 AM), https://www.latimes.com/opinion/op-ed/la-oe-kerry-ccpa-data-privacy-laws-201904 25-story.html [https://perma.cc/QR6Y-MA69]; Cameron F. Kerry & John B. Morris, Jr., *Why Data Ownership Is the Wrong Approach to Protecting Privacy*, BROOKINGS (June 26, 2019), https://www.brookings.edu/blog/techtank/2019/06/26/why-data-ownership-is-the-wrong-approach-to-protecting-privacy/ [https://perma.cc/QT9S-SNAD].

## I. UNDERSTANDING PRIVATE-SECTOR SURVEILLANCE OF INTIMATE LIFE

This Part gives us a glimpse of the private sector's wide-ranging surveillance of intimate life.[47] First, Section A describes scenarios of first-party collection—or instances in which people have relationships with businesses collecting their intimate information. Then, Section B gives examples of third-party collection—or instances in which people lack a direct relationship with private entities handling their intimate information. I use the concepts of first- and third-party data collection to organize the varied commercial scenarios in which intimate information is collected, processed, used, and shared.[48]

### *A. Cataloging First-Party Collection*

Businesses routinely gather intimate information directly from individuals.[49] First-party collection occurs on sites related to sexual

47. Karen Levy has a wonderful short symposium piece focusing on surveillance practices in the home, often (though not always) involving consensual intimate partners. Karen E.C. Levy, *Intimate Surveillance*, 51 IDAHO L. REV. 679 (2015). In that work, Professor Levy divides intimate surveillance into three categories: dating, tracking intimate and romantic partners, and fertility monitoring. *Id.* at 681-86. In this Article, I explore the collection, use, sharing, and storage of information relating to all aspects of intimate life, including—but not limited to—the home, building on my work on commercial databases of sensitive information, cyber civil rights, nonconsensual pornography, cyber stalking apps, sexual privacy, and deep fakes. *See* Citron, *Reservoirs of Danger*, *supra* note 44; Citron, *Cyber Civil Rights*, *supra* note 40; Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345 (2014); Danielle Keats Citron, *Protecting Sexual Privacy in the Information Age*, *in* PRIVACY IN THE MODERN AGE 46 (Marc Rotenberg, Julia Horwitz & Jeramie Scott eds., 2015); Citron, *Spying Inc.*, *supr*a note 7; Citron, *Sexual Privacy*, *supra* note 7; Danielle Keats Citron, *Why Sexual Privacy Matters for Trust*, 96 WASH. U. L. REV. 1189 (2019) [hereinafter Citron, *Why Sexual Privacy Matters for Trust*]; Bobby Chesney & Danielle Keats Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753 (2019). I discuss first- and third-party data collection as a way to understand the broad array of firms involved in collecting, using, sharing, and storing intimate information.

48. It is worth noting that while the very concept of first- and third-party data collection makes those processes seem normal and routine, they are anything but. I am using those shorthand references given their prevalence in public conversation.

49. *See* Levy, *supra* note 47, at 679-80.

and reproductive health, porn sites, dating apps, and personal devices.[50]

*1. Our Bodies: Our Sexual and Reproductive Health*

Countless websites and apps are devoted to the collection of information about our bodies, including our sexual and reproductive health. These sites and apps let people track their sex lives—including when they had sex, with whom, whether they used protection—and when they masturbate.[51] Some platforms host community forums where subscribers can connect with each other to discuss their sex lives.[52] Health apps let users track their sexual activity.[53] A start-up founded by five men claims that its app developed an algorithm that identifies and proves female orgasms.[54]

Some sexual health start-ups are focused on men.[55] For instance, Ro sends erectile dysfunction drugs directly to consumers.[56] Hims provides treatments for male hair and sexual issues.[57] Each firm raised more than $80 million in financing.[58]

Far more extensive, however, is the tracking of women's health. The term "femtech" describes apps, services, products, and sites that

50. *See* Emma McGowan, *How Tracking Your Sex Life Can Make It Better & 7 Apps to, Uh, Do It with*, BUSTLE (Jan. 9, 2020), https://www.bustle.com/p/tracking-your-sex-life-with-apps-makes-it-super-easy-19779217 [https://perma.cc/RCL3-7HVX].

51. *Id.*

52. *Id.*

53. Lux Alptraum, *Apple's Health App Now Tracks Sexual Activity, and That's a Big Opportunity*, VICE: MOTHERBOARD (Oct. 23, 2016, 1:00 PM), https://www.vice.com/en/article/8q8kpk/apples-health-app-now-tracks-sexual-activityand-that-a-big-opportunity [https://perma.cc/8QJT-VFSL].

54. *See* RELIDA LIMITED, https://www.relidalimited.com/ [https://perma.cc/4J5P-D427]; Rachel Moss, *5 Guys Created an Algorithm to 'Validate the Female Orgasm'. It Went as Well as You'd Expect*, HUFFINGTON POST UK (June 12, 2020), https://www.huffingtonpost.co.uk/entry/5-guys-created-an-algorithm-to-validate-the-female-orgasm-and-it-went-as-well-as-youd-expect_uk_5ee0dc35c5b6cdc3fd432666 [https://perma.cc/CR5M-RV6V] (noting that Relida Limited was founded by five men and that the company claimed on its website that the app's algorithm was created by a woman). After some bad publicity, the start-up's website now says that it is meant to measure orgasms of men and women. *See* RELINDA LIMITED, *supra*.

55. *See* Dana Olsen, *This Year Is Setting Records for Femtech Funding*, PITCHBOOK (Oct. 31, 2018), https://pitchbook.com/news/articles/this-year-is-setting-records-for-femtech-funding [https://perma.cc/TC8G-RAK4].

56. *Id.*

57. *Id.*

58. *Id.*

collect information about women's period cycles, fertility, pregnancies, menopause, and sexual and reproductive histories.[59] Nearly one-third of women in the United States have used period-tracking apps.[60] Menstrual tracking apps "are the fourth most popular health app among adults and the second most popular among adolescent females."[61] The start-up Gennev provides a "free" online menopause health assessment that "collects 72 data points—and nearly 35,000 women took it in 2019."[62] Menopause start-ups have raised more than $250 million from 2009 to 2019.[63] Overall, femtech start-ups raised nearly $500 million in 2019 alone.[64]

Subscribers of menstrual tracking apps enter, among other things, their weight, temperatures, moods, reading material, sexual encounters, tampon use, alcohol consumption, cigarette and coffee habits, bodily secretions, and birth control pills.[65] Apple's Health

---

59. Harwell, *supra* note 9.

60. Donna Rosato, *What Your Period Tracker App Knows About You*, CONSUMER REPS. (Jan. 28, 2020), https://www.consumerreports.org/health-privacy/what-your-period-tracker-app-knows-about-you/ [https://perma.cc/B6PN-A5UW]. There are also fertility apps that track women's menstrual cycles and pregnancy apps that monitor women's habits, mood, fetal movements, and more. *See* Vanessa Rizk & Dalia Othman, *Quantifying Fertility and Reproduction Through Mobile Apps: A Critical Overview*, 22 ARROW FOR CHANGE 13, 13-14 (2016). Some apps, such as Glow, cover all aspects of fertility, including tracking women's cycles, fertility, pregnancy, and a baby's development in the first year. *E.g.*, Jerry Beilinson, *Glow Pregnancy App Exposed Women to Privacy Threats, Consumer Report Finds*, CONSUMER REPS. (Sept. 17, 2020), https://www.consumerreports.org/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats/ [https://perma.cc/AQK7-TZS6].

61. *See* Michelle L. Moglia, Henry V. Nguyen, Kathy Chyjek, Katherine T. Chen & Paula M. Castaño, *Evaluation of Smartphone Menstrual Cycle Tracking Applications Using an Adapted APPLICATIONS Scoring System*, 127 OBSTETRICS & GYNECOLOGY 1153, 1153 (2016) (footnote omitted).

62. Eliza Haverstrock, *Narrative Change: VCs Are Finally Ready to Talk About Menopause*, PITCHBOOK (May 28, 2020), https://pitchbook.com/news/articles/vc-menopause-femtech [https://perma.cc/4K6C-SRB7].

63. *Id.*

64. *Id.*

65. *See No Body's Business but Mine*, *supra* note 1. For instance, the app Clue goes further and asks subscribers to track "not just [the] dates and details of periods and menstrual cycles," but also their discharge of cervical fluids, their use of medication, and their sex life, injections, illnesses, and cervical position. *See* Sadaf Khan, *Data Bleeding Everywhere: A Story of Period Trackers*, DEEP DIVES (June 7, 2019), https://deepdives.in/data-bleeding-everywhere-a-story-of-period-trackers-8766dc6a1e00 [https://perma.cc/UD2K-PQXF]. The Ovia Fertility app lets users indicate the consistency of their cervical discharge, from "egg whites, water, or a bottle of school glue." *Id.* Period-tracking apps are also marketed to people's partners so that they can manage their relationships around menstrual cycles. Levy, *supra* note 47, at 685-86 (discussing apps such as PMSTracker and iAmAMan, which enable subscribers to track

app syncs with period and fertility tracking apps and allows subscribers to track their sexual activity.[66] The Flo app provides extra features such as period predictions and health reports that can be shared with doctors.[67] Some services let subscribers obtain discounts on products, such as tampons.[68]

Consider the Eve Glow app.[69] Subscribers must record their sex drive status with the following choices: "DO ME NOW," "I'm down," or "MIA."[70] To complete their health log, subscribers must input whether they orgasmed during sex.[71] The app's screen enables subscribers to answer "YASSS," "No," or "Faked It."[72] They are asked to indicate whether they are experiencing cramps, tender breasts, or bloating.[73]

Femtech apps like Eve Glow host discussion boards where people using the services talk to each other about their intimate lives, including their experiences with sex, fertility, abortions, or miscarriages.[74] A user of Eve Glow explained that she "kind of lose[s her] inhibition because so many other women are talking about" their intimate lives on the discussion boards.[75] The apps track and store those communications.[76]

Three million people use Glow's suite of apps, which include Eve Glow, Glow, Glow Nurture, and Glow Baby.[77] The company is part of HVF Labs, whose "objective is to take advantage of potential low

---

multiple women's cycles and use multiple passwords to allow users to conceal their tracking activity).

66. Alptraum, *supra* note 53. Some apps are exclusively designed to track people's sexual activity. For example, the BedPost app allows subscribers to track the names of sexual partners, track the dates of sexual experiences, and rank those sexual experiences. *See* BEDPOST, http://www.bedposted.com [https://perma.cc/2JAD-V8FL].

67. *See* Rosato, *supra* note 60.

68. *Id.*

69. EVE GLOW, https://glowing.com/apps [https://perma.cc/T99X-UD2V].

70. Khan, *supra* note 65. MIA presumably means "Missing In Action."

71. *Id.*

72. *Id.*

73. *Id.*

74. *See id.*

75. *Id.*

76. *Id.*

77. *See* Natasha Felizi & Joana Varon, *MENSTRUAPPS—How to Turn Your Period into Money (for Others)*, CODING RIGHTS: CHUPADADOS, https://chupadados.codingrights.org/en/menstruapps-como-transformar-sua-menstruacao-em-dinheiro-para-os-outros/ [https://perma.cc/NGJ2-3NFG].

cost sensors, the gradual increase in access to broadband, and the *high storage capacity to collect and explore data as a commodity*."[78] Glow's privacy policy says that the company may decide to share information collected on the app with third parties to inform users about goods and services including those conducting medical research.[79] Only some of the user data shared is "made anonymous."[80]

Businesses pair health devices with apps to track individuals' intimate data. Looncup, for instance, is poised to offer a smart menstrual cup that records the volume and color of menstrual fluid on its app, ostensibly for health benefits.[81] Trackle links a vaginal thermometer with an app measuring women's inner temperature.[82]

Reproductive health apps market themselves as providing expert advice.[83] Yet many such apps—particularly those that are "free"—are riddled with inaccurate information.[84] In one study, researchers evaluated 108 free menstrual cycle tracking apps and concluded that more than 80 percent of them were "inaccurate, contain[ed] misleading health information, or d[id] not function."[85]

Femtech apps also have been prone to security problems. In 2016, Consumer Reports found that anyone could access Glow subscribers' health data, including the dates of abortions and sexual encounters, if they had their email addresses.[86] Flo was caught sending Facebook subscribers' information, including when they were trying to conceive and having their periods.[87]

---

78. *Id.* (emphasis added) (internal quotation marks omitted).

79. *Id.*

80. *Id.*

81. *See, e.g.*, *LOONCUP—The World's First SMART Menstrual Cup*, KICKSTARTER, https://www.kickstarter.com/projects/700989404/looncup-the-worlds-first-smart-menstrual-cup [https://perma.cc/M7Q9-YZUW].

82. *How Trackle Works*, TRACKLE, https://trackle.de/en/about-trackle-2/how-trackle-works/ [https://perma.cc/34WJ-T5F9].

83. *See, e.g.*, EVE GLOW, *supra* note 69.

84. *See* Moglia et al., *supra* note 61, at 1157.

85. *Id.*

86. Beilinson, *supra* note 60.

87. *See* Sam Schechner & Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook*, WALL ST. J. (Feb. 22, 2019, 11:07 AM), https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636 [https://perma.cc/4BHA-BNZB]

*2. Adult Sites*

Pornography sites collect and store a wealth of information about people's sexual interests, desires, and sexual practices.[88] They track people's search queries, the time and frequency of their visits, and private chats.[89] The most popular free porn site, PornHub, reports that some of the most searched terms on the site include "lesbian," "milf," "step mom," and "teen."[90] The very nature of some adult sites reveals people's sexual interests, such as bestiality or incest sites.[91]

Some specialty sites require members to provide email addresses, passwords, and credit card information.[92] A zoophilia forum accumulated personal information for about 71,000 individuals, including usernames, birth dates, and IP addresses.[93] Rosebuttboard.com, a forum dedicated to "extreme anal dilation and anal fisting," recorded the personal information of 100,000 user accounts, including the email addresses of military members and federal employees.[94]

Adult sites are some of the most popular sites online. They garner more visitors a month than Amazon, Netflix, and Twitter

88. Maris et al., *supra* note 2, at 2019.

89. *See id.*

90. *See The 2019 Year in Review*, PORNHUB INSIGHTS (Dec. 11, 2019), https://www.pornhub.com/insights/2019-year-in-review#searches [https://perma.cc/D3Y8-WHKD]; *see also* Michael Castleman, *Surprising New Data from the World's Most Popular Porn Site*, PSYCH. TODAY (Mar. 15, 2018), https://www.psychologytoday.com/us/blog/all-about-sex/201803/surprising-new-data-the-world-s-most-popular-porn-site [https://perma.cc/377Z-K8WQ].

91. Maris et al., *supra* note 2, at 2027.

92. Joseph Cox, *Thousands of Bestiality Website Users Exposed in Hack*, VICE: MOTHERBOARD (Mar. 29, 2018, 1:59 AM), https://www.vice.com/en_us/article/evqvpz/bestiality-website hacked-troy-hunt-have-i-been-pwned [https://perma.cc/VY5W-3AUW] (explaining that hack of bestiality site revealed more than 3,000 users' email addresses as well as users' password hashes, birthdates, IP addresses, and private messages).

93. *See* Have I Been Pwned (@haveibeenpwned), TWITTER (Oct. 19, 2019, 5:25 PM), https://twitter.com/haveibeenpwned/status/1185668262538838016 [https://perma.cc/8XDD-F34B]. Hackers exposed the personal details of the users of the bestiality site online. Waqas, *Animal Abuse Website Hacked; Thousands of Users Exposed*, HACKREAD (Mar. 30, 2018), https://www.hackread.com/animal-abuse-website-hacked-users-exposed/ [https://perma.cc/335L-5K8T].

94. Joseph Cox, *Another Day, Another Hack: Is Your Fisting Site Updating Its Forum Software?*, VICE: MOTHERBOARD (May 10, 2016, 9:54 AM), https://www.vice.com/en_us/article/qkjj4p/rosebuttboard-ip-board [https://perma.cc/8YKX-DYXT]; Jonathan Keane, *Hack Shows Government and Military Employees Used Their Email Addresses on Hardcore Fetish Site*, DIGIT. TRENDS (May 13, 2016), https://www.digitaltrends.com/computing/rosebutt-hack/ [https://perma.cc/9RDE-EDUN]; Troy Hunt (@troyhunt), TWITTER (May 10, 2016, 10:06 AM), https://twitter.com/troyhunt/status/730036184651431937 [https://perma.cc/EMZ5-6SNF].

combined.[95] In 2018, PornHub had 33.5 billion visits.[96] It had an average of 63,000 visitors per minute.[97] In 2019, that number grew to 80,000 visitors per minute.[98]

*3. Dating Apps*

Dating apps and services collect broad swaths of people's intimate information, including their names, photographs, occupations, locations, relationship status, romantic or sexual interests, sexual orientation, interest in extramarital affairs, and sexually transmitted infections.[99] Adults are not the only ones on dating apps; teenagers also subscribe to Tinder, MeetMe, Hot or Not, MyLOL, and Kik.[100] Such sites are commonly used by LGBTQ youth who lack supportive networks at school to connect with others.[101]

Simple behaviors on these apps and sites, such as how long a user views a particular profile or image, can reveal the characteristics or features that a person looks for in a romantic partner.[102] Journalist Judith Duportail discovered just how extensive her disclosures to

95. Maris et al., *supra* note 2, at 2019.

96. *Digital Fingerprints: How the Porn You Watch May Be Watching You*, FIGHT THE NEW DRUG (Feb. 15, 2019), https://fightthenewdrug.org/how-your-porn-may-be-watching-you/ [https://perma.cc/L9N7-HFX4].

97. *Can You Guess 2018's Most-Viewed Categories on the Largest Porn Site?*, FIGHT THE NEW DRUG (July 9, 2019), https://fightthenewdrug.org/pornhub-visitors-in-2018-and-review-of-top-searches/ [https://perma.cc/3STF-AV9J].

98. *The 2019 Year in Review*, *supra* note 90.

99. *See* Thomas Germain, *How Private Is Your Online Dating Data?*, CONSUMER REPS. (Sept. 21, 2019), https://www.consumerreports.org/privacy/how-private-is-your-online-dating-data/ [https://perma.cc/MF52-4ENF] ("You might never choose to share those thousands of intimate facts with a friend or family member, but if you use dating apps, you are providing the information to companies that will collect and retain every detail."); *see also* Michael Zimmer, *OKCupid Study Reveals the Perils of Big-Data Science*, WIRED (May 14, 2016, 7:00 AM), https://www.wired.com/2016/05/okcupid-study-reveals-perils-big-data-science/ [https://perma.cc/DN53-CJRL]. It is worth noting the rise of dating intelligence apps like Lulu. This app "allows women to anonymously review and rate men." *See Dating Intelligence App Lulu Acquired by Badoo*, PITCHBOOK (Feb. 10, 2016), https://pitchbook.com/newsletter/dating-intelligence-app-lulu-acquired-by-badoo [https://perma.cc/427V-HM6Q]. Lulu raised $6 million in venture funding and was acquired by Badoo in 2016. *Id.*

100. Christine Elgersma, *Tinder and 7 More Dating Apps Teens Are Using*, COMMON SENSE MEDIA (Feb. 12, 2019), https://www.commonsensemedia.org/blog/tinder-and-7-more-dating-apps-teens-are-using [https://perma.cc/PVT4-4659]. Teenagers can access some of these apps via Facebook. *Id.*

101. *Id.*

102. Germain, *supra* note 99.

Tinder were when the company complied with her request for her records as required by the General Data Protection Regulation (GDPR).[103] The company returned eight hundred pages detailing her activities and interactions.[104] A review of the 1,700 messages Duportail sent through the app revealed her "hopes, fears, sexual preferences and deepest secrets."[105]

All of this intimate information is ripe for exploitation and disclosure.[106] In some cases, this data may appear in the profiles of potential matches.[107] As explored below, it may be shared with advertisers and other firms.[108]

And firms' data collections may be inadequately secured and stolen. Hackers have targeted dating services to steal intimate

---

103. Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

104. Judith Duportail, *I Asked Tinder for My Data. It Sent Me 800 Pages of My Deepest, Darkest Secrets*, GUARDIAN (Sept. 26, 2017, 2:10 AM), https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold [https://perma.cc/WS2Z-U2J2]. The documents included Duportail's Facebook likes and number of friends, links to her Instagram photos, her education, the age-range of men she was interested in, the number of times she opened the app, the number of people she matched with, and where and when each conversation with a match took place. *Id.* Facebook started a dating app in 2019. Nathan Sharp, *It's Facebook Official, Dating Is Here*, FACEBOOK (Sept. 5, 2019), https://about.fb.com/news/2019/09/facebook-dating/ [https://perma.cc/Q5CZ-QKVD] (announcing the launch of Facebook's dating app); *see also* Charlie Warzel, *Don't Trust Facebook With Your Love Life*, N.Y. TIMES (Sept. 5, 2019), https://www.nytimes.com/2019/09/05/opinion/facebook-dating-app.html [https://perma.cc/H45K-UPG4].

105. Duportail, *supra* note 104.

106. *Id.* ("Tinder's privacy policy clearly states: 'you should not expect that your personal information, chats, or other communications will always remain secure.'"); *see also Privacy Policy*, TINDER, https://www.gotinder.com/privacy [https://perma.cc/8UL2-TFVN] ("As with all technology companies, although we take steps to secure your information, we do not promise, and you should not expect, that your personal information will always remain secure.").

107. In 2016, Danish researchers refused to anonymize a data set containing 70,000 OK Cupid users' "usernames, age, gender, location, what kind of relationship (or sex) they're interested in, personality traits, and answers to thousands of profiling questions." Zimmer, *supra* note 99. The researchers argued that the information was already "publicly available," though Zimmer notes that this is not entirely accurate. *Id.* "Since OkCupid users have the option to restrict the visibility of their profiles to logged-in users only, it is likely the researchers collected—and subsequently released—profiles that were intended to not be publicly viewable." *Id.* (emphasis omitted).

108. *See infra* Part I.B.

information in order to blackmail and extort subscribers.[109] In 2015, a data breach resulted in hackers publishing online the personal details of subscribers to Ashley Madison, a site for people seeking extramarital affairs. Millions of subscribers' names, emails, sexual preferences, and sexual desires were posted online in a searchable format.[110] Criminals continue to use the intimate information shared with Ashley Madison in extortion schemes.[111]

Membership of or browsing on particular dating sites may reveal someone's sexual preferences and habits.[112] In October 2016, hackers obtained 412 million account records from Friend Finder Networks.[113] The information exposed included "email addresses,

---

109. Lily Hay Newman, *Hacks, Nudes, and Breaches: It's Been a Rough Month for Dating Apps*, WIRED (Feb. 15, 2019, 4:44 PM), https://www.wired.com/story/ok-cupid-dating-apps-hacks-breaches-security/ [https://perma.cc/SE99-ZWPS] ("The same factors that make dating sites an appealing target for hackers also make them useful for romance scams: It's easier to assess and approach people on a site that are already meant for sharing information with strangers.").

110. Zak Doffman, *Ashley Madison Hack Returns to 'Haunt' Its Victims: 32 Million Users Now Watch and Wait*, MEDIUM (Feb. 1, 2020, 7:06 AM), https://www.forbes.com/sites/zakdoffman/2020/02/01/ashley-madison-hack-returns-to-haunt-its-victims-32-million-users-now-have-to-watch-and-wait/#6151c2395677 [https://perma.cc/6QNP-NHCU] (explaining that the Ashley Madison hack resulted in the leaking of intimate information of 32 million people). Ashley Madison touted its service as enabling "infidelity and married dating." Kim Zetter, *Hackers Finally Post Stolen Ashley Madison Data*, WIRED (Aug. 18, 2015, 5:55 PM), https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/ [https://perma.cc/P672-Z6YF]. The data released by hackers included names, passwords, addresses, and phone numbers submitted by users of the site. *Id.* Also included were users' credit card transactions, revealing people's real names and addresses. *Id.* The data dump revealed members' sexual fantasies and desires, such as "I like lots of foreplay and stamina, fun, discretion, oral, even willingness to experiment." *Id.* As Karen Levy wisely noted, "The real benefit of self-tracking is always to the company.... People are being asked to do this at a time when they're incredibly vulnerable and may not have any sense where that data is being passed." Harwell, *supra* note 9 (quoting Cornell professor Karen Levy). Nor do they realize how easy it is to re-identify such information. *See id.*

111. Doffman, *supra* note 110 (explaining that victims of Ashley Madison hack continue to receive emails with embarrassing details from the breach and with demands for bitcoin ransoms to be paid in "a limited amount of time").

112. *See, e.g.*, Cox, *supra* note 92; Michelle Broder Van Dyke, *Pastor Exposed by Ashley Madison Hack Kills Himself*, BUZZFEED NEWS (Sept. 8, 2015, 8:52 PM), https://www.buzzfeednews.com/article/mbvd/pastor-exposed-by-ashley-madison-hack-commits-suicide [https://perma.cc/HE5H-7GXB].

113. Samuel Gibbs, *Adult Friend Finder and Penthouse Hacked in Massive Personal Data Breach*, GUARDIAN (Nov. 14, 2016, 6:21 AM), https://www.theguardian.com/technology/2016/nov/14/adult-friend-finder-and-penthouse-hacked-in-largest-personal-data-breach-on-record [https://perma.cc/B56T-EWXS] ("Among the leaked account details were 78,301 US military email addresses, 5,650 US government email addresses and over 96 [million] Hotmail

passwords, dates of last visits, browser information, IP addresses and site membership status across sites run by Friend Finder Networks," including Adult Friend Finder, Cams.com, Penthouse.com, and three other sites.[114] Three years later, a hacker obtained 250,000 "email addresses, usernames, IP addresses, and hashed passwords" from the Dutch sex-work forum Hookers.nl where "clients discuss[ed] their experiences with sex workers."[115]

*4. Personal Devices*

An array of devices records people's intimate activities and interactions. Sex toys are obvious examples. We-Vibe, a networked vibrator, allows subscribers to control others' devices via an app.[116] The app also enables partners to communicate with each other via text or video chat.[117] The Lioness vibrator similarly enables subscribers to live stream "what's going on in the moment" and permits partners to remotely control the device.[118] Companies sell Wi-Fi

accounts. The [leak] ... also included the details of what appear to be almost 16 [million] deleted accounts.").

114. *Id.* "This is not the first time Adult Friend Network has been hacked. In May 2015 the personal details of almost four million users were leaked by hackers, including their login details, emails, dates of birth, post codes, sexual preferences and whether they were seeking extramarital affairs." *Id.* The inclusion of data from Penthouse.com in the 2016 breach was particularly concerning as Friend Finder Networks sold the site to Penthouse Global Media in February 2016. *Id.*

115. Samantha Cole & Joseph Cox, *A Hacker Stole 250k User Account Details from a Dutch Sex Work Site*, VICE: MOTHERBOARD (Oct. 10, 2019, 10:32 AM), https://www.vice.com/en_us/article/d3a5gy/hacker-stole-user-account-details-from-a-dutch-sex-work-site-hookers-nl [https://perma.cc/R4V4-T7G7] ("Although prostitution is legal and regulated in the Netherlands, people still seek anonymity when they're buying services—whether from websites like Hookers.nl or in person at brothels."); Thomas Brewster, *Dutch Prostitution Site Hookers.nl Hacked—250,000 Users' Data Leaked*, FORBES (Oct. 10, 2019, 8:43 AM), https://www.forbes.com/sites/thomasbrewster/2019/10/10/dutch-prostitution-site-hookersnl-hacked--250000-users-data-leaked/?sh=41fadb1822f8 [https://perma.cc/WG74-VGUB] ("Dutch broadcaster NOS, which broke the story ... viewed some of the data and said it could determine some real names of users.").

116. Musil, *supra* note 3.

117. *Id.*

118. *Now You Can See Your Orgasm in Real Time*, LIONESS (Apr. 15, 2019), https://blog.lioness.io/now-you-can-see-your-orgasm-in-real-time-359afbdfa6d0 [https://perma.cc/N8ST-BYE3]. We-Vibe recorded the dates and times of a vibrator's use and the intensity and mode selected by subscribers without their consent, leading to a class action lawsuit discussed in Part II. *See* Amended Class Action Complaint & Demand for Jury Trial at 1-2, N.P. v. Standard Innovation Corp., Case No. 1:16-cv-8655 (E.D. Ill. Feb. 27, 2017).

enabled butt plugs, vibrating masturbators for men, and devices for the penis that track thrusting.[119] Like many consumer goods, internet-connected sex toys are not developed with privacy and security in mind.[120]

While voice-enabled personal assistants that listen to and record people's activities are less obviously related to intimate life, they are no less important.[121] Amazon's Echo and other Alexa-enabled devices are marketed as in-home hubs for managing day-to-day tasks.[122] They record people's communications, storing them as voice recordings and text transcripts in the cloud.[123] Amazon retains text transcripts even after subscribers choose to delete the saved audio files of their voice interactions with the device.[124]

According to researchers, voice-activated assistants, such as Alexa and Echo, do not only wake and record when subscribers say the "wake word."[125] Indeed, the systems are error prone and have recorded intimate conversations.[126] Apple's Siri has captured recordings of sexual encounters.[127] Computer science researchers at Northeastern University conducted a study of smart speakers by exposing devices to three audiobooks and nine episodes of the

---

119. Emily Dreyfuss, *Don't Get Your Valentine an Internet-Connected Sex Toy*, WIRED (Feb. 14, 2019, 10:02 AM), https://www.wired.com/story/internet-connected-sex-toys-security/ [https://perma.cc/ER73-9LFK]; Rebecca "Burt" Rose, *How Fit Is Your Dick, Exactly? The Sex-Fit Ring Knows All the Answers*, JEZEBEL (Aug. 8, 2014, 6:10 PM), https://jezebel.com/how-fit-is-your-dick-exactly-the-sexfit-ring-knows-al-1618065007 [https://perma.cc/YQX8-DBMR].

120. *See IoD Goals*, INTERNET OF DONGS PROJECT, https://internetofdon.gs/about/ [https://perma.cc/F9K8-M9RC]. Security researchers involved in "The Internet of Dongs Project" report on security vulnerabilities and work with companies interested in fixing problems. *Id.* The researchers have published guidance documents on the reporting of security vulnerabilities and ensuring secure software development lifecycle to prevent vulnerabilities from occurring in the first place. *Vendor Resources*, INTERNET OF DONGS PROJECT, https://internetofdon.gs/vendor-resources/ [https://perma.cc/SK3H-WD3T].

121. Alex Hern, *Apple Contractors 'Regularly Hear Confidential Details' on Siri Recordings*, GUARDIAN (July 26, 2019, 12:34 PM), https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings [https://perma.cc/DB24-B927].

122. Kelly & Statt, *supra* note 6.

123. *Id.*

124. *Id.*

125. Allen St. John, *Smart Speakers that Listen When They Shouldn't*, CONSUMER REPS. (Aug. 29, 2019), https://www.consumerreports.org/smart-speakers/smart-speakers-that-listen-when-they-shouldnt/ [https://perma.cc/WK4T-2KH4].

126. *Id.*; Hern, *supra* note 121.

127. Hern, *supra* note 121.

television show *Gilmore Girls*.[128] Their study found 63 false positives in 21 hours—meaning that the home devices recorded 63 conversations that it should not have in a 21-hour time span.[129]

Amazon employs thousands of people worldwide to analyze and transcribe voice clips to improve Alexa's accuracy.[130] Some employees have watched people's home camera footage.[131] One German Amazon customer inadvertently received hundreds of Alexa recordings and transcripts from another user in response to a GDPR request in August 2018.[132] The person could be heard in multiple locations, including the shower, as could a frequent female guest.[133] A German magazine found it "fairly easy to identify the person involved and his female companion" using "[w]eather queries, first names, and even someone's last name."[134] In July 2019, Google admitted to a similar breach after a contractor shared with a news site more than one thousand sound recordings of customer conversations made by Google Assistant.[135] Included in the recordings were people talking about medical conditions.[136]

Amazon plans to expand Alexa's reach, with one executive telling the *New York Times* that "[t]here is no reason not to put them everywhere in your house."[137] Amazon has released a tiny version of

---

128. St. John, *supra* note 125.

129. *Id.*

130. Aimee Picchi, *Amazon Workers Are Listening to What You Tell Alexa*, CBS NEWS (Apr. 11, 2019, 12:35 PM), https://www.cbsnews.com/news/amazon-workers-are-listening-to-what-you-tell-alexa/ [https://perma.cc/WF5F-ZX3L].

131. Natalia Drozdiak, Giles Turner & Matthew Day, *Amazon Workers May Be Watching Your Cloud Cam Home Footage*, BLOOMBERG (Oct. 11, 2019, 5:56 PM), https://www.bloomberg.com/news/articles/2019-10-10/is-amazon-watching-you-cloud-cam-footage-reviewed-by-humans [https://perma.cc/R32W-338H].

132. Brown, *supra* note 4. Amazon later claimed this occurred because of a "one-time error" by a staff member and disabled the link that provided access to the data. *Id.*

133. *Id.*

134. *Id.*

135. Todd Haselton, *Google Admits Partners Leaked More than 1,000 Private Conversations with Google Assistant*, CNBC (July 11, 2019, 1:11 PM), https://www.cnbc.com/2019/07/11/google-admits-leaked-private-voice-conversations.html [https://perma.cc/582V-HZR3].

136. *Id.*

137. Karen Weise, *Amazon Wants Alexa to Move (With You) Far Beyond the Living Room*, N.Y. TIMES (Sept. 25, 2019), https://www.nytimes.com/2019/09/25/technology/amazon-alexa-new-devices.html [https://perma.cc/BM8B-B9R4]. Kohler took Amazon's advice to heart, announcing a version of its Moxie showerhead that includes a removable Alexa-enabled speaker imbedded right in the showerhead itself. Chris Davies, *Kohler Put Alexa in Your Showerhead and Gave Your Toilet an App*, SLASHGEAR (Jan. 3, 2020, 11:48 AM), https://

the device, Echo Flex, meant for bathrooms, which plugs into wall outlets.[138] Customized, location-specific versions of Alexa are being sold and deployed in hotel rooms around the country.[139]

### *B. Surveying Third-Party Collection*

First-party collection is directly tied to third-party collection. A vast universe of companies purchase intimate data from first-party collectors.[140] Companies also obtain intimate information from someone who lacks authority to share, disclose, or sell it.[141] This Section provides illustrations.

#### *1. The Data Hand Off: Advertising and Analytics*

First-party data collectors routinely allow advertising firms to collect subscribers' intimate information for a fee.[142] Period-tracking apps share user data with online advertisers who may further resell the information.[143] For instance, Maya and MIA Fem share data

---

www.slashgear.com/kohler-put-alexa-in-your-showerhead-and-gave-your-toilet-an-app-03605166/ [https://perma.cc/7U2X-LKWD].

138. Weise, *supra* note 137.

139. Chris Welch, *Amazon Made a Special Version of Alexa for Hotels with Echo Speakers in Their Rooms*, VERGE (June 19, 2018, 6:00 AM), https://www.theverge.com/2018/6/19/17476688/amazon-alexa-for-hospitality-announced-hotels-echo [https://perma.cc/FW3P-3ULT]. In 2019, to my surprise, I found an Alexa in my hotel room at the Oklahoma City Ambassador Hotel. A card under the black unassuming device said, "Need something? Just ask Alexa." It continued, "Ready for bed? Tell Alexa to play white noise." The device enabled live connections to the front desk, room service, and housekeeping. I went to the front desk to complain because the room did not otherwise have a phone. The attendant explained that I was the first person to object to the device and that most guests did not mention even noticing it.

140. Shilpa Patel, Dominic Field & Henry Leon, *Responsible Marketing with First-Party Data*, BCG (May 18, 2020), https://www.bcg.com/publications/2020/responsible-marketing-with-first-party-data [https://perma.cc/V9VP-UBK6].

141. *Id.*

142. *Id.*

143. At least eleven apps sent Facebook intimate information even though some of the app subscribers were not Facebook members at all and those who used Facebook were not logged into the site. Daniel Moritz-Rabson, *Does Facebook Collect Your 'Intimate Secrets' from Apps? Gov. Andrew Cuomo Orders Investigation*, NEWSWEEK (Feb. 22, 2019, 3:58 PM), https://www.newsweek.com/new-york-governor-directs-investigation-facebook-information-collection-1341170 [https://perma.cc/H43L-QY9J]. Facebook claimed the apps sharing information with it violated its terms of service. *Apps Send Intimate User Data to Facebook: Report*, HINDU (Feb. 23, 2019, 9:52 PM), https://www.thehindu.com/sci-tech/technology/apps-send-intimate-user-data-to-facebook-report/article26352817.ece [https://perma.cc/DPW9-GQPS].

about subscribers' contraception and sexual encounters with Facebook's advertising system (even if those individuals do not have Facebook accounts themselves).[144] Although the apps and services explored above (first-party collectors) are marketed to consumers as "free," the advertising and analytics ecosystem makes clear that their price is people's most intimate information.[145]

First-party data collectors let firms place trackers on their sites. For instance, Grindr shared subscribers' HIV status (noted as "positive, positive and on HIV treatment, negative, or negative and on PrEP") with two companies hired to optimize the app.[146] It also disclosed to advertisers their subscribers' "precise GPS position, 'tribe' (meaning what gay subculture they identify with), sexuality, relationship status, ethnicity, and phone ID."[147] Some of the information shared with advertisers appeared in plain text.[148]

Third-party trackers are pervasive on porn sites. Researchers found that 93 percent of the 22,484 porn sites that they analyzed allowed third parties to collect information about people's browsing

144. Marie C. Baca, *These Apps May Have Told Facebook About the Last Time You Had Sex*, WASH. POST (Sept. 17, 2019, 3:21 PM), https://www.washingtonpost.com/technology/2019/09/10/these-apps-may-have-told-facebook-about-last-time-you-had-sex/ [https://perma.cc/R3DP-U86Q]. For instance, users tried to block tracking by using anonymizing browsers. *Id.*

145. Hoofnagle & Whittington, *supra* note 10, at 626-28.

146. Ghorayshi & Ray, *supra* note 6. Grindr defended its sharing with the analytics companies, Apptimize and Localitics, as essential to making the app better. *Id.* Localytics describes its services as combining people's profile data (who they are) and behavioral data (how they behave online) to personalize mobile advertising. *The Stages of Personalization*, UPLAND LOCALYTICS, https://uplandsoftware.com/localytics/resources/ebook/the-stages-of-personalization/ [https://perma.cc/QCS6-DFE9]. Profile data, the company explains, can originate from many sources. *Id.* More than 37,000 apps use the service. *Id.* In response to bad press and pushback from subscribers, Grindr announced that it would stop sharing HIV status information with third parties. Azeen Ghorayshi, *Grindr Will Stop Sharing Users' HIV Data with Other Companies*, BUZZFEED NEWS (Apr. 2, 2018, 11:03 PM), https://www.buzzfeednews.com/article/azeenghorayshi/grindr-stopped-sharing-hiv-status [https://perma.cc/89S4-SNHX].

147. Ghorayshi & Ray, *supra* note 6. In late 2019, Norwegian researchers found that Grindr uses various advertising networks and some received information about the type of relationship users are looking for. ANDREAS CLAESSON & TOR E. BJØRSTAD, NORWEGIAN CONSUMER COUNCIL, "OUT OF CONTROL"—A REVIEW OF DATA SHARING BY POPULAR MOBILE APPS 30 (2020), https://fil.forbrukerradet.no/wp-content/uploads/2020/01/mnemonic-security-test-report-v1.0.pdf [https://perma.cc/7KX5-P4SM].

148. Ghorayshi & Ray, *supra* note 6. Grindr's privacy policy states that if subscribers "choose to include information in [their] profile[s], and make [their] profile[s] public, that information will also become public." *Id.*

habits.[149] On average, porn sites had seven companies tracking viewers' information.[150] Google trackers appeared on 74 percent of the sites studied, Oracle on 24 percent, and Facebook on 10 percent.[151] Porn-specific trackers included exoClick, JuicyAds, and EroAdvertising.[152] Another 2019 study found that more than half of the one hundred most popular porn sites host third-party trackers that use a technique allowing cookies to be synchronized across sites.[153] Microsoft's Elena Maris noted that "[t]he fact that the mechanism for adult site tracking is so similar to, say, online retail should be a huge red flag."[154]

Third-party trackers collected people's IP addresses, their phones' advertising identification numbers, and information suggesting their sexual desires.[155] Adult advertising networks collect IP addresses, browsers, locations, basic computer details, and other information including how much time people spend viewing certain videos and the categories of porn they select.[156] Forty-five percent of

149. Maris et al., *supra* note 2, at 2019, 2025.

150. *Id.* at 2025.

151. *Id.* After the study was released, Google denied its software was collecting information to build advertising profiles. James Vincent, *Google and Facebook's Tracking Software Is Widely Used on Porn Sites, Shows New Study*, VERGE (July 18, 2019, 8:01 AM), https://www.theverge.com/2019/7/18/20699025/porn-browsing-sites-google-facebook-oracle-ad-tracking-incognito-mode-study [https://perma.cc/H2JU-2F6K]. The company also claimed that "tags for [their] ad services are never allowed to transmit personally identifiable information." *Id.*

152. Maris et al., *supra* note 2, at 2025.

153. Pelayo Vallina, Álvaro Feal, Julien Gamba, Narseo Vallina-Rodriguez & Antonio Fernández Anta, *Tales from the Porn: A Comprehensive Privacy Analysis of the Web Porn Ecosystem*, PROC. INTERNET MEASUREMENT CONF., Oct. 2019, at 245, 252.

154. Charlie Warzel, *Facebook and Google Trackers Are Showing Up on Porn Sites*, N.Y. TIMES (July 17, 2019), https://www.nytimes.com/2019/07/17/opinion/google-facebook-sex-websites.html [https://perma.cc/688Q-KAR2].

155. *Id.* This is a noted change in practice for the most trafficked porn sites, those owned by Pornhub. In 2013, Pornhub's Vice President said that the Pornhub network, including YouPorn and RedTube, "[did] not allow third parties to access ... users' activity on the site[s] or their web histor[ies]." Tracy Clark-Flory, *Who's Tracking Your Porn*, SALON (Dec. 12, 2013, 5:00 AM), https://www.salon.com/2013/12/12/whos_tracking_your_porn/ [https://perma.cc/5KXQ-T2ZW]. Pornhub now has trackers, including adult advertising networks. Dylan Curran, *Browsing Porn in Incognito Mode Isn't Nearly as Private as You Think*, GUARDIAN (May 27, 2018, 11:33 AM), https://www.theguardian.com/commentisfree/2018/may/27/incognito-mode-what-does-it-mean-history-google-chrome-privacy-settings [https://perma.cc/7A3G-LBBG].

156. Curran, *supra* note 155.

porn site URLs include words or phrases suggesting a particular sexual preference or interest.[157]

*2. Data Brokers*

Data brokers amass and sell dossiers with thousands of data points on every person, categorizing them based on intimate information. Their dossiers pair basic information like names, addresses, employers, and contact information, with far more sensitive material.[158] They detail people's sexual preferences, porn consumption, sex toy purchases, escort service usage, and reproductive choices.[159] People are tagged as rape victims, erectile dysfunction sufferers, sex toy purchasers, AIDS/HIV diagnosed, and gay Air Force personnel.[160]

Data brokers sell lists of gay and lesbian adults, rape victims, people with sexual addictions, individuals with sexually transmitted diseases, and purchasers of adult material and sex toys.[161] Some data brokers specialize in dating profiles. For instance, USDate sells dating profiles that include people's photographs, "usernames, e-mail addresses, nationality, gender, ... [and] sexual orientation."[162] Exact Data sells customer lists of adult dating service subscribers, dating and escort services, and "Suddenly Single."[163]

The data-broker industry generates two hundred billion dollars annually.[164] People's personal information is harvested from a vast

157. Maris et al., *supra* note 2, at 2027.

158. Michal Wlosik, *What Is a Data Broker and How Does It Work?*, CLEARCODE, https://clearcode.cc/blog/what-is-data-broker/ [https://perma.cc/XV4H-3QHK].

159. Curran, *supra* note 155.

160. Wlosik, *supra* note 158.

161. Jeff Roberts, *With Data Brokers Selling Lists of Alcoholics to Big Business, the Feds Have Some Thinking to Do*, GIGAOM (Mar. 13, 2004, 5:00 AM), https://gigaom.com/2014/03/13/with-data-brokers-selling-lists-of-alcoholics-to-big-business-the-feds-have-some-thinking-to-do/ [https://perma.cc/KA3N-CDXE].

162. Joana Moll, *The Dating Brokers: An Autopsy of Online Love*, TACTICAL TECH (Oct. 2018), https://datadating.tacticaltech.org/viz [https://perma.cc/Q5RZ-XGRW]; Samantha Cole, *Shady Data Brokers Are Selling Online Dating Profiles by the Millions*, VICE (Nov. 12, 2018, 2:05 PM), https://www.vice.com/en_us/article/59vbp5/shady-data-brokers-areselling-online-dating-profiles-by-the-millions [https://perma.cc/CB6Q-5FYT]; Warzel, *supra* note 154.

163. *See Mailing Lists with "Dating" in the Title*, EXACT DATA, https://www.exactdata.com/mailing-lists.html?keyword=dating [https://perma.cc/F9HR-F86T].

164. Wlosik, *supra* note 158.

array of sources, including first-party collectors, government records, advertisers, and analytics firms, largely without individuals' knowledge or assent.[165] Thousands of data brokers operate in the United States.[166] Data brokers have personal information on 95 percent of the U.S. population.[167]

Data brokers say that their dossiers enhance online advertising and email marketing campaigns.[168] They offer their services far beyond the advertising ecosystem. They serve as "people search sites" to anyone interested in finding out about specific individuals.[169] They sell risk-mitigation products described as helping clients prevent fraud that can adversely affect people's ability to obtain certain benefits.[170] Clients include alternative payment providers, educational institutions, insurance companies, lenders, political campaigns, pharmaceutical companies, technology firms, and real estate services.[171] Customers also include government agencies and law enforcement.[172] As Chris Hoofnagle put it years ago, data brokers serve as "Big Brother's Little Helpers."[173]

---

165. FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014) [hereinafter FTC, DATA BROKERS], https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/K555-J7ML].

166. Wlosik, *supra* note 158.

167. Kalev Leetaru, *The Data Brokers So Powerful Even Facebook Bought Their Data—but They Got Me Wildly Wrong*, FORBES (Apr. 5, 2018, 4:08 PM), https://www.forbes.com/sites/kalevleetaru/2018/04/05/the-data-brokers-so-powerful-even-facebook-bought-their-data-but-they-got-me-wildly-wrong/#7d52df5d3107 [https://perma.cc/2J9X-C5VM].

168. Yael Grauer, *What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?*, VICE: MOTHERBOARD (Mar. 27, 2018, 10:00 AM), https://www.vice.com/en_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection [https://perma.cc/G2NY-EVGK].

169. *Id.*

170. FTC, DATA BROKERS, *supra* note 165, at viii, 32-33, 48.

171. *Id.* at 39-40.

172. *See* David Gray & Danielle Keats Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 65-66 (2013); Danielle Keats Citron & David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. F. 262, 263 (2013).

173. Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 595 (2003).

*3. Cyber Stalking Apps*

As I have explored elsewhere, one infamous "sector of the surveillance economy involves the provision of spyware, a type of malware installed on someone's device without knowledge or consent."[174] Cyber stalking apps enable continuous real-time monitoring of everything phone owners do and say with their devices.[175] In real time, people (often domestic abusers or suspicious partners) can track a phone owner's calls, texts, medical appointments, online searches, porn watching, and minute-to-minute movements.[176] Targeted phones can be used as bugging devices, recording conversations within a fifteen-foot radius.[177]

A selling point of cyber stalking apps is their secretive nature. App developers assure subscribers that once they download the app to an unsuspecting person's phone, the phone owner will not be able to detect the spyware.[178] The goal, as they know well, is the stealth surveillance of intimate partners or ex-intimate partners.[179] Firms try to conceal this fact by taking innocuous names. For instance, an app developer changed the name of its app from "GirlFriend Call Tracker" to "Family Locator," but the service remains the same.[180] The Electronic Frontier Foundation's Eva Galperin has been watching the industry closely and she explains that "[t]he people who end up with this software on their phones can become victims of physical abuse, of physical stalking. They get beaten. They can be killed. Their children can be kidnapped."[181]

174. Citron, *Spying Inc.*, *supra* note 7, at 1244.
175. *Id.* at 1247.
176. *Id.*
177. *Id.* at 1246.
178. *Id.*
179. *Id.* at 1247.
180. Laura Hautala, *Stalkerware Sees All, and US Laws Haven't Stopped Its Spread*, CNET (June 5, 2020, 7:10 AM), https://www.cnet.com/news/stalkerware-sees-all-and-us-laws-havent-stopped-its-spread/ [https://perma.cc/WB9G-R9P6].
181. Andy Greenberg, *Hacker Eva Galperin Has a Plan to Eradicate Stalkerware*, WIRED (Apr. 3, 2019, 6:00 AM), https://www.wired.com/story/eva-galperin-stalkerware-kaspersky-antivirus/ [https://perma.cc/5JL7-Q8UZ].

*4. Purveyors of Nonconsensual (Sometimes Fake) Porn*

Invasions of sexual privacy are the business of countless sites. Many traffic in nonconsensual pornography—sexually explicit images disclosed without subjects' consent.[182] Sites solicit users to post people's nude photos and contact information.[183] Some are devoted to gay men and others to women.[184] Sites earn revenue from online advertising, profiting directly from their trade in human misery.[185]

Online hubs hosting nonconsensual pornography are plentiful. More than three thousand porn sites feature revenge porn as a genre.[186] Sites have also emerged that solicit users to post "deepfake" sex videos.[187] Much like revenge porn sites, the business model of these sites is online advertising, and it is lucrative. As the founder of the group Battling Against Demeaning & Abusive Selfie Sharing (BADASS) Katlyn Bowden explains, sites hosting nonconsensual pornography have grown crueler in their practices.[188]

---

182. *See* Citron & Franks, *supra* note 47, at 345-46.

183. Danielle Keats Citron & Woodrow Hartzog, *The Decision that Could Finally Kill the Revenge Porn Business*, ATLANTIC (Feb. 3, 2015), https://www.theatlantic.com/technology/archive/2015/02/the-decision-that-could-finally-kill-the-revenge-porn-business/385113/ [https://perma. cc/KE8N-9SU4].

184. I hesitate to name sites here for fear of giving publicity to destructive sexual-privacy invasions that they facilitate and encourage.

185. *See, e.g.*, Carolyn A. Uhl, Katlin J. Rhyner, Cheryl A. Terrance & Noël R. Lugo, *An Examination of Nonconsensual Pornography Websites*, 28 FEMINISM & PSYCH. 50, 51 (2018).

186. *Action Sheet on Revenge Porn*, MCALLISTER OLIVARIUS (Jan. 12, 2016), https://perma.cc/4XVN-PHG7. Even when such sites are taken down, they can reappear. For example, a notorious revenge porn site reappeared in January 2020 after being shuttered by Danish authorities in 2018. *See* Joe Uchill, *Someone Is Trying to Revive the Infamous Revenge Porn Site Anon-IB*, VICE: MOTHERBOARD (Feb. 14, 2020, 8:39 AM), https://www.vice.com/en/article/pke3j7/someone-is-trying-to-revive-the-infamous-revenge-porn-site-anon-ib [https://perma.cc/R685-W2XT]. The new site has taken the name and appearance of the old one, which gained notoriety after hosting the hacked nude photos of female celebrities in 2014. *Id.* Within three weeks of the site's reopening, over 1,500 posters had uploaded or commented on nude images. *Id.*

187. Chesney & Citron, *supra* note 47, at 1758 (2019) ("Deep-fake technology is the cutting-edge of that trend. It leverages machine-learning algorithms to insert faces and voices into video and audio recordings of actual people and enables the creation of realistic impersonations out of digital whole cloth. The end result is realistic-looking video or audio making it appear that someone said or did something. Although deep fakes can be created with the consent of people being featured, more often they will be created without it.").

188. Uchill, *supra* note 186.

Instead of considering victims' requests to remove their nude images, the most popular sites move the images behind a paywall.[189]

In a variation on this theme, software developers are creating and selling apps that allow subscribers to upload photographs of women that then generate fake nude photos. One such app was described as artificial intelligence software that "ma[de] it easy for anyone to generate realistic nude images of women simply by feeding the program a picture of the intended target wearing clothes."[190] The service charged a flat fee for the premium version.[191] Similarly, a group of programmers claims to have created an app that uses facial recognition software to cross reference faces in pornography videos and people's social media profiles.[192] One of the app's programmers states that their "goal is to help others check whether their girlfriends ever acted in those films."[193]

## II. ASSESSING THE DAMAGE AND LAW'S RESPONSE

The private sector's vast reservoirs of intimate information threaten the values and crucial life activities secured by sexual privacy, inflicting damage to human well-being. This Part takes stock of the fallout. Then, it explores existing legal protections and the gaps in the law.

### *A. Undermining the Values Secured by Sexual Privacy*

In prior scholarship, I have explored the crucial life activities and aspects of human flourishing that sexual privacy makes possible.[194]

---

189. *Id.*

190. James Vincent, *New AI Deepfake App Creates Nude Images of Women in Seconds*, VERGE (June 27, 2019, 6:23 AM), https://www.theverge.com/2019/6/27/18760896/deepfake-nude-ai-app-women-deepnude-non-consensual-pornography [https://perma.cc/MJ8X-H3PS]. Some services say that they may use the photos and post them online unless the person paying for them requests otherwise. *See* Drew Harwell, *A Shadowy AI Service Has Transformed Thousands of Women's Photos into Fake Nudes: 'Make Fantasy a Reality*,*'* WASH. POST (Oct. 20, 2020, 10:28 AM), https://www.washingtonpost.com/technology/2020/10/20/deep-fake-nudes/ [https://perma.cc/KX94-3LGZ].

191. Vincent, *supra* note 190.

192. Cara Curtis, *Creepy Programmer Builds AI Algorithm to 'Expose' Adult Actresses*, NEXT WEB (May 29, 2019), https://tnw.to/R7A0f [https://perma.cc/9KMQ-HTNX].

193. *Id.*

194. *See* Citron, *Sexual Privacy*, *supra* note 7; Citron, *Why Sexual Privacy Matters for*

Here, I will highlight them: self-development, sexual autonomy, and self-expression; dignity; intimacy; and equality. None alone are why intimate privacy matters. All are. Indeed, all are essential for human development, and all are why intimate privacy deserves robust protection.

Sexual privacy allows people to set the boundaries around their intimate lives.[195] With sexual privacy, people enjoy sexual autonomy. They get to decide who learns about their innermost fantasies, sexual history, and sexual and reproductive health.[196] They have the freedom to go "backstage" to experiment with their bodies, sexuality, and gender to express themselves as they wish, either alone or with others who they choose to share that expression.[197]

The private sector's handling of intimate data undermines our ability to decide for ourselves who has access to our intimate lives. For example, the dating app Jack'd endangered individuals' choice to keep their nude photos private by making it easy for strangers to find them online.[198] Grindr negated subscribers' decision to share intimate information only with potential partners by giving it to advertisers and analytics firms.[199] There is every reason to believe that subscribers were distressed (to say the least) by the denial of their autonomy.[200]

Private-sector surveillance of intimate information imperils self-expression and the ability of people to explore new information and ideas.[201] The social conformity theory of chilling effects helps explain

---

*Trust*, *supra* note 47. My book project, tentatively entitled *The Privacy Mirage: How Intimacy Became Data and How to Protect It*, will explore the global threat to intimate privacy and make the case for intimate privacy as a human or civil right deserving robust protection.

195. My prior work explores the value of sexual privacy in great detail. *See* Citron, *Sexual Privacy*, *supra* note 7, at 1882-93; Citron, *Why Sexual Privacy Matters for Trust*, *supra* note 47, at 1193-1203 (exploring the importance of sexual privacy for trust in intimate relationships).

196. Citron, *Sexual Privacy*, *supra* note 7, at 1880, 1882.

197. *See id.* at 1883-85.

198. Christian Gollayan, *Gay Dating App Jack'd Exposed Millions of Nude Photos*, N.Y. POST (Feb. 7, 2019, 4:07 PM), https://nypost.com/2019/02/07/gay-dating-app-jackd-exposed-millions-of-nude-photos/ [https://perma.cc/4DJV-ZMCV].

199. Julia Belluz, *Grindr Is Revealing Its Users' HIV Status to Third-Party Companies*, VOX (Apr. 3, 2018, 10:26 AM), https://www.vox.com/2018/4/2/17189078/grindr-hiv-status-data-sharing-privacy [https://perma.cc/EB42-72DJ].

200. *See, e.g.*, Gollayan, *supra* note 198.

201. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1260 (1998). For a masterful exploration of the importance of intellectual privacy, see NEIL

why.[202] People may refrain from searching, browsing, and expressing themselves if their expression and exploration fall outside of the mainstream.[203] Fearing that intimate information may be collected and shared in unwanted ways, people may stop visiting sites devoted to gender, sexuality, or sexual health. They may not use period-tracking apps that help them manage anxiety, pain, and uncertainty.[204] They may stop visiting adult sites that enable "vicarious expression and satisfaction of minority interests that are difficult, embarrassing, and occasionally illegal to indulge in reality."[205] They might avoid communicating about intimate matters for fear of unwanted exposure.[206] Self-censorship can be subtle, though significant, for self-development and self-expression. As Jonathon Penney explains, we may see this chilling when people change their modes of engagement and expression from experimental, nonmainstream ones to more socially conforming, mainstream ones.[207]

Public health officials feared this kind of chilling effect after news broke that Grindr had shared its customers' HIV status with analytics firms.[208] A Grindr subscriber told BuzzFeed News that he removed his HIV status from his profile after learning about the

---

M. RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE (2015). Sexual privacy and intellectual privacy are both foundational privacy rights that often intersect. *See id.*

202. *See* Jonathon W. Penney, Understanding Chilling Effects and Their Harms 50-51 (June 2, 2020) (unpublished manuscript) (on file with author) [hereinafter Penney, *Harms*]; Penney, *Case Study*, *supra* note 29, at 1; Alex Marthews & Catherine Tucker, *The Impact of Online Surveillance on Behavior*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 437, 437 (David Gray & Stephen E. Henderson eds., 2017); Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, JOURNALISM & MASS COMMC'N Q., 2016, at 1, 1-3.

203. Penney, *Harms*, *supra* note 202, at 58-62.

204. *See* Khan, *supra* note 65.

205. Maris et al., *supra* note 2, at 2020 (quoting LARRY GROSS, UP FROM INVISIBILITY: LESBIANS, GAY MEN, AND THE MEDIA IN AMERICA 221 (2001)). *See generally* Sharif Mowlabocus, *Porn 2.0? Technology, Social Practice, and the New Online Porn Industry*, *in* PORN.COM: MAKING SENSE OF ONLINE PORNOGRAPHY 69 (Feona Attwood ed., 2010).

206. *See* Maris et al., *supra* note 2, at 2019; Marthews & Tucker, *supra* note 202, at 446-48.

207. Penney, *Harms*, *supra* note 202, at 66.

208. Belluz, *supra* note 199. In response to news that analytics firms obtained people's HIV status from dating sites like Grindr, sexual health researcher Dr. Jeffrey Klausner underscored his "concern[] that this would undermine years of efforts to promote people recording their HIV status in their profile, and sharing their status with others to promote safer sex." *Id.*

disclosure. He explained that "[s]ome people's jobs may be in jeopardy if the wrong people find out about their status—or maybe they have difficult family situations.... It can put people in danger, and it feels like an invasion of privacy."[209] This example is consistent with studies showing that victims of nonconsensual pornography tend to withdraw from online engagement and expression.[210]

The loss of sexual privacy undermines human dignity by changing self-perception. When people realize their intimate life is being observed, tracked, and trafficked, they view themselves as "*something* seen through another's eyes."[211] As Anita Allen explains, privacy invasions risk "form[ing] humiliating, despicable pictures of their victims that interfere with their victims' self-concepts and self-esteem, making them doubt they are the people they have worked to be."[212] The loss of sexual privacy also undermines dignity by having others see people as just parts of their intimate lives and not as fully integrated human beings.[213]

When people's nude photos are posted online without consent, they see themselves as just their genitals or breasts and believe that others will see them that way. For example, in 2018, a young lawyer stayed in a hotel for work.[214] Without her knowledge or permission, a hotel employee placed a camera in the bathroom and recorded her as she showered.[215] The employee posted the video and her personal

209. Ghorayshi & Ray, *supra* note 6.

210. *See generally* CITRON, HATE CRIMES IN CYBERSPACE, *supra* note 23; Danielle Keats Citron, *Civil Rights in Our Information Age*, *in* THE OFFENSIVE INTERNET: SPEECH, PRIVACY, AND REPUTATION 31, 31 (Saul Levmore & Martha C. Nussbaum eds., 2010); Danielle Keats Citron & Jonathon W. Penney, *When Law Frees Us to Speak*, 87 FORDHAM L. REV. 2317, 2327-32 (2019); Danielle Keats Citron & Neil M. Richards, *Four Principles for Digital Expression (You Won't Believe #3!)*, 95 WASH. U. L. REV. 1353, 1365 (2018) ("[N]ot everyone can freely engage online. This is especially true for women, minorities, and political dissenters who are more often the targets of cyber mobs and individual harassers."); Citron & Franks, *supra* note 47, at 385; Citron, *Cyber Civil Rights*, *supra* note 40, at 106.

211. Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 223, 227 (Ferdinand David Schoeman ed., 1984) (emphasis added).

212. ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? 15 (2011).

213. *See* Citron, *Sexual Privacy*, *supra* note 7, at 1882-84.

214. Phone Interview with Joan (Oct. 15, 2018); Interview with Joan (May 3, 2019). I will explore the invasion of Joan's sexual privacy in greater detail in my book project. *See supra* note 194.

215. Interview with Joan (Oct. 15, 2018), *supra* note 214.

details on various porn sites.[216] The woman told me that after finding out about the postings, she despaired at seeing herself and at being seen as just a naked body relieving and washing herself.[217]

Private-sector handling of intimate information can jeopardize the trust that is essential for the development of intimate relationships. As Charles Fried argued years ago, privacy is the "oxygen" for intimacy.[218] Intimacy develops as partners share vulnerable aspects of themselves.[219] Partners must believe that their confidences will be kept not only by their partners but also by the firms handling their intimate information. If people lose faith in the companies facilitating their intimate interactions, then they may stop using their services, to the detriment of the project of intimacy. The loss of trust is especially profound when sites disclose people's nude images without consent. People stop dating for fear that future partners will frequent porn sites and revenge porn sites to post their nude photos in violation of their trust and confidence.[220]

Equal opportunity is on the line as well. The surveillance of intimate life will be particularly costly to women, sexual minorities, and nonwhite people. The damage stems from demeaning gender, racial, and homophobic stereotypes and the social construction of sexuality.[221] When heterosexual men appear in videos having sex or are designated as users of sex toys, they may even be socially empowered by the performance or activity whereas women, racial minorities, and LGBTQ individuals are stigmatized, marginalized, and disempowered.[222] Women, sexual minorities, and nonwhites are marked by stereotypes and other social forces that reconstruct them "as devian[t] and inferior[ ]" and "confine them to a nature which is often attached in some way to their bodies, and which thus cannot easily be denied."[223] Martha Nussbaum explains that "a universal

---

216. *Id.* The perpetrator sent a video of her showering to her LinkedIn contacts. *Id.*

217. *Id.*

218. *See* Fried, *supra* note 24, at 477-78.

219. *See id.* at 484; Citron, *Why Sexual Privacy Matters for Trust*, *supra* note 47, at 1200-01.

220. Citron, *Why Sexual Privacy Matters for Trust*, *supra* note 47, at 1209. When domestic violence victims learn that they are being tracked on their cellphones, they may fear purchasing new phones lest abusers install a cyber stalking app again.

221. *See* CITRON, HATE CRIMES IN CYBER SPACE, *supra* note 23, at 14-15.

222. *See id*; Citron, *Sexual Privacy*, *supra* note 7, at 1908, 1919-20, 1928.

223. IRIS MARION YOUNG, JUSTICE AND THE POLITICS OF DIFFERENCE 59 (1990). Stereotypes

human discomfort with bodily reality" often works to undermine women, sexual minorities, and nonwhite people as disgusting and pathological.[224] As Kimberlé Crenshaw's "intersectionality" framework shows, the forces that marginalize individuals tend to operate on multiple levels, often compounding the harm suffered.[225]

Consider the disproportionate impact of sites trafficking in nonconsensual pornography. A majority of the nude images posted online without consent involve women and sexual minorities.[226] Thus, nonconsensual porn impacts women and girls far more frequently than men and boys.[227] Individuals who identify as sexual minorities are more likely than heterosexual individuals to experience threats of, or actual, nonconsensual pornography.[228] As Ari Waldman has found, gay and bisexual male users of geosocial dating apps are more frequently victims of nonconsensual pornography than both the general population and the broader lesbian, gay, and bisexual communities.[229]

We see the disproportionate impact on women featured on deep fake sex video sites. According to a 2019 study, 96 percent of all of the nearly fifteen thousand deep fake videos online are deep fake

---

often place women, sexual minorities, and nonwhite people into an experience of "double consciousness" so that information is inevitably interpreted to their disadvantage. *See id.* at 60. For instance, if information suggests that a woman is sexually active, then she will be viewed as a slut; if information suggests that a woman is sexually inactive, then she will be viewed as frigid, manhater, or a lesbian. *See id.* at 59-60.

224. MARTHA C. NUSSBAUM, FROM DISGUST TO HUMANITY: SEXUAL ORIENTATION AND CONSTITUTIONAL LAW, at xv (2010).

225. Kimberlé Crenshaw, *Mapping the Margins: Intersectionality, Identity Politics, and Violence Against Women of Color*, 43 STAN. L. REV. 1241, 1244 (1991).

226. ASIA A. EATON, HOLLY JACOBS & YANET RUVALCABA, CYBER C.R. INITIATIVE, 2017 NATIONWIDE ONLINE STUDY OF NONCONSENSUAL PORN VICTIMIZATION AND PERPETRATION: A SUMMARY REPORT 12 (2017), https://www.cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf [https://perma.cc/DL6C-AQ6U]. For other studies confirming this finding, see Citron, *Sexual Privacy*, *supra* note 7, at 1919 n.307.

227. *See* EATON ET AL., *supra* note 226, at 12.

228. *See* Citron, *Sexual Privacy*, *supra* note 7, at 1919-20 (discussing various studies confirming this finding); Ari Ezra Waldman, *Law, Privacy, and Online Dating: "Revenge Porn" in Gay Online Communities*, 44 LAW & SOC. INQUIRY 987, 987 (2019) ("According to the Data & Society Research Institute, 15 percent of lesbian, gay, and bisexual (LGB) Internet users report that someone has threatened to share their explicit images; 7 percent say someone has actually done it." (citing AMANDA LENHART, MICHELLE YBARRA & MYESHIA PRICE-FEENEY, DATA & SOC. RSCH. INST., NONCONSENSUAL IMAGE SHARING: ONE IN 25 AMERICANS HAS BEEN A VICTIM OF 'REVENGE PORN' (2016))).

229. Waldman, *supra* note 228, at 988.

sex videos and 99 percent of those videos involve inserting women's faces into porn without consent.[230] In the past year, the number of deep fake sex videos has grown exponentially as has deep fake sex videos featuring women without consent.[231]

Consider the potential risks to women as a result of femtech services.[232] According to media reports, some employers and health insurers have access to employees' period- and fertility-tracking apps.[233] Women's intimate information could be used to raise the cost of employer-provided health insurance, adjust wages, or scale back employment benefits.[234] It could affect the ability to obtain life insurance, keep jobs, and get promotions. Medical researcher Paula Castaño explains that the information tracked by fertility apps raises concerns because it offers little insight as a clinical matter and instead "focus[es] on variables that affect time out of work and insurance utilization."[235]

If intimate information is shared with data brokers, it could be used in the actuarial scoring of women, sexual minorities, and non-white people to their detriment. As the Federal Trade Commission explains, data brokers' scoring processes are not transparent, which "means that consumers are unable to take actions that might mitigate the negative effects of lower scores, such as being limited

---

230. HENRY AJDER, GIORGIO PATRINI, FRANCESCO CAVALLI & LAURENCE CULLEN, DEEPTRACE, THE STATE OF DEEPFAKES: LANDSCAPE, THREATS, AND IMPACT 1-2 (2019), https://regmedia.co.uk/2019/10/08/deepfake_report.pdf [https://perma.cc/3P8K-J62S]. Eight of the top ten pornography websites host deepfake pornography, and there are nine deepfake pornography websites hosting 13,254 fake porn videos (mostly featuring female celebrities without their consent). *Id.* at 6. These sites generate income from advertising. *Id.* Indeed, as the first comprehensive study of deepfake video and audio explains, "[D]eepfake pornography could represent a growing business opportunity, with all these websites featuring some form of advertising." *Id. See generally* Chesney & Citron, *supra* note 47, at 1758.

231. Zoom Interview with Henry Ajder, Head of Commc'ns & Rsch., Deeptrace (now Sensity).

232. As discussed above, this is a direct result of the work of femtech companies. *See supra* notes 35-40 and accompanying text.

233. Harwell, *supra* note 9.

234. *Id.* The video game company Activision Blizzard pays employees a dollar a day to give it access to the data that they generate with a pregnancy-tracking app provided by Ovia Health. *Id.* The company uses a special version of the app that relays health data in de-identified form to the employer's internal website accessible by human resources personnel. *Id.* Ovia Health contends that intimate information can help employers cut back on medical costs and help usher women back to work after birth. *Id.*

235. *Id.*

to ads for subprime credit or receiving different levels of service from companies."[236] Moreover, insurance companies can potentially use scoring processes to infer that individuals are "higher risk."[237] Finally, scoring processes could negatively impact the interest rates charged on loans.[238] News about the disproportionately higher creditworthiness of men as compared to women for Apple's new credit card demonstrates the point.[239]

Reservoirs of intimate information shared with advertisers and sold to data brokers make their way into the hands of vendors who use that data to train algorithms used in hiring, housing, insurance, and other crucial decisions.[240] As more intimate information is collected, used, and shared, it will increasingly be used to entrench bias. People's sexual assaults, abortions, painful periods, HIV infections, escort use, extramarital affairs, and porn preferences may be used to train job-recruitment and housing-matching algorithms.[241] A wealth of scholarship and research explores the discriminatory impacts of algorithmic discrimination in the commercial sector.[242] A prevailing concern is that algorithmic tools "replicate

236. FTC, DATA BROKERS, *supra* note 165, at 48.

237. *Id.*

238. Rosato, *supra* note 60.

239. *E.g.*, Neil Vigdor, *Apple Card Investigated After Gender Discrimination Complaints*, N.Y. TIMES (Nov. 10, 2019), https://nyti.ms/2CuelOT [https://perma.cc/DVX5-ERCE].

240. *EPIC AI Rulemaking Petition*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/ftc/ai/epic-ai-rulemaking-petition/#legal [https://perma.cc/AW4S-ZB3U]. *See generally* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 18-20 (2014).

241. *See, e.g.*, *Complaint and Request for Investigation, Injunction, and Other Relief*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/ftc/airbnb/EPIC_FTC_Airbnb_Complaint_Feb2020.pdf [https://perma.cc/F3XE-CWX9]. EPIC raised concerns about Airbnb's deployment of a "risk assessment" tool that assigns secret ratings to prospective renters based on behavioral traits using an opaque proprietary algorithm that is trained on personal information obtained from third parties. *Id.* at 5. The complaint noted that Airbnb's machine learning inputs include personal data collected from "web pages, information from databases, posts on the person's social network account," and other information. *Id.* Moreover, "Airbnb's algorithm claims to identify 'negative traits' including whether the individual ... is involved in sex work, ... is involved in pornography ... , or has interests that indicate negative personality or behavior traits." *Id.* (quoting U.S. Patent No. 9,070,088 col. 2 l. 7-15 (filed June 30, 2015)).

242. Solon Barocas, Kate Crawford, Deborah Hellman, Anna Lauren Hoffman, Ifeoma Injuwa, Pauline Kim, Jason Schultz, Andrew Selbst, and Meredith Whittaker have been doing pathbreaking work in this area. *See, e.g.*, CAROLINE CRIADO PEREZ, INVISIBLE WOMEN: DATA BIAS IN A WORLD DESIGNED FOR MEN (2019); Anna Lauren Hoffmann, *Data Violence and How Bad Engineering Choices Can Damage Society*, MEDIUM (Apr. 30, 2018), https://medium.com/s/story/data-violence-and-how-bad-engineering-choices-can-damage-society-39e44150e1d4

historical hierarchies by rendering people along a continuum of least to most 'valuable.'"[243]

The opacity of commercial algorithms makes identifying and challenging discrimination difficult.[244] But examples do exist. Consider, for example, Amazon's experimental hiring tool that ranked job candidates by learning from data about the company's past practices. A *Reuters* story revealed that the hiring algorithm "downgraded" resumes from candidates who attended two women's colleges along with any resume that included the word "women's."[245] Amazon abandoned the tool when it could not ensure that it was not free of bias against women.[246]

### *B. Surveying the Damage*

The widespread collection, storage, use, and disclosure of intimate information risks emotional, physical, and reputational harm. It makes people vulnerable to manipulation, blackmail, and

---

[https://perma.cc/C4JE-HYS7]; Inioluwa Deborah Raji & Joy Buolamwini, *Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products*, PROC. CONF. ON A.I., ETHICS, & SOC'Y, Jan. 2019, at 429; Allyson E. Gold, *Redliking: When Redlining Goes Online*, 62 WM. & MARY L. REV. 1841 (2021).

243. WEST ET AL., *supra* note 34, at 10; *see also* Jevan Hutson, Jessie G. Taft, Solon Barocas & Karen Levy, *Debiasing Desire: Addressing Bias & Discrimination on Intimate Platforms*, 2 PROC. ASS'N COMPUTING MACH. HUM.-COMPUT. INTERACTION, Nov. 2018, at 2, 4-8; Sasha Costanza-Chock, *Design Justice, A.I., and Escape from the Matrix of Domination*, J. DESIGN & SCI. (July 16, 2018), https://jods.mitpress.mit.edu/pub/costanza-chock [https://perma.cc/MEN5-2438]; Kate Crawford, *Artificial Intelligence's White Guy Problem*, N.Y. TIMES (June 25, 2016), https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html [https://perma.cc/PP7V-RFJP].

244. *See*, *e.g.*, *In re HireVue*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/ftc/hirevue/ [https://perma.cc/Z5R4-RXHK] (arguing that "hiring algorithms are more likely to be biased by default" and that HireVue keeps secret "the training data, factors, logic, or techniques used to generate each algorithmic assessment"). Indeed, career staff in the offices of state attorneys general have told me that the most challenging problem is figuring out which of the countless vendors to target with civil investigative demands and the likelihood that those demands will be met by claims of trade secrecy.

245. Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women*, REUTERS (Oct. 10, 2018, 7:04 PM), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G/ [https://perma.cc/6JZT-ZC4S].

246. *Id.*

extortion.[247] The examples of suffering are as plentiful as they are disturbing.

Consider the aftermath of the hack of Ashley Madison for John Gibson, a married father and Baptist minister who was one of many exposed in the hack. He committed suicide days after the public learned about the hack.[248] Gibson's wife explained that her husband's suicide note described his deep shame at having his name on the site: "We all have things that we struggle with, but it wasn't so bad that we wouldn't have forgiven it.... But for John, it carried such a shame, and he just couldn't see that."[249] Gibson's daughter likewise concluded that at least "part of the reason ... he killed himself [was] because he wasn't willing to share his shame with [his family]."[250] Gibson's wife believed that he was "worried about losing his job."[251] In disputing rumors that Gibson was fired, however, his daughter explained that he resigned after the church learned about the exposure of his information in the hack.[252] Gibson's fear about losing his job was well-founded. Victims of sexual-privacy invasions have been fired or encountered great difficulty obtaining work.[253]

Stories abound of scammers using emails and passwords hacked from porn sites to blackmail people. Criminals write to individuals claiming they recorded them watching porn online and demanding money to keep the videos secret. Over a seven-month stretch in 2018, victims lost $332,000 to these scams.[254] More than 89,000

247. For a superb discussion of such risks for governmental and private sector collection of personal data, see Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1953-54 (2013).

248. Broder Van Dyke, *supra* note 112. Gibson's was not the only suicide related to the Ashley Madison hack. Two people in Canada killed themselves in the wake of the leak. Chris Baraniuk, *Ashley Madison: 'Suicides' Over Website Hack*, BBC (Aug. 24, 2015), https://www.bbc.com/news/technology-34044506 [https://perma.cc/ATH5-4D4B].

249. Broder Van Dyke, *supra* note 112.

250. Jon Ronson, *The Yes Ladder*, THE BUTTERFLY EFFECT, at 19:10 (Nov. 3, 2017), https://www.stitcher.com/show/the-butterfly-effect-with-jon-ronson/episode/the-butterfly-effect-ep-5-the-yes-ladder-52105431 [https://perma.cc/UZS6-MVBP].

251. Broder Van Dyke, *supra* note 112.

252. Ronson, *supra* note 250, at 12:26.

253. CITRON, HATE CRIMES IN CYBERSPACE, *supra* note 23, at 193; *see, e.g.*, Complaint for Permanent Injunction & Other Equitable Relief at 14, FTC v. EMP Media, Inc., No. 2:18-cv-00035-APG-NJK, 2018 WL 372707 (D. Nev. Jan. 9, 2018) (explaining that victims of nonconsensual pornography "have lost their jobs—or are concerned that they might be fired from a current job").

254. Isobel Asher Hamilton, *Criminal Groups Are Offering $360,000 Salaries to*

people were targeted, and on average they paid $540.[255] Increasingly, criminals are targeting high-earning victims, including company executives, doctors, and lawyers.[256]

The national security implications of this kind of activity are significant. The concentration of sensitive information on dating sites presents an inviting target for governments seeking leverage over political activists, dissidents, or foreign agents.[257] National security experts raised these concerns after the Chinese government bought the gay dating app Grindr.[258] Peter Mattis, a former U.S. government analyst and China specialist, remarked:

> What you can see from Chinese intelligence practices is a clear effort to collect a lot of personal information on a lot of different people, and to build a database of names that's potentially useful either for influence or for intelligence.... Then later, when the party-state comes into contact with someone in the database, there's now information to be pulled.[259]

Criminals and hostile states are not the only ones who exploit intimate information to serve their own ends at the expense of ours. When companies use people's acute emotional fragility or membership in a protected class to override their wishes, their actions can

---

*Accomplices Who Can Help Them Scam CEOs About Their Porn-Watching Habits,* BUS. INSIDER (Feb. 24, 2019, 3:06 AM), https://www.businessinsider.com/scammers-squeezed-330000-people-webcam-porn-2019-2 [https://perma.cc/PV6D-9FMD].

255. *Id.*

256. *Id.*

257. "Tinder is the fourth dating app in the nation to be forced to comply with the Russian government's request for user data, Moscow Times reports, and it's among 175 services that have already consented to share information with the nation's Federal Security Service, according to a registry online." Melanie Ehrenkranz, *The Russian Government Now Requires Tinder to Hand Over People's Sexts*, GIZMODO (June 3, 2019, 12:05 PM), https://gizmodo.com/the-russian-government-now-requires-tinder-to-hand-over-1835201563 [https://perma.cc/58PA-AQ7U]. In response to these reports a Tinder spokesperson asserted that "this registration in no way shares any user or personal data with any Russian regulatory bodies and we have not handed over any data to their government." *Id.*

258. Steven Blum, *What Does a Chinese Company Want with Gay Hookup App Grindr?*, L.A. MAG. (Nov. 4, 2019), https://www.lamag.com/citythinkblog/grindr-china-fbi/ [https://perma.cc/N5JM-THH5].

259. Josh Rogin, *Can the Chinese Government Now Get Access to Your Grindr Profile?*, WASH. POST (Jan. 12, 2018, 6:00 AM), https://www.washingtonpost.com/news/josh-rogin/wp/2018/01/12/can-the-chinese-government-now-get-access-to-your-grindr-profile/ [https://perma.cc/3X82-A6LE].

be viewed as "dark patterns."[260] "The Spinner" exemplifies the troubling nature of dark patterns. It promises to bend the will of people's intimate partners with its advertising services.[261] The online service sends innocent-looking links to people via text that, when clicked, create cookies that send targeted advertisements.[262] The company claims to have swayed people to get back together with lovers, to initiate sex, and to settle their divorces.[263] The company's most requested service is its "Initiate Sex" feature, which sends ads trumpeting reasons why people should initiate sex.[264]

Another illustration of troubling manipulation is the period-tracking app FEMM, which uses subscribers' intimate information to dissuade them from terminating their pregnancies.[265] An anti-abortion group runs the app, but it does not disclose that to subscribers.[266] The app's marketing materials simply say:

> Are you looking to track your menstrual cycles and symptoms, get pregnant or avoid pregnancy? The FEMM app is more than just a period tracker: it provides you with cutting edge science that helps you keep track of your health, understand what is going on with your body, flag potential issues and connect with

260. STIGLER COMM. ON DIGIT. PLATFORMS, *supra* note 15, at 240-41. As the Stigler report notes, using personal data to manipulate people can be benign, such as by serving them ads for restaurants around lunchtime. *Id.* Yet the practice is morally and legally troubling when companies use sensitive data to exploit and manipulate people. *Id.* The Stigler report invokes the concept of dark patterns to evaluate user-interface systems that nudge people to disclose information that they otherwise would not disclose if they had time to consider the implications. *Id.* Such systems might not be understood as deceptive under traditional understanding of consumer protection laws. *Id.* at 249.

261. Parmy Olson, *For $29, This Man Will Help Manipulate Your Loved Ones with Targeted Facebook and Browser Links*, FORBES (Jan. 15, 2019, 7:20 AM), https://www.forbes.com/sites/parmyolson/2019/01/15/a-shadowy-entrepreneur-claims-his-online-manipulation-business-is-thriving/#6176936572a9 [https://perma.cc/3NNN-CN5D].

262. *Id.*; Fiona Tapp, *New Service Promises to Manipulate Your Wife into Having Sex with You*, ROLLING STONE (Aug. 18, 2018, 11:38 AM), https://www.rollingstone.com/culture/culture-features/spinner-service-manipulate-wife-sex-712385/ [https://perma.cc/X2D9-UY55].

263. Kevin Poulsen, *For $29, This Company Swears It Will 'Brainwash' Someone on Facebook*, DAILY BEAST (Jan. 22, 2019, 10:07 AM), https://www.thedailybeast.com/for-dollar29-this-company-swears-it-will-brainwash-someone-on-facebook [https://perma.cc/3RBW-5N8L].

264. *Id.*

265. Jessica Glenza, *Revealed: Women's Fertility App Is Funded by Anti-Abortion Campaigners,* GUARDIAN (May 30, 2019, 2:00 AM), https://www.theguardian.com/world/2019/may/30/revealed-womens-fertility-app-is-funded-by-anti-abortion-campaigners [https://perma.cc/ZHD9-H6QM].

266. *Id.*

> a network of doctors and nurses to provide you the best health care. We're a new revolution in women's health![267]

The app provides materials claiming that birth control is unsafe and highlighting information that promotes pregnancy.[268] The app misleads subscribers about its motives and propagates misinformation.[269]

### *C. Understanding the Legal Landscape*

In the United States, information privacy law does little to curtail the private sector's amassing of vast amounts of intimate information, at least outside of the provision of health care.[270] It generally presumes the propriety of commercial collection of personal data.[271] As William McGeveran explains in his influential privacy casebook, American law treats the processing of personal data as both inevitable and prosocial.[272]

#### *1. Privacy Legislation*

American privacy law generally does not curtail data collection.[273] Instead, it focuses on procedural protections, such as ensuring the transparency of corporate data practices (referred to as notice) and

---

267. *FEMM Health Period and Ovulation Tracker*, GOOGLE PLAY, https://play.google.com/store/apps/details?id=org.femmhealth.femm&hl=en_US [https://perma.cc/LNA2-NCRU].

268. *See* Glenza, *supra* note 265.

269. *See id.*

270. The Children's Online Privacy Protection Act (COPPA) of 1998 is the rare exception. It limits the collection of children's online information to instances in which parents have explicitly provided consent. Children's Online Privacy Protection Act of 1998 § 1303(a), 15 U.S.C. § 6502. Similarly, in the European Union, the GDPR protects information pertaining to individuals' "sex life" as sensitive information, precluding its collection except upon explicit consent. GDPR, *supra* note 103, at 38.

271. Citron, *A Poor Mother's Right to Privacy*, *supra* note 8, at 1141.

272. *See* WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 382-83 (2016); Citron, *Reservoirs of Danger*, *supra* note 44, at 245.

273. Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 771 (2016) [hereinafter Citron, *Privacy Policymaking*]. Some states limit commercial contexts in which Social Security numbers and zip codes can be collected. *See, e.g.*, CAL. CIV. CODE § 1798.85 (West 2015) (Social Security numbers); TEX. BUS. & COM. CODE ANN. § 505.003 (West 2009) (zip codes).

securing certain rights over personal data (referred to as choice).[274] Even its more reform-oriented elements continue this trend. For example, the California Consumer Privacy Act (CCPA), enacted in 2018, gives consumers the right to know what personal information has been collected and to opt-out of its sale.[275]

So long as companies post privacy policies and offer opt-out rights under state law,[276] they can largely collect, use, and sell intimate information without limitation.[277] It should therefore not be a surprise that Grindr's privacy policy warns that its advertising partners may "also collect information directly from you."[278] The femtech market is doing the same. A recent study showed that ten popular fertility-tracking apps including Clue sold subscribers' personal information to at least 135 companies.[279] Individuals should not be reassured if companies pledge to de-identify intimate information before selling it given the ease of re-identification.[280] As

274. *See, e.g.*, CAL. BUS. & PROF. CODE § 22575 (West 2014); CAL. CIV. CODE § 1798.100 (West 2020). State attorneys general played an important role in getting legislation passed to require privacy policies. Citron, *Privacy Policymaking*, *supra* note 273, at 764-65.

275. *See* California Consumer Privacy Act, CAL. CIV. CODE §§ 1798.100-.198. Under the CCPA, websites must detail the categories of personal information that they collect and the categories of third parties with whom that information may be shared. *Id.* On the CCPA generally and its comparison to GDPR, see Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733 (2021).

276. *See* CAL. CIV. CODE § 1798.120. Of course, compliance with notice requirements is not perfect. For instance, according to researchers, only 11 percent of the privacy policies posted by porn sites disclose that third-party trackers may be collecting visitors' information. Maris et al., *supra* note 2, at 2027. Many consumers will not invoke their opt-out rights due to the stickiness of defaults and the sheer number of companies that would need to be contacted to make a dent in the effort to reduce the trafficking of one's personal information. *See generally* WOODROW HARTZOG, PRIVACY'S BLUEPRINT (2018).

277. *See* Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1723 (2020). Indeed, a long-standing critique of the fair information practice principles is that they enable data collection to proceed unencumbered for the sake of efficiency. JAMES RULE, DOUGLAS MCADAM, LINDA STEARNS & DAVID UGLOW, THE POLITICS OF PRIVACY 93 (1980).

278. Thomas Germain, *Popular Apps Share Intimate Details About You with Dozens of Companies*, CONSUMER REPS. (Jan. 14, 2020), https://www.consumerreports.org/privacy/popular-apps-share-intimate-details-about-you/ [https://perma.cc/NN9D-DRU9].

279. Rosato, *supra* note 60.

280. Dániel Kondor, Behrooz Hashemian, Yves-Alexandre de Montjoye & Carlo Ratti, *Towards Matching User Mobility Traces in Large-Scale Datasets*, IEEE TRANSACTIONS ON BIG DATA, Sept. 24, 2018, at 1, 10.

Julie Cohen has underscored, American informational capitalism is built on the edifice of this legal structure.[281]

Under federal and state law, companies must store intimate information in a reasonably secure manner. Legal obligations stem from data security,[282] data disposal,[283] encryption,[284] breach notification,[285] and unfair and deceptive acts and practices (UDAP) laws.[286] Companies may have a duty to adopt certain data security practices, such as having a comprehensive data-security program addressing potential risks to consumers.[287] As explored below, companies have faced suit for inadequately securing intimate information.

One might assume that privacy law limits all of the private sector's collection of intimate information related to health conditions. The crucial protections of the federal Health Insurance Portability and Accountability Act (HIPAA),[288] however, only cover data collected during the provision of health care and not health data generally. HIPAA is a health care portability law with privacy protections, not a health privacy bill.[289] It covers particular health-care providers (known as covered entities), such as medical practices, hospitals, and health insurance companies.[290] HIPAA, for

---

281. Cohen, *supra* note 43, at 11 ("Data harvesting and processing are one of the principal business models of informational capitalism, so there is little motivation either to devise more effective methods of privacy regulation or to implement existing methods more rigorously.").

282. *See, e.g.*, CAL. CIV. CODE § 1798.81.5(b) (West 2020); 201 MASS. CODE REGS. 17.01(1) (LexisNexis 2020).

283. *See, e.g.*, CONN. GEN. STAT. ANN. § 42-471 (West 2017); MASS. GEN. LAWS ANN. ch. 93I, § 2 (West 2008).

284. *See, e.g.*, CAL. CIV. CODE § 1798.85(a)(3).

285. *See, e.g.*, *id.* § 1798.82.

286. *See, e.g.*, CONN. GEN. STAT. ANN. § 42-110a to -110q.

287. William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1140, 1176-1180 (2019).

288. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 194-191, 110 Stat. 1936.

289. *Id.* (describing HIPAA as a law that Congress enacted "to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes").

290. When it enacted HIPAA in 1996, Congress delegated authority to the Department of Health and Human Services (HHS) to enact national data privacy or confidentiality and data security standards. ALLEN, *supra* note 212, at 113-14. HHS issued its Standards for Privacy of Individually Identifiable Health Information in 2000, which is commonly known as the

instance, requires that covered entities obtain consent before using or disclosing individually identifiable "protected health information."[291] That provision does not apply to the broad array of non-covered entities, including femtech apps, search engines, medical information sites, or dating sites.[292] When a dating app collects people's HIV status or when a femtech app amasses the dates of abortions and miscarriages, it is not constrained by HIPAA's obligations around explicit consent.[293]

*2. Privacy Policy Making of Law Enforcers*

In the rare case, the Federal Trade Commission and state attorneys general have set norms around the collection and storage of intimate information.[294] Federal and state UDAP laws provide support for this activity.[295] The following examples provide precedent

---

HIPAA Privacy Rule. OFF. FOR C.R., DEP'T HEALTH & HUM. SERVS., OCR PRIVACY BRIEF: SUMMARY OF THE HIPAA PRIVACY RULE 1-2, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html [https://perma.cc/5FUP-CWXT]. The HIPAA Privacy Rule applies only to covered entities—healthcare providers who engage in certain electronic healthcare transactions, health plans, and healthcare clearinghouses like hospital billing providers and insurers. 45 C.F.R. §§ 160.102-103 (2019).

291. *See* 45 C.F.R. § 164.502(a).

292. *See id.* §§ 160.102-03. Period-tracking app Ovia claims to comply with HIPAA, surely due to the fact that the company shares de-identified data with employers who provide health insurance to employees. Harwell, *supra* note 9.

293. In *FAA v. Cooper*, the Supreme Court considered whether the Federal Aviation Administration's disclosure of a pilot's HIV status to another federal agency without consent violated the Privacy Act of 1974. 566 U.S. 284, 289 (2012). The Court found that the plaintiff's emotional distress did not amount to "actual damages"—which would require proof of economic harm. *Id.* at 302.

294. Citron, *Privacy Policymaking, supra* note 273, at 773-75. The Consumer Financial Protection Bureau also has the authority to regulate abusive conduct, at least within the banking and financial services sector. *See* 12 U.S.C. § 5531. Under 12 U.S.C. § 5531, an abusive practice is one that "materially interferes with the ability of ... consumer[s] to understand a term or condition of a consumer financial product or service or ... takes unreasonable advantage of" their lack of understanding of such a service or product's "material risks" or of their inability to protect their interests. *Id.* § 5531(d).

295. The Federal Trade Commission has enforcement authority to police unfair and deceptive commercial acts and practices under section 5 of the Federal Trade Commission Act. Federal Trade Commission Act § 5, 15 U.S.C. § 45. In the 1970s, state lawmakers followed the federal government's lead in adopting so-called baby section 5 acts, that is, UDAP laws. *See* Citron, *Privacy Policymaking*, *supra* note 273, at 754. With this authority, state attorneys general have served as crucial privacy norm entrepreneurs using their authority under state UDAP laws. *Id.* at 763-78. I had the great fortune of witnessing creative state attorney general privacy policy making in advising then-California AG Kamala Harris from 2014 to 2016.

for entities handling intimate information in the relevant jurisdictions.

The Massachusetts Attorney General's office has considered the collection of information about women's visits to abortion clinics, inferred from geolocation data, to constitute an unfair and deceptive business practice.[296] In 2015, an advertising company in Brookline, Massachusetts, was hired to bombard "abortion-minded women" with pro-life advertisements as they visited certain health providers.[297] Geofencing technology was key to the effort. It let the advertising company target women's cell phones as they entered "Planned Parenthood clinic[s], hospitals, [and] doctor's offices that perform abortions."[298] Women saw ads entitled "Pregnancy Help," "You Have Choices," and "You're Not Alone" that linked to live web chats with a "pregnancy support specialist."[299] Once an individual's device had been tagged, then that person would continue to see pro-life ads for the next thirty days.[300]

The Massachusetts Attorney General's office viewed the company's collection of location data to infer women's pregnancies as constituting an unfair and deceptive business practice.[301] The

*Id.* at 773 n.174.

296. Assurance of Discontinuance at 4-5, *In re* Copley Advertising, LLC, No. 1784CV01033 (Mass. Super. Ct. Apr. 4, 2017).

297. *Id.* at 3.

298. *Id.* (first alteration in original) (quoting Naquanna Comeaux, *Target Marketing to Reach Clients ... in a Planned Parenthood Waiting Room*, PREGNANCY HELP NEWS (July 22, 2015), https://pregnancyhelpnews.com/target-marketing-to-reach-clients-in-a-planned-parenthood-waiting-room [https://perma.cc/83EC-JXZ7]).

299. *Id.* at 3-4 (quoting Comeaux, *supra* note 298).

300. *Id.* at 4.

301. *Id.* at 4-5. In a series of consent decrees, the FTC has made clear that it considers geolocation information as sensitive information requiring explicit, opt-in consent before collecting it. *See* Press Release, Fed. Trade Comm'n, FTC Approves Final Order Settling Charges Against Flashlight App Creator (Apr. 9, 2014), https://www.ftc.gov/news-events/press-releases/2014/04/ftc-approves-final-order-settling-charges-against-flashlight-app [http://perma.cc/NA4X-5VRN]. For a discussion of the norms around collection of geolocation data, see Danielle Keats Citron, *BEWARE: The Dangers of Location Data*, FORBES (Dec. 24, 2014, 3:04 PM), https://www.forbes.com/sites/daniellecitron/2014/12/24/beware-the-dangers-of-location-data/#6037ba1543cb [https://perma.cc/5JGB-WHHG]. The U.S. Supreme Court has held that obtaining cell-site location data from third parties constitutes a search under the Fourth Amendment. Carpenter v. United States, 138 S. Ct. 2206, 2217-18 (2018) (finding that location data "hold[s] for many Americans the 'privacies of life'" and that a government with access to historic location data "achieves near perfect surveillance" (quoting Riley v. California, 573 U.S. 373, 403 (2014))); *see also* United States v. Jones, 565 U.S. 400, 404 (2011). I have been advising federal lawmakers on efforts to provide stronger regulatory

Massachusetts AG argued that the firm's practice violated state law "because it intrude[d] upon a consumer's private health or medical affairs or status [or it] result[ed] in the gathering or dissemination of private health or medical facts about the consumer without his or her knowledge or consent."[302]

The advertising company and the AG's office entered into a settlement agreement under which the company vowed not to use geofencing technology near medical centers or physician offices to infer people's "health status, medical condition, or medical treatment."[303] Although the agreement is enforceable only against this specific advertising company (one of the limits of governance by settlement agreements), it established a norm against the collection of geolocation data to infer consumers' reproductive health data under Massachusetts law.[304]

In another effort to curtail the collection of intimate data, the FTC brought a regulatory action against mobile spyware company Retina-X under its UDAP authority in section 5 of the Federal Trade Commission Act.[305] The complaint alleged that the defendant's spyware injured consumers by enabling stalkers to monitor people's physical movements, sensitive information, and online activities without consent.[306] The unwanted collection of cellphone activity risked exposing victims to emotional distress, financial losses, and physical harm, including death.[307] The FTC charged that

---

protections for location data. This effort is not new. In 2014, then-Senator Al Franken proposed the federal Location Privacy Protection Act, but the bill failed to pick up traction. *See* Citron, *Spying Inc.*, *supra* note 7, at 1274.

302. *See* Assurance of Discontinuance, *supra* note 296, at 4-5.

303. *Id.* at 7.

304. *See* Citron, *Privacy Policymaking*, *supra* note 273, at 785; Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 620-25 (2014).

305. *See* Complaint, *In re* Retina-X Studios, LLC, No. C-4711 (F.T.C. Oct. 22, 2019). Section 5 of the Federal Trade Commission Act prohibits unfair and deceptive acts and practices. Federal Trade Commission Act § 5, 15 U.S.C. § 45. It has served as the template for state UDAP laws, which are often referred to as mini-FTC Acts. *See* CAROLYN L. CARTER, NAT'L CONSUMER L. CTR., CONSUMER PROTECTION IN THE STATES: A 50-STATE REPORT ON UNFAIR AND DECEPTIVE ACTS AND PRACTICES STATUTES 5-6 (2009), https://www.nclc.org/images/pdf/udap/report_50_states.pdf [https://perma.cc/89MT-WQGZ]; Lydia F de la Torre, *FTC Privacy and Cyber-Security Authority Under the FTC Act*, MEDIUM (Jun. 15, 2019), https://medium.com/golden-data/the-ftc-act-4b7bde468e5f [https://perma.cc/HW3G-SYM9].

306. *See* Complaint, *supra* note 305, at 3.

307. *Id.*

the mobile spyware constituted an unfair practice because consumers could not reasonably avoid the secret spying and the harm was not outweighed by the countervailing benefits.[308] In 2020, the FTC entered into a consent decree with Retina-X. The defendant agreed to obtain express written agreement from purchasers that they would use the product only for legitimate and lawful purposes.[309] Regrettably, the defendant was not required to refrain from selling monitoring products in the future,[310] a result that shows another limit of governance by consent decree.

State and federal enforcement efforts have set important precedent regarding sites amassing people's nude images as part of extortion schemes. In her capacity as California's Attorney General, Kamala Harris "prosecuted operators of sites that encouraged users to post nude photos and [then] charged for their removal."[311] In one case, site operator Kevin Bollaert faced charges of extortion, conspiracy, and identity theft after urging users to post ex-lovers' nude photos and offering to remove those images for hundreds of dollars.[312] Bollaert was convicted of twenty-seven felony counts and sentenced to eight years of imprisonment and ten years of mandatory supervision.[313]

The FTC sued another revenge porn operator under section 5 of the FTC Act for exploiting nude images shared in confidence for commercial gain.[314] The operator agreed to shutter the site and delete the images.[315] The FTC joined forces with the Nevada

---

308. *Id.* at 7.

309. Press Release, Fed. Trade Comm'n, FTC Gives Final Approval to Settlement with Stalking Apps Developer (Mar. 27, 2020), https://www.ftc.gov/news-events/press-releases/2020/03/ftc-gives-final-approval-settlement-stalking-apps-developer [https://perma.cc/URN6-A5AA].

310. *See* Complaint, *supra* note 305, at 8.

311. Citron, *Privacy Policymaking*, *supra* note 273, at 775.

312. Dana Littlefield, *'Revenge Porn' Website Operator Convicted*, SAN DIEGO UNION-TRIB. (Feb. 2, 2015, 6:07 PM), https://www.sandiegouniontribune.com/sdut-revenge-porn-site-operator-guilty-felony-charges-2015feb02-htmlstory.html [https://perma.cc/3Q2G-232Y].

313. Lyndsay Winkley & Dana Littlefield, *Sentence Revised for Revenge Porn Site Operator*, SAN DIEGO UNION-TRIB. (Sept. 21, 2015, 5:09 PM), https://www.sandiegouniontribune.com/sdut-kevin-bollaert-revenge-porn-case-resentencing-2015sep21-story.html [https://perma.cc/WA2P-YQAT].

314. *See* Complaint at 1-2, *In re* Craig Brittain, No. C-4564 (F.T.C. Jan. 29, 2015).

315. Press Release, Fed. Trade Comm'n, Website Operator Banned from the 'Revenge Porn' Business After FTC Charges He Unfairly Posted Nude Photos (Jan. 29, 2015), https://www.ftc.gov/news-events/press-releases/2015/01/website-operator-banned-revenge-porn-business-after-

Attorney General in an investigation of yet another revenge porn site that solicited nude images and charged victims from $499 to $2,800 for their removal.[316] A federal court ordered the site to destroy all intimate images and personal information in its possession and to pay more than $2 million in penalties.[317]

Norms around data security have similarly emerged based on federal and state enforcement activity. The FTC follows "a process-based approach to data security, which entails assessing steps taken by entities to achieve 'reasonable security.'"[318] State attorneys general, adhering to this approach, often serve as "first responders" to data breaches, at times in coordination with the FTC.[319]

The FTC and state attorneys general have brought investigations in the wake of data breaches involving intimate information. For instance, the FTC and the Vermont Attorney General's office sued the owners of Ashley Madison for failing to adequately secure customers' personal data.[320] The Vermont Attorney General's complaint in state court highlighted the site's failure "to maintain documented information security policies" and to use "multi-factor authentication."[321] The complaint alleged that the site's inadequate security

---

ftc-charges [https://perma.cc/ZU2Y-FM7V]; *see also* Citron & Hartzog, *supra* note 183. The Cyber Civil Rights Initiative joined together with Without My Consent to file a comment to the consent decree in that case. *See* Comments of the Cyber Civil Rights Initiative, Inc. & Without My Consent, Inc., No. 132-3120, at 1 (F.T.C. Feb. 23, 2015).

316. Complaint for Permanent Injunction & Other Equitable Relief, *supra* note 253, at 12; Press Release, Fed. Trade Comm'n, Nevada Obtain Order Permanently Shutting Down Revenge Porn Site MyEx (June 22, 2018), https://www.ftc.gov/news-events/press-releases/2018/06/ftc-nevada-obtain-order-permanently-shutting-down-revenge-porn [https://perma.cc/CH4U-R8YL]. The Nevada Attorney General argued that the site violated state UDAP law by intimidating people into paying for the removal of their photos. *See* Complaint for Permanent Injunction & Other Equitable Relief, *supra* note 253, at 20.

317. FTC v. EMP Media, Inc., No. 2:18-cv-00035-APG-NJK, 2018 WL 3025942, at *2-3 (D. Nev. June 15, 2018), *motion to set aside judgment denied*, 334 F.R.D. 611 (D. Nev. Apr. 9, 2020).

318. Citron, *Privacy Policymaking*, *supra* note 273, at 781 (quoting Thomas J. Smedinghoff, An Overview of Data Security Legal Requirements for All Business Sectors (Oct. 8, 2015) (unpublished manuscript), https://papers.ssrn.com/so13/papers.cfm?abstract_id=2671323).

319. *Id.* at 780.

320. *E.g.*, Press Release, Fed. Trade Comm'n, Operators of AshleyMadison.com Settle FTC, State Charges Resulting from 2015 Data Breach that Exposed 36 Million Users' Profile Information (Dec. 14, 2016), https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting [https://perma.cc/9G9A-H9GV].

321. Consumer Protection Complaint at 4, Vermont v. Ruby Corp., No. 730-12-16 (Vt. Super. Ct. Dec. 14, 2016).

amounted to an unfair business practice that risked "significant harm to ... consumer[s'] reputation[s], relationships, and personal li[ves]" and raised people's risk of identity theft.[322] The case resulted in a consent decree with the FTC and settlements with state attorneys general.[323]

The New York Attorney General's office similarly investigated Jack'd, a gay, bisexual, and transgender dating app, for failing to protect the nude images of approximately 1,900 individuals.[324] The dating app allegedly deceived customers by breaking its promise to ensure the confidentiality of photos marked "private."[325] Although the site had been warned about the security vulnerability more than a year earlier, it had failed to take remedial action.[326]

*3. Private Suits*

Civil suits have gained traction for deceptive collections of intimate information related to networked sex toys. Subscribers sued vibrator manufacturer Lovense for collecting intimate information despite its promise that "[a]bsolutely no sensitive data (pictures, video, chat logs) pass through (or are held) on our servers."[327] The complaint alleged that the defendant intruded on the plaintiffs' privacy by recording their communications and activities without consent in violation of the federal and state wiretap laws and state privacy tort law.[328] Subscribers brought similar claims against

322. *Id.*

323. *See* Press Release, *supra* note 320.

324. Press Release, N.Y. State Off. Att'y Gen., Attorney General James Announces Settlement with Dating App for Failure to Secure Private and Nude Photos (June 28, 2019), https://ag.ny.gov/press-release/2019/attorney-general-james-announces-settlement-dating-app-failure-secure-private-and [https://perma.cc/7YZL-ZPEJ].

325. *Id.*

326. *Id.*

327. *See* First Amended Class Action Complaint & Demand for Jury Trial at 9, S.D. v. Hytto Ltd., No. 18-cv-00688-JSW (N.D. Cal. Aug 23, 2018).

328. *Id.* at 14-15. The case presumably proceeded to discovery after the court rejected the defendant's motion to dismiss. S.D. v. Hytto Ltd., No. 18-cv-00688-JSW, 2019 WL 8333519, at *1 (N.D. Cal. May 15, 2019).

We-Vibe for recording information about their use of the defendant's vibrators.[329] The case settled for $3.75 million.[330]

By contrast, individuals have been unable to hold platforms accountable for hosting their nude images without consent.[331] Section 230 of the federal Communications Decency Act (CDA) has barred their efforts.[332] The irony is significant—the CDA was principally concerned with censoring porn (and was mostly struck down), yet the only part of the law left standing now enables the distribution of the very worst kinds of obscenity. Under section 230, providers or users of interactive computer services are shielded from liability for under- or over-filtering user-generated content.[333] Section 230(c)(1) says that providers or users of interactive computer services will not "be treated as ... publisher[s] or speaker[s] of any information provided by another information content provider."[334]

Lower federal and state courts have dismissed victims' civil claims even though site operators solicited, chose to republish, or failed to remove nonconsensual pornography.[335] Section 230 did not bar the state attorney general and FTC suits discussed above

---

329. *See* Amended Class Action Complaint & Demand for Jury Trial, *supra* note 118, at 11-14.

330. Kimiko de Freytas-Tamura, *Maker of 'Smart' Vibrators Settles Data Collection Lawsuit for $3.75 Million*, N.Y. TIMES (Mar. 14, 2017), https://www.nytimes.com/2017/03/14/technology/we-vibe-vibrator-lawsuit-spying.html [https://perma.cc/83GY-QRSH]. This recalls the success plaintiffs have had in obtaining redress after being secretly recorded in their bedrooms. Citron, *Sexual Privacy*, *supra* note 7, at 1934 n.425 (collecting cases).

331. Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 FORDHAM L. REV. 401, 413-14 (2017); Danielle Keats Citron, *Cyber Mobs, Disinformation, and Death Videos: The Internet as It Is (and as It Should Be)*, 118 MICH. L. REV. 1073, 1088-89 (2020) [hereinafter Citron, *Cyber Mobs*].

332. Citron & Wittes, *supra* note 331, at 413-14; *Fostering a Healthier Internet to Protect Consumers: Hearing Before the H. Comm. on Energy & Com.*, 116th Cong. (2019) (statement of Danielle Keats Citron, Professor of Law, Boston University School of Law). For an enlightening history of section 230's adoption and judicial interpretation, see JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET (2019).

333. 47 U.S.C. § 230(c); *see also* Citron & Wittes, *supra* note 331, at 416.

334. § 230(c)(1). Section 230(c)(2) extends the legal shield to "good faith" removal or blocking of offensive, harassing, or otherwise offensive user-generated content. *Id.* § 230(c)(2).

335. MARY ANNE FRANKS, THE CULT OF THE CONSTITUTION (2019); CITRON, HATE CRIMES IN CYBERSPACE, *supra* note 23, at 173-75; Danielle Keats Citron & Mary Anne Franks, *The Internet as a Speech Machine and Other Myths Confounding Section 230 Speech Reform*, 2020 U. CHI. LEGAL F. 45, 46; Citron & Wittes, *supra* note 331, at 407; Mary Anne Franks, *Sexual Harassment 2.0*, 71 MD. L. REV. 655, 695 & n.197 (2012).

because they concerned site operators' own extortion schemes, not their publication of user-generated content.[336]

Individuals have sued companies for failing to properly secure personal information. Companies have faced lawsuits in the wake of data breaches, but those suits are often dismissed early on in the litigation due to the plaintiffs' lack of standing or cognizable harm under state law.[337] Those lawsuits have a greater likelihood of surviving motions to dismiss if plaintiffs have suffered financial harm, such as identity theft, as opposed to the increased risk of such harm.[338]

One might think antidiscrimination law would serve as a crucial tool to preventing the use of discriminatory hiring algorithms in employment decisions. The major barrier to private civil rights claims (or even federal and state enforcement actions) is the opacity of vendors' proprietary systems. Firms may be mining intimate information and ranking, rating, and scoring them in ways that have a disparate impact on individuals from protected groups, but any such impact is impossible to detect absent whistleblowers. If corporate decisions relying on intimate information remain a black box, there can be no basis for lawsuits challenging them.[339]

*4. Criminal Law*

Only a narrow set of commercial practices—spyware and cyber stalking apps—implicate the criminal law. As I have explored in prior work, Title III of the Wiretap Act includes a provision covering those involved in the manufacture, sale, and advertisement of covert surveillance devices.[340] Congress passed that provision, 18 U.S.C.

336. *See supra* notes 318-26 and accompanying text; *see also* CITRON, HATE CRIMES IN CYBERSPACE, *supra* note 23, at 175-76.

337. Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 739-43 (2018).

338. *Id.* at 742.

339. *See* WEST ET AL., *supra* note 34, at 3-4 (explaining that AI tools claim to detect sexuality from headshots and such systems replicate gender and racial bias in ways that deepen and justify historical inequality but are often impossible to review and challenge when deployed in the commercial sector); ALEX CAMPOLO, MADELYN SANFILIPPO, MEREDITH WHITTAKER & KATE CRAWFORD, AI NOW INST., AI NOW 2017 REPORT 16 (2017), https://ainowinstitute.org/AI_Now_2017_Report.pdf [https://perma.cc/CFW4-4WDD].

340. Citron, *Spying Inc.*, *supra* note 7, at 1263-64.

§ 2512, to eliminate "a significant source of equipment" that is "highly useful" for private nonconsensual surveillance.[341]

Section 2512 makes it a crime for someone to intentionally manufacture, sell, or advertise a device if they know or have reason to know that its design "renders it primarily useful for the ... surreptitious interception of wire, oral, or electronic communications."[342] Defendants face fines, up to five years imprisonment, or both.[343] Section 2512 covers "a relatively narrow category of devices whose principal use is likely to be for wiretapping or eavesdropping."[344] At least "[t]wenty-five states and the District of Columbia have adopted similar statutes."[345]

Nonetheless, prosecutions remain rare. Despite the prevalence of spyware and the hundreds of purveyors of cyber stalking apps, federal prosecutors have only brought a handful of cases. As I have noted elsewhere,

> In September 2014, federal prosecutors brought § 2512 charges against StealthGenie's CEO Hammad Akbar. StealthGenie's spyware app secretly intercepted communications to and from mobile phones.... The federal indictment alleged that the app's target population was "spousal cheat: Husband/Wife or boyfriend/girlfriend suspecting their other half of cheating or any other suspicious behavior or if they just want to monitor them." A federal judge issued a temporary restraining order authorizing the FBI to disable the site hosting StealthGenie.[346]

The defendant pleaded guilty to the charges and was ordered to pay $500,000 in fines.[347] There have been no subsequent reported federal criminal cases against spyware purveyors since the StealthGenie

341. *See* S. REP. NO. 90-1097, at 95 (1968).
342. 18 U.S.C. § 2512(1)(b).
343. *Id.*
344. United States v. Shriver, 989 F.2d 898, 905 (7th Cir. 1992).
345. Citron, *Spying Inc.*, *supra* note 7, at 1265 & n.132 (collecting statutes).
346. *Id.* at 1266-67 (footnotes omitted).
347. Press Release, U.S. Dep't of Just., Man Pleads Guilty for Selling "StealthGenie" Spyware App and Ordered to Pay $500,000 Fine (Nov. 25, 2014), https://www.justice.gov/opa/pr/man-pleads-guilty-selling-stealthgenie-spyware-app-and-ordered-pay-500000-fine [https://perma.cc/NVS4-J7VD].

case. At the state level, prosecutions "ha[ve] been virtually nonexistent."[348]

While criminal law provides a foothold for the prosecution of the manufacturers, it has been hampered by the requirement that the device be primarily designed for the secret interception of electronic communications.[349] As privacy advocate James Dempsey has argued, the small number of section 2512 prosecutions is attributable, at least in part, to "the fact that it is hard to demonstrate that equipment is 'primarily' designed for stealth interception of communications."[350]

Individual sexual-privacy invaders are a different matter, as my prior scholarship has explored.[351] Consider nonconsensual pornography. Today, forty-six states, the District of Columbia, and Guam criminalize the posting of nude photos without consent.[352] Law enforcement has been slowly but surely pursuing cases under those laws.[353]

## III. REIMAGINING PROTECTIONS FOR INTIMATE INFORMATION

This Part sketches some guiding principles for the protection of intimate information in the commercial sector. My goal is three-fold: to stem the tidal wave of data collection; to restrict certain uses of intimate data; and to expand the suite of remedies available to courts.

---

348. Citron, *Spying Inc.*, *supra* note 7, at 1267.

349. *Id.* at 1267-68 (citing James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65, 111 (1997)).

350. *Id.*

351. Citron, *Sexual Privacy*, *supra* note 7, at 1931-33; Citron & Franks, *supra* note 47, at 387.

352. *See 46 States + DC + One Territory Now Have Revenge Porn Laws*, CYBER C.R. INITIATIVE (2020), https://www.cybercivilrights.org/revenge-porn-laws/ [https://perma.cc/A69J-B3WX]. In 2014, before Dr. Mary Anne Franks and the Cyber Civil Rights Initiative began working with lawmakers, three states criminalized the practice. Mary Anne Franks, *"Revenge Porn" Reform: A View from the Front Lines*, 69 FLA. L. REV. 1251, 1255 (2017); *see also* Citron & Franks, *supra* note 47, at 371-74 (discussing the development of so-called revenge porn laws).

353. *See* Citron, *Privacy Policymaking*, *supra* note 273, at 757-58.

### *A. Special Protections for Intimate Information*

Before turning to the special protections owed to intimate information, I want to emphasize the need for strong baseline protections for *all* personal data collected in the private sector.[354] The reasons why we need sexual privacy support the adoption of comprehensive data protections. Technological advances may soon enable firms to turn innocuous personal data into intimate data with a high degree of accuracy.[355] Paul Ohm and Scott Peppet have memorably termed this prospect "everything reveals everything."[356] Soon, if companies have enough information about us, no matter how innocuous, they will be able to infer the most intimate information about us. The "everything reveals everything" phenomenon is why we need to stem the tide of over-collection and to restrict downstream use, sharing, and storage of *all* personal data. Indeed, someday soon, copious amounts of personal data will likely be turned into intimate information. Thus, we need strong privacy protections for even the most seemingly benign personal data, lest it become a shell game whose end goal is the revelation of intimate information.

Whether or not lawmakers pass comprehensive privacy reforms, intimate information warrants special protection. If we can get lawmakers to act on this issue—the protection of intimate information—then we should do so. This Section focuses on areas worthy of reform. Certain data collection should be off-limits. Certain uses of intimate data should be sharply restricted. Injunctive relief should be available in court, including the possibility of a "data death penalty" for the very worst sexual-privacy violators.[357]

---

354. Personally identifiable information is a central concept in privacy law. Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1816 (2011). Federal and state laws address what constitutes personal information in different ways. *Id.* An organizing principle is whether an individual is identified or can be reasonably identified. *Id.* at 1817.

355. Paul Ohm & Scott Peppet, *What if Everything Reveals Everything?*, *in* BIG DATA IS NOT A MONOLITH 45, 55 (Cassidy R. Sugimoto, Hamid R. Ekbia & Michael Mattioli eds., 2016).

356. *Id.* at 45. That possibility certainly supports the call for strong baseline rules for the handling of personal information.

357. *See infra* Part III.A.3.

*1. Limits on Collection*

The default assumptions around the handling of intimate information must change. The norm of collection is not inevitable—unless law and society make it so. The status quo jeopardizes crucial aspects of human flourishing and well-being enabled by sexual privacy.

The collection of intimate information can produce more upside than downside in certain contexts. Law should work to ensure that collection occurs in those contexts and no others. Although no legal approach can guarantee this outcome, the following reforms are offered with that goal in mind.

Certain collection practices should be off-limits. Law should prohibit services whose *raison d'être* is the nonconsensual collection of intimate data.[358] Period. The end. No exceptions. Software that "undresses" women in photographs runs afoul of this mandate. So do apps that facilitate the secret and undetectable monitoring of someone's cellphone, as do sites hosting nonconsensual pornography and deep fake sex videos. To ensure that this reform would apply to revenge porn sites and their ilk, Congress should amend the federal law shielding online services from liability for user-generated content.[359]

We have recognized no-collection zones in other contexts. American law has long banned the collection of information crucial to the exercise of civil liberties. Under the Privacy Act of 1974, for instance, federal agencies cannot collect information that exclusively concerns individuals' First Amendment activities.[360] In *NAACP v. Alabama*, the Supreme Court struck down a court order requiring the civil rights group to produce its membership list on the ground that privacy in group associations is indispensable to

358. Such a rule would reinforce, not defeat, sexual expression including the legal practice of pornography—the recording and sharing of nude imagery *with the subject's explicit consent*.

359. Section 230 of the Communications Decency Act secures a shield from liability for sites that under- or over-filter content provided by another information content provider. 47 U.S.C. § 230(c). My prior work has explored suggestions for amending section 230, so I will not belabor the point here. *See* CITRON, HATE CRIMES IN CYBERSPACE, *supra* note 23, at 177-79; Citron, *Cyber Mobs*, *supra* note 331, at 1088-91; Citron, *Cyber Civil Rights*, *supra* note 40, at 117, 121-25; Citron & Franks, *supra* note 335; Citron & Wittes, *supra* note 331.

360. Privacy Act of 1974 § 3, 5 U.S.C. § 552a(e)(7).

preserving the freedom to associate.[361] Apps and services designed to facilitate the collection of intimate information without individuals' permission are an equal affront to civil rights and civil liberties, and they should be prohibited.

What about firms that fall outside the no-collection zone? Those firms should be required to obtain meaningful consent from individuals before collecting their intimate information. As a baseline rule, firms should only be allowed to request consent to collect intimate data if such collection is strictly necessary for a legitimate business purpose or medical research.[362]

Now for some thoughts on the manner of the request. The "gold standard of consent" has several features. To ensure meaningful consent, requests for consent should be infrequent. Firms should not be permitted to pepper people with requests.[363] Repeated requests overwhelm people and exert pressure on them to say yes. They often succeed not because people have thought about the request and actually agree but because they simply want firms to stop asking.[364] Firms should spell out the request clearly and explain the risks in concrete and vivid terms so that individuals understand what happens if intimate data is leaked or improperly used or shared.[365]

The gold standard for consent combines the "knowing and voluntary" waiver standard from constitutional law and the informed consent standard from biomedical ethics.[366] To satisfy the knowing requirement, requests for consent must be clear and understandable. They should explain what intimate data would be collected, how it would be used, and how long it would be retained. When possible, requests for consent should be made separately from the process of signing up for a service. Moreover, such requests should be designed in a way that enhances the likelihood that people will understand them.[367] Lessons from design psychology can

---

361. 357 U.S. 449, 466 (1958).

362. This sort of approach should be followed for all personal data.

363. Richards & Hartzog, *Pathologies of Digital Consent*, *supra* note 46, at 1494.

364. *Id.* at 1493-94.

365. *Id.* at 1492. Richards and Hartzog also argue that for consent to be meaningful, it must occur in contexts in which people have the incentive to take the request seriously. For platforms collecting sensitive information, Richards and Hartzog argue that people may be more inclined to consider the risks if requests do not arrive in dribs and drabs. *Id.* at 1498.

366. *Id.* at 1465, 1475.

367. Ryan Calo has done important work in this area. *See, e.g.*, M. Ryan Calo, *Against*

be leveraged to make it more likely that people consider the question rather than simply clicking "I Agree."[368] As for voluntariness, requests for consent should not be "take it or leave it" propositions *if* a firm can provide its service without collecting intimate data. It should be as easy to reject requests as it is to accept them. Firms should not make it difficult for people to deny requests. They should also not be allowed to engage in other activity designed to "coerce, wheedle, and manipulate people to grant [consent]."[369]

Consider the issue of consent in the context of a first-party data-collector adult site. People should be given an easy way to decline a porn site's request to collect data so that they can easily continue browsing and searching the site. Most porn sites do not need to collect that data (the content that individuals have browsed and searched) to operate. Thus, the adult site would need to present individuals with a real choice. It would have to provide a good reason for people to give up their privacy—money, additional services, and the like—and it could only ask for permission if it had a legitimate business reason, such as advertising, for collecting the data and explained that reason. So long as requests are clear about the contours of the trade, visceral about the risks, and made infrequently, then individuals would have a chance to consider the requests and make knowing and voluntary decisions.

Some apps and services require the collection of certain intimate data to function—that is certainly true of many dating apps, to take an example.[370] There, requests for collection could permissibly be presented as "take it or leave it." Requests for consent would have to make clear that the service depends upon the collection of intimate data and that the firm would collect the data only to provide the service and for no other reason. In that case, firms could decline to provide their services to people who reject their request without running afoul of the voluntariness requirement.

---

*Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027 (2012). Calo explores various mechanisms for delivering notice that rely on consumer experience rather than entirely on words or symbols. *Id.* at 1039-47.

368. *See* Eur. Data Prot. Bd., *Guidelines 05/2020 on Consent Under Regulation 2016/679*, at 21 (May 4, 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf [http://perma.cc/2PNB-C4FY].

369. Richards & Hartzog, *Pathologies of Digital Consent*, *supra* note 46, at 1489.

370. *See, e.g.*, *supra* Part I.A.1.

Not so for third-party data collectors. Third-party data collectors must make clear that individuals can decline their requests without consequence. They would have to spell out their legitimate business interest in the intimate data. They would have to provide an incentive for people to grant their request. Furthermore, they would have to ensure that consent is meaningful in all other respects.

This approach is autonomy-respecting: it lets people decide for themselves if their intimate data is collected for a legitimate business purpose, such as advertising or research. It is intimacy-enhancing: people will be more inclined to use apps and services to communicate with partners if they are not worried about the unwanted collection of intimate data. This approach erects roadblocks that are currently absent in the now-unbridled world of corporate intimate surveillance.

With less collection comes less risk. Less collection would curtail downstream damage. It would also reduce the incidence of data breaches leaking intimate data to blackmailers, extorters, and reputation destroyers. There would be fewer misuses of intimate data in ways that deprive women, sexual minorities, and nonwhite people of crucial life opportunities.

This recommendation would alter the ground rules for the marketplace of intimate information. At present, third-party advertisers and data brokers do not have to ask people for permission to track their intimate data.[371] They do not have to pay people for it. Advertisers and data brokers would have to internalize some of the costs of the data-collection imperative. They would have to seek meaningful consent to collect intimate data and offer a legitimate business reason for doing so. They would have to offer individuals something for their intimate information.

The gains for sexual privacy are worth the potential loss in data brokerage and advertising profits. The advertising and data brokerage industries would not end. Instead, all that would end would be the default presumption that intimate information can be collected

371. Narseo Vallina-Rodriguez & Srikanth Sundaresan, *7 in 10 Smartphone Apps Share Your Data with Third-Party Services*, SCI. AM. (May 30, 2017), https://www.scientificamerican.com/article/7-in-10-smartphone-apps-share-your-data-with-third-party-services/ [https://perma.cc/BT29-W82G] ("[O]nce an app has permission to collect [your personal] information, it can share your data with anyone the app's developer wants to—letting third-party companies track where you are, how fast you're moving and what you're doing.").

unbeknownst to individuals and without their permission. The sky would not fall.

My experience working with companies and lawmakers on the nonconsensual hosting of nude images informs this approach. Cyber Civil Rights Initiative President and my frequent collaborator Mary Anne Franks has long argued that nude images should not be posted online without written consent.[372] After the first California Cyber Exploitation Task Force in-person meeting in the spring of 2015, Franks suggested as much to a tech company safety official. Her suggestion, wise then and wise now, was met with shock and dismay. The safety official—a thoughtful person with extensive content moderation experience—explained that social media companies could not possibly require prior written consent from the subject of a photo before the subject's nude images were posted online. "Why not?" we asked. The official responded that if written consent was required, then it might be more likely that nude photos would not be posted because the subjects of those photos would not give their consent.

Then, as now, we wondered what the problem was.[373] As we noted then, written consent would not prevent the posting of nude photos, just nude photos in which the subject did not consent (or at least in which the poster was not willing to sign something saying that the subject consented to the posting). This sentiment applies not only to sites trafficking in nonconsensual pornography and deep fake sex videos but also to data brokers and advertisers. If firms want to collect intimate information, then they should obtain people's knowing and voluntary consent to do so.

Privacy laws covering certain sensitive information often include affirmative consent requirements though they fall short of the "gold standard." The Illinois Biometric Identification Privacy Act conditions the collection of biometric data on consent given after a firm informs consumers of the fact that biometric information is being collected and stored; the reason for the collection, use, and storage; and the duration of the storage.[374] HIPAA's Privacy Rule permits data use necessary for the treatment, payment, or health care

372. *See, e.g.*, Franks, *supra* note 352, at 1283.

373. Of course, we knew the problem was that online platforms optimize for likes, clicks, and shares so that they can earn advertising income.

374. 740 ILL. COMP. STAT. 14/15(b) (2020).

system operations data and requires consent for any uses beyond those purposes.[375] Under federal law, cable providers generally may not disclose subscribers' information to anyone without subscribers' consent.[376]

An alternative approach would be to limit the collection of intimate information to instances in which entities have a legitimate, reasonable basis for collecting intimate data and in which individuals would reasonably expect the collection.[377] The advertising industry would surely prefer this approach. Advertisers have a legitimate business reason for collecting personal data, and their practices might comport with people's reasonable expectations depending on the context. The outcome would be different for data brokers. People do not reasonably expect unknown shadowy actors to amass their intimate information in digital dossiers. In my view, this approach is far less compelling than requiring meaningful consent. Left as it is, the data collection imperative for intimate data would continue with too little friction restraining it.

Finally, it is worth noting the synergy between limits on collection and limits on the retention of intimate information. Restrictions on collection should be paired with an obligation to delete or otherwise destroy intimate information as soon as it is no longer needed to fulfill the purpose prompting its collection. This obligation would minimize the potential for leaks or the sale of intimate data.[378] The

---

375. 45 C.F.R. § 164.502(a)(1) (2019).

376. 47 U.S.C. § 551(c). The European Union's General Data Protection Regulation requires opt-in consent for the placement of tracking cookies. *See* GDPR, *supra* note 103, at 38. For sensitive information including information about individuals' sexuality, companies can only collect such information with explicit, affirmative consent. *Id.*

377. For thoughtful proposals on the issue, see Kerry, *Proposed Language*, *supra* note 46 ("Collection and processing [defined terms] of personal data shall have a reasonable, articulated basis that takes into account reasonable business needs of the [covered entity/controller/etc.] engaged in the collection balanced with the intrusion on the privacy and the interests of persons whom the data relates to."). Kerry notes, and I agree, that his proposal would "take provisions or rulemaking that exclude certain sensitive data fields or targeting to establish boundaries for behavioral advertising." *Id.* He notes further that "even if behavioral advertising in general is considered a reasonable business purpose, this collection language could be construed as barring Target's processing of purchasing data to deliver ads for maternity products to a secretly pregnant teenager as an excessive intrusion on her privacy and interests." *Id.*

378. *See* Seda Gürses, Carmela Troncoso & Claudia Diaz, Engineering Privacy by Design Reloaded 14-15 (2015) (unpublished manuscript), https://iapp.org/media/pdf/resource_center/Engineering-PbD-Reloaded.pdf [https://perma.cc/H4E8-989Q].

Fair Credit Reporting Act (FCRA) and the Video Privacy Protection Act (VPPA) similarly require the destruction of records from background checks or movie watching as soon as practicable.[379] Under the GDPR, the European Union's data protection law, personal data can be kept only for as long as is necessary to fulfill the original basis for its collection and processing.[380]

*2. Use Restrictions*

Policymakers should restrict the uses of intimate data to protect the opportunities secured by sexual privacy and reduce the risks to well-being. Companies collect massive quantities of personal information on the expectation that it will generate significant returns. As Paul Ohm observes: "Chasing profits, [companies] hoard this data for future, undefined uses; redistribute it to countless third parties; and repurpose it in ways their customers never imagined."[381]

Intimate data collected for a legitimate business purpose should not be repurposed for another reason without obtaining separate permission. This mirrors the approach of the Fair Information Practice Principles (FIPPs).[382] The FIPPs are the foundation for most privacy laws in the United States and around the world, as well as for most understandings of information ethics.[383] Under the FIPPs, information obtained for one purpose cannot be used or made available for other purposes without the person's consent.[384] That

379. 15 U.S.C. § 1681w (discussing disposal of records in consumer financial information context); 18 U.S.C. § 2710(e) (requiring destruction of old records in context of video rental or sale records).

380. GDPR, *supra* note 103, at 35 ("Personal data shall be ... adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').").

381. Ohm, *supra* note 44, at 1128.

382. *The Code of Fair Information Practices*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/consumer/code_fair_info.html [https://perma.cc/GS43-AAY3]. The FIPPs were first articulated by privacy scholar Alan Westin in 1967 and popularized by the U.S. Department of Health, Education, and Welfare in 1973. *See id.*; ALAN F. WESTIN, PRIVACY AND FREEDOM (1967).

383. *See, e.g.*, *Privacy Policy Guidance Memorandum*, DEP'T. HOMELAND SEC. (Dec. 30, 2008), https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf [https://perma.cc/9X9F-QQGV].

384. *See* Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 341, 350 (Jane K. Winn ed., 2006).

restriction is often referred to as a "secondary use limitation."[385] A better way to put it would be as a default ban on the nonconsensual secondary use of intimate data unless that ban had been lifted.[386]

Under this approach, firms could not use properly collected intimate data for other purposes without meaningful consent. In that context, obtaining separate, meaningful consent would be expensive. As the bioethics field shows,[387] having to track people down and ask them for separate permission to use intimate data for a distinct purpose would be costly. Those costs would ensure that firms only ask if they think that the costs of asking are worth it. Subscribers' intimate information, of course, could be used for the purpose for which it was collected and for which firms obtained meaningful consent. To return to the case of a dating app, this would include allowing subscribers to message each other and to post intimate information.

We also need clear rules against the exploitation of intimate information to manipulate people to act in ways consistent with another's ends rather than their own. As explored in Part II,[388] law enforcers have investigated uses of personal data to target the vulnerabilities of protected groups as unfair commercial practices.[389] Such cases, however, remain rare. A ban would make clear that such practices are unlawful and would thus reduce the need for enforcement actions directed at such exploitative practices.[390] More broadly, privacy law should require firms to act in the best interest of individuals whose intimate data they have collected consistent with a duty of loyalty and care.[391]

Strong use restrictions would protect sexual privacy and the human flourishing that it makes possible. Individuals would not

---

385. *Id.*; *The Code of Fair Information Practices*, *supra* note 382.

386. Thanks to Ryan Calo for suggesting this.

387. *See, e.g.*, Celia B. Fisher & Deborah M. Layman, *Genomics, Big Data, and Broad Consent: A New Ethics Frontier for Prevention Science*, 19 PREVENTION SCI. 871, 874 (2018).

388. *See supra* Part II.C.2.

389. HARTZOG, *supra* note 276, at 131 (explaining that UDAP laws are designed to prevent the exploitation of human vulnerabilities).

390. *See* Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. LEGAL ANALYSIS 43, 97-98 (2021).

391. Richards & Hartzog, *supra* note 13, at 5-6; Richards & Hartzog, *Pathologies of Digital Consent*, *supra* note 46, at 1500 (arguing that lawmakers should create rules designed to protect our trust—meaning "being *discreet* with our data, *honest* about the risk of data practices, *protective* of our personal information, and, above all, *loyal* to us, the data subjects").

have their autonomy undermined by a dating app's repurposing of their intimate data. They would not be chilled from using reproductive-health apps for fear that their struggles with painful periods or infertility would be used in assessments other than tracking their reproduction, such as employment or insurance matters. These restrictions would ban uses of intimate data that deny people crucial life opportunities without their say so. In that way, it would establish important protections such that crucial life opportunities are enjoyed by women, sexual minorities, and non-white people on equal terms.

### *3. Remedies: Halt Processing and the Data Death Penalty*

Injunctive relief against improper processing of intimate data should be part of the suite of remedies for the very worst offenders.[392] Privacy debates of late have focused on the wisdom of recognizing civil actions for damages or administrative fines.[393] Injunctive relief, however, has not been a key part of the discussion. It should be.

Privacy legislation should recognize judicial power to order injunctive relief in cases involving serial offenders. In such cases, injunctive relief should be mandatory to assure meaningful protection of sexual privacy and make clear its priority over competing interests.[394]

---

392. The topic of privacy remedies has not attracted sustained attention. Lauren Henry Scholz's important work is an important exception. *See, e.g.*, Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L.J. 653 (2019) (arguing for the recognition of restitution as a privacy remedy).

393. *See, e.g.*, Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 831 (2020) ("[A]ny new privacy law must include a private right of action.... Civil litigation made dangerous machines safer; private lawsuits gave us seatbelts, stronger automobile frames, safer doors, side impact protection, and many other car safety features. Little if any of that would have happened if car safety was the exclusive responsibility of a small, underfunded regulatory agency that has acceded to a self-governing privacy regime." (footnotes omitted)). Industry lobbyists strongly oppose privacy bills that include private rights of action. Issie Lapowsky, *Tech Lobbyists Push to Defang California's Landmark Privacy Law*, WIRED (Apr. 29, 2019, 3:09 PM), https://www.wired.com/story/california-privacy-law-tech-lobby-bills-weaken/ [https://perma.cc/Z77Q-8E2W]. Private rights of action are essential given the limited resources available to federal and state law enforcers.

394. Lawmakers must make clear that such injunctive relief is automatic. In the absence of clear legislative intent, courts are reluctant to order equitable remedies. *See, e.g.*, Winter v. Nat. Res. Def. Council, 555 U.S. 7, 24 (2008). There is an extensive scholarly debate about

As for substantive duties so for remedies: civil rights law provides a model for reform. Injunctive relief is a core feature of civil rights law.[395] Federal, state, and local antidiscrimination statutes permit injunctive relief,[396] and courts have employed equitable remedies in flexible and creative ways. In workplace sexual harassment cases, for example, courts have ordered employers to implement anti-harassment policies and procedures, provide training, retain personnel records, and install security cameras.[397]

Lawmakers should recognize a court's power to order parties to halt processing intimate information for repeat offenders. Figuring out if a firm qualifies as a repeat offender would entail three steps. Under the first step, the court would issue an order directing the party to fulfill its legal obligations. If the court is presented with clear evidence that the party has violated the first order, then the court would turn to the second step. Under the second step, the court would order the firm to stop processing intimate data until compliance has been achieved as shown by an independent third-party audit.[398] For the third and final step, if the court is shown clear evidence that the party has failed to comply for the third time,

---

whether courts should be required to issue injunctions to remedy statutory violations. Michael T. Morley, *Enforcing Equality: Statutory Injunctions, Equitable Balancing Under* eBay*, and the Civil Rights Act of 1964*, 2014 U. CHI. LEGAL F. 177, 194. In the environmental context, Daniel Farber argues that when statutes impose absolute duties on people, injunctive relief is essential to prevent future violations. Daniel A. Farber, *Equitable Discretion, Legal Duties, and Environmental Injunctions*, 45 U. PITT. L. REV. 513, 515 (1984).

395. OWEN M. FISS, THE CIVIL RIGHTS INJUNCTION 6 (1978) (explaining that injunctive relief was understood after *Brown v. Board of Education* as the most effective way to guarantee civil rights). For a thoughtful exploration of how courts exercise their equitable powers granted under Title VII, see Morley, *supra* note 394.

396. *See, e.g.*, Civil Rights Act of 1964, 204(a), 42 U.S.C. § 2000a-3(a); 43 PA. STAT. AND CONS. STAT. ANN. § 962(c)(3) (West 2020); *Availability of Injunctive Relief Under State Civil Rights Acts*, 24 U. CHI. L. REV. 174, 180 (1956). In some civil rights statutes, injunctions are the only available remedy. For instance, Title III of the Americans with Disabilities Act only allows injunctive relief as opposed to monetary damages. *E.g.*, Dudley v. Hannaford Bros. Co., 333 F.3d 299, 304 (1st Cir. 2003) (citing Americans with Disabilities Act, 42 U.S.C. § 12188(a)(1)).

397. *See, e.g.*, United States v. Greenwood Cmty. Sch. Corp., No. 1:03-cv-01055-DFH-TAB, at 2-3 (S.D. Ind. July 28, 2003); Carey v. O'Reilly Auto. Stores, No. 18-81588-CIV, 2019 WL 3412170, at *10-11 (S.D. Fla. May 31, 2019) (declining, at an early stage of the litigation, to dismiss plaintiff's requests for injunctive relief in the form of the installation of "monitored security cameras" and the termination of "certain employees"), *report and recommendation adopted*, 2019 WL 3408926 (S.D. Fla. June 17, 2019).

398. A schedule would be set to report the auditor's findings to the court.

then and only then would the court impose what can be called the "data death penalty"—an order permanently stopping the firm from processing intimate information.

Under a stop-processing order, providers of cyber stalking apps and sites devoted to nonconsensual pornography would have to halt their services.[399] Such orders would be crucial to securing an effective remedy to individuals whose sexual privacy had been repeatedly violated.

There is nothing novel about a halt-processing remedy. Under article 58 of the GDPR, data protection authorities have authority to impose temporary or permanent bans on the processing of personal data.[400] Halt processing orders must be "appropriate, necessary and proportionate" to ensure compliance with legal obligations.[401] In 2019, the Hamburg Commissioner for Data Protection and Freedom of Information started an administrative procedure to stop Google employees and contractors from listening to voice recordings of Google Home device subscribers for three months.[402] The Hamburg Commissioner explained that, "effective protection of those affected from eavesdropping, documenting and evaluating private conversations by third parties can only be achieved by prompt execution."[403] Google responded by pledging not to transcribe voice recordings collected from its personal assistant device.[404]

European Union data protection authorities had been issuing halt-processing orders even before the GDPR's adoption. For instance, Ireland's data protection authority ordered Loyaltybuild

399. In the case of revenge porn sites and their ilk, such relief would depend upon changes to section 230. *See supra* note 359 and accompanying text.

400. GDPR, *supra* note 103, at 24.

401. *Id.*

402. Press Release, Hamburg Comm'r for Data Prot. & Freedom Info., Speech Assistance Systems Put to the Test – Data Protection Authority Opens Administrative Proceedings Against Google (Aug. 1, 2019), https://datenschutz-hamburg.de/assets/pdf/2019-08-01_press-release-Google_Assistant.pdf [https://perma.cc/FC87-2GWL]. The GDPR permits data protection authorities to take measures to protect the rights of data subjects for a period not to exceed three months. *Id.*

403. *Id.* Recall that whistleblowers reported that Google Home was inadvertently recording private and intimate conversations and that contractors were transcribing those conversations in order to analyze whether the device was correctly processing information. *See* Haselton, *supra* note 135.

404. Press Release, *supra* note 402. Google seemingly has not altered its position.

to halt processing personal data for three months after learning that the firm's data breach involved the personal data of 1.5 million people.[405] The firm was directed to notify clients about the security breach, delete certain data, and achieve compliance with PCI-DSS standards for the processing of credit card data.[406] It took the company seven months to fulfill those obligations.[407]

To be sure, even temporary stop-processing orders exact significant costs. Loyaltybuild lost millions of euros in revenue, a considerable blow to the firm.[408] For some entities, halting processing for even a month might cause their collapse. New entrants will no doubt find it more challenging to absorb the costs of stop-processing orders than established entities.[409] But the grave risk to individuals and society posed by the handling of intimate information warrants strong remedies.

### *B. Objections*

The new compact will raise questions about the market and free speech. This Section addresses some concerns about the broader social welfare consequences of my reform proposals. It explains why the reform proposals enhance free speech values and would withstand First Amendment challenges.

---

405. *Cease Processing Orders Under GDPR: How the Irish DPA Views Enforcement*, IAPP (Sept. 11, 2018), https://iapp.org/news/a/cease-processing-orders-under-the-gdpr-how-the-irish-dpa-views-enforcement/ [https://perma.cc/YA73-K9SL].

406. *Id.*

407. *Id.*

408. *Id.*

409. At a faculty workshop at Boston University School of Law, David Webber and Michael Meuer asked me about potential perverse incentives of stop-processing orders. Might new entrants collect intimate information in violation of the law and then just shut down and restart in a game of endless whack-a-mole? That is surely possible depending on the start-up costs and availability of necessary financing. Criminals have certainly engaged in this sort of whack-a-mole activity in the face of shut-down orders as in the case of Anon-IB. *See* Uchill, *supra* note 186. Nonetheless, the reputational costs of this strategy would be significant. New entrants seeking third-party capitalization would be less inclined to engage in this sort of behavior.

*1. Market*

These proposals would surely change the value proposition for many online services. A significant number of apps and services explored above do not charge fees for their services because they earn advertising money.[410] In some markets, third parties may have invested in them as we have seen in the sexual wellness and dating markets.[411] As a result, people might have more limited choices.

If advertising fees and outside funding dropped significantly, firms would surely look to other revenue sources. They might charge subscription fees. They might keep basic services at low or no cost and increase the costs for premium or add-on services. A nontrivial number of people might not be able to afford these services.

Nonprofit organizations might support efforts to provide some services free of charge. The femtech market seems a likely possibility. Reproductive justice organizations might contribute funds for period-tracking apps providing helpful and truthful information. LGBTQ advocacy groups might hire technologists to create dating apps for community members.

Some gaps would remain, leaving some people unable to afford dating apps, period-tracking services, and subscriptions to adult sites. Failing to protect intimate data exacts too great a cost to sexual privacy even if it means that services tracking intimate life remain out of reach for some.

More broadly, we should not discount the role that privacy plays in enhancing market operations. As Ryan Calo has explored, a

---

410. *See* Hoofnagle & Whittington, *supra* note 10, at 633.

411. Dana Olsen, *The Top 13 VC Investors in Femtech Startups*, PITCHBOOK (Nov. 2, 2018), https://pitchbook.com/news/articles/the-top-13-vc-investors-in-femtech-startups [https://perma.cc/M8EY-LH7A] (explaining that a decade ago only $23 million worth of venture capital was invested in the global femtech industry whereas there has been nearly $400 million in venture capital funding in 2018); Kate Clark, *Dating Startup Raises VC as Facebook Enters the Relationship Biz*, PITCHBOOK (May 4, 2018), https://pitchbook.com/news/articles/dating-app-raises-vc-as-facebook-enters-the-relationship-biz [https://perma.cc/B8FW-SPT3] (explaining that app-based dating services have attracted venture funding including apps like Happn, Hinge, Clover, and The League). 2018 set records for investment in apps devoted to women's and men's health issues. Olsen, *supra* note 55. Two venture capital funds have emerged that are devoted exclusively to investing in the funding of women's health enterprises. *Id.* One of those firms, Astarte Ventures, has invested in Lola, a startup that "provides subscription-based delivery of organic tampons, Flo, ... a period-tracking app, and Future Family, a business that offers reproductive healthcare services." *Id.*

firm's commitment to privacy engenders trust.[412] Individuals may be more inclined to pay to use services because they believe that a firm's service is worth their price.[413]

*2. Free Speech*

The proposed reforms will garner objections on free speech grounds. For some scholars, all data privacy laws regulate "speech" and thus may be inconsistent with the First Amendment.[414] These arguments illustrate what Leslie Kendrick has criticized as "First Amendment expansionism"—the tendency to treat speech as normatively significant no matter the actual speech in question.[415] As Kendrick underscored, freedom of speech is a "term of art that does not refer to all speech activities, but rather designates some area of activity that society takes, for some reason, to have special importance."[416]

Just because activity can be characterized as speech does not mean that the First Amendment protects it from government regulation.[417] Neil Richards helpfully explains that free speech protections hinge on whether government regulations of commercial data flows are "particularly threatening to longstanding First Amendment values."[418] Indeed.

---

412. Ryan Calo, *Privacy and Markets: A Love Story*, 91 NOTRE DAME L. REV. 649, 650 (2015).

413. *Id.* at 661.

414. *E.g.*, Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1051 (2000) (arguing that government imposed fair information practice rules that restrict the ability of speakers to communicate truthful data about others is inconsistent with basic First Amendment principles); Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 63 (2014) ("[F]or all practical purposes, and in every context relevant to the current debates in information law, data is speech.").

415. Citron & Franks, *supra* note 335, at 60 (citing Leslie Kendrick, *First Amendment Expansionism*, 56 WM. & MARY L. REV. 1199, 1212 (2015)).

416. Kendrick, *supra* note 415, at 1212.

417. *Id.*

418. Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501, 1507 (2015). For a compelling exploration of those values and how the First Amendment should be understood to secure and enhance the diversity and vitality of public debate, see Genevieve Lakier, *The First Amendment's Real* Lochner *Problem*, 87 U. CHI. L. REV. 1241 (2020).

The assertion that all speech (or all data) has normative significance elides the different reasons why speech (or data) warrants protection from particular government regulations but not others.[419] Some government regulations censor speech central to self-governance or the search for truth while others raise no such concerns.[420] Some government regulations imperil speech crucial to self-expression while others pose no such threat.[421]

The proposed reforms would not threaten First Amendment values. The nonconsensual surveillance of intimate life is not necessary for the public to figure out how to govern itself. Requiring meaningful consent to handle data about people's HIV status, abortion, sex toy use, or painful cramps would have little impact on discourse about political, cultural, or other matters of societal concern. People's miscarriages, erectile dysfunction, abortions, and sexual fantasies have nothing to do with art, politics, or social issues. Nude photos posted without consent contribute nothing to discussions about issues of broad societal interest. Someone's abortion, miscarriage, and rape are not facts or ideas to be debated in the service of public debate.

Regulating the surveillance of intimate life with explicit consent requirements and narrow no-collection zones would not chill self-expression but rather secure the basic conditions for self-expression and engagement in self-governance.[422] The nonconsensual collection of people's sex toy habits or porn site searches risks undermining their willingness to engage in sexual expression.[423] People whose nude photos appear on revenge porn sites have difficulty interacting with others and often retreat from online engagement and self-expression.[424] The handling of intimate information risks self-censorship and a retreat from public debate—the result is less diverse voices in the mix.

The Supreme Court has made clear the inextricable tie between the absence of privacy protections and the chilling of self-expression. In *Bartnicki v. Vopper*, the Supreme Court observed that "the fear

419. *See* Kendrick, *supra* note 415, at 1212-13.
420. *See id.* at 1214.
421. *See id.* at 1213.
422. Citron & Richards, *supra* note 210, at 1379.
423. *See* CITRON, HATE CRIMES IN CYBERSPACE, *supra* note 23, at 195.
424. *Id.*

of public disclosure of private conversations might well have a chilling effect on private speech."[425] In *Carpenter v. United States*, the Court held that pervasive, persistent police surveillance of location information enables inferences about one's sexuality and intimate partners so as to chill "familial, political, professional, religious, and sexual associations."[426]

With the proposed reforms, people would be less fearful of engaging in sexual and gender expression or interacting with close friends and lovers. If individuals trust firms to use intimate information only for the purpose for which it was collected and no other unless they say otherwise, then they will be more willing to use those services to experiment with ideas and to share their innermost thoughts and confidences. They will be more inclined to browse sites devoted to gender experimentation and to express themselves on dating apps.

For all of these reasons, the Court has made clear that laws regulating speech about "purely private" matters do not raise the same constitutional concerns as laws restricting speech on matters of public interest.[427] As the Court explained in *Snyder v. Phelps*, speech on public matters enjoys rigorous protection "to ensure that we do not stifle public debate."[428] In contrast, speech about "purely private" matters receives "less rigorous" protection because the threat of liability would not risk chilling the "meaningful dialogue of ideas" and "robust debate of public issues."[429] Its restriction "does not pose the risk of 'a reaction of self-censorship' on matters of public import."[430] Indeed, without such restrictions, we risk self-

425. 532 U.S. 514, 533 (2001); *see also* CITRON, HATE CRIMES IN CYBERSPACE, *supra* note 23, at 208-10 (discussing the Court's recognition in *Bartnicki v. Vopper* that privacy protections foster private speech).

426. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018); *see also* Gray & Citron, *supra* note 172, at 77 (exploring the chilling effect of indiscriminate, continuous police collection of geolocation data).

427. Kenneth S. Abraham & Edward G. White, *First Amendment Imperialism and the Constitutionalization of Tort Liability*, 98 TEX. L. REV. 813, 857 (2020). As Kenneth Abraham and Edward White argue, the "all speech is free speech" view devalues the special cultural and social salience of speech about matters of public concern. *Id.* at 818-19.

428. Snyder v. Phelps, 562 U.S. 443, 461 (2011). For an extended discussion of *Snyder v. Phelps*, see CITRON, HATE CRIMES IN CYBERSPACE, *supra* note 23, at 213-15.

429. *Snyder*, 562 U.S. at 452.

430. *Id.* (quoting Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 760 (1985) (plurality opinion)).

censorship on purely private matters crucial to self-development, close relationships, and the experience of love. To illustrate a "purely private matter," the Court pointed to an individual's credit report and videos showing someone engaged in sexual activity.[431] The proposed reforms suggested here relate to purely private matters, including videos showing someone engaged in sexual activity.

The proposed reforms comport with First Amendment doctrine.[432] Rules governing the collection of information raise few, if any, First Amendment concerns.[433] These rules "prohibit[ ] information collection by separating the public sphere from the private."[434] Trespass laws, intrusion on seclusion tort claims, and video-voyeurism statutes have withstood constitutional challenge.[435] Courts have upheld laws requiring informed consent before entities can collect personal data, such as FCRA, federal and state wiretapping laws, and the Children's Online Privacy Protection Act (COPPA).[436]

Many of my reform proposals center on obtaining people's consent before firms collect or use intimate information. The Court has held "that private decisionmaking can avoid government partiality and thus insulate privacy measures from First Amendment challenge."[437] Indeed, explicit consent is part and parcel of data collection laws like FCRA, COPPA, and VPPA.[438]

As Neil Richards argues, "information collection rules ... do not fall within the scope of the First Amendment under either current First Amendment doctrine or theory."[439] Rather, such "rules are of

---

431. *Id.* at 452-53. In the latter instance, the employee's loss of public employment was constitutionally permissible because the videos shed no light on the employer's operation and instead concerned speech on purely private matters. City of San Diego v. Roe, 543 U.S. 77, 84-85 (2004) (per curiam).

432. RICHARDS, *supra* note 201, at 157.

433. Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1182 (2005).

434. *Id.*

435. RICHARDS, *supra* note 201, at 155-57. It is also worth noting that statutes prohibiting the disclosure of purely private matters like nonconsensual pornography or health data have been upheld in the face of First Amendment challenges. For an example of judicial refusal to strike down a law against nonconsensual porn, see People v. Austin, 155 N.E.3d 439 (Ill. 2019), *cert. denied*, 141 S. Ct. 233 (2020).

436. *See* Richards, *supra* note 433, at 1167-68, 1185.

437. Sorrell v. IMS Health Inc., 564 U.S. 552, 573-74 (2011) (citing Rowan v. Post Office Dep't., 397 U.S. 728 (1970)).

438. *See* Richards, *supra* note 433, at 1185.

439. *Id.* at 1186.

'general applicability,' neither discriminating against nor significantly impacting the freedoms guaranteed by the First Amendment."[440] The Supreme Court has held that even media defendants enjoy no privilege against the application of ordinary private law in their efforts to collect newsworthy information.[441]

Trespassers cannot avoid liability by contending that they infringed others' property rights in order to collect information.[442] Computer hackers cannot avoid criminal penalties by insisting that they were only trying to obtain information.[443] Websites cannot avoid responsibility under COPPA by insisting that they should not have to ask for parental consent because they need access to children's online information.[444] Employers cannot avoid liability under FCRA by arguing that they are just trying to learn about people and so should not have to ask for permission to see their credit reports.[445]

Reform proposals restricting the use of intimate information without meaningful consent would not run afoul of the First Amendment. Countless laws restrict certain uses of personal information, from state and federal antidiscrimination laws and trade secret laws to FCRA and census rules.[446] Laws restricting secondary uses of information have not been held to violate the First Amendment.[447] In *Bartnicki v. Vopper*, the Supreme Court assessed the First Amendment implications of legal prohibitions on the use or disclosure of intercepted communications.[448] The Court underscored that "the prohibition against the 'use' of the contents of an illegal interception ... [is] a regulation of conduct" whereas the prohibition of the disclosure or publication of information amounts to speech.[449]

---

440. *Id.* (quoting Cohen v. Cowles Media Co., 501 U.S. 663, 670 (1991)).

441. *Id.* at 1188 ("[I]n *Cohen v. Cowles Media*, the Court held that '[t]he press may not with impunity break and enter an office or dwelling to gather news.'" (second alteration in original) (quoting *Cohen*, 501 U.S. at 669)).

442. *See id.* at 1182.

443. *See id.* at 1185.

444. *See id.* at 1203-04.

445. *See id.* at 1191.

446. *See id.* at 1190-91.

447. *Id.* at 1194.

448. 532 U.S. 514, 517-18 (2001).

449. *Id.* at 526-27.

*Sorrell v. IMS Health*, decided in 2011, does not cast doubt on the likely constitutionality of the collection and use restrictions suggested here.[450] In *Sorrell*, the Court struck down a Vermont law banning two types of activities.[451] First, the law prohibited pharmacies, health insurers, or similar entities from disclosing doctors' prescription data for marketing purposes.[452] Second, the law prohibited pharmaceutical companies and health data brokers from using doctors' prescription data for marketing purposes unless the medical prescriber consented.[453] Data brokers and an association of pharmaceutical companies challenged the regulations on the grounds that they violated their free-speech rights.[454]

Justice Kennedy, writing for the majority, struck down the law on First Amendment grounds.[455] Under First Amendment doctrine, discrimination against particular speakers or messages—known as viewpoint-based discrimination—is "presumptively unconstitutional."[456] The *Sorrell* Court found that the law did precisely that. It held that the "law impose[d] a burden based on the content of the speech and the identity of the speaker."[457] The majority underscored that the law "imposed content- and speaker-based restrictions on the availability and use of prescriber-identifying information."[458]

As the majority found, the law told pharmacies and regulated entities that they could not sell or give away prescription data for marketing purposes but it could be sold or given away for purposes other than marketing.[459] Under the law, pharmacies could share prescriber information with academics and other private entities.[460] The Court explained, "The State has burdened a form of protected expression that it found too persuasive. At the same time, the State has left unburdened those speakers whose messages are not in accord with its own views. This the State cannot do."[461]

---

450. *See* 564 U.S. 552 (2011).
451. *Id.* at 557.
452. *Id.*
453. *Id.*
454. *Id.* at 561.
455. *Id.* at 557.
456. RICHARDS, *supra* note 201, at 80.
457. *Sorrell*, 564 U.S. at 567.
458. *Id.* at 571.
459. *Id.* at 562.
460. *Id.* at 563.
461. *Id.* at 580.

The Court found viewpoint-based discrimination in the law's targeting of specific speakers—data brokers and pharmaceutical companies—and not others.[462] As the majority noted, academic institutions could buy prescription data "in countering the messages of brand-name pharmaceutical manufacturers and in promoting the prescription of generic drugs," but pharmaceutical companies and detailers were denied the "means of purchasing, acquiring, or using prescriber-identifying information."[463]

The majority rejected the State's argument that the consent provision insulated the law's use restriction from constitutional concerns.[464] The problem was that the State gave "doctors a contrived choice: Either consent, which will allow your prescriber-identifying information to be disseminated and used without constraint; or, withhold consent, which will allow your information to be used by those speakers whose message the State supports."[465] The majority explained that privacy could be chosen only if it "acquiesce[d] in the State's goal of burdening disfavored speech by disfavored speakers."[466]

The Court held that the State failed to provide a sufficiently compelling reason to justify the law and that the State's interest was proportional to the burdens placed on speech and that the law sought to "suppress a disfavored message."[467] Moreover, the law failed to advance the interest of medical privacy, as the State claimed, given that it did not restrict the sale or use of prescriber data for countless reasons other than marketing.[468] The majority emphasized that the law allowed prescriber data "to be studied and used by all but a narrow class of disfavored speakers."[469]

Bambauer has suggested[470] that Justice Kennedy's opinion in *Sorrell* casts doubt on the constitutionality of data protection laws by recognizing that "a strong argument [exists] that prescriber-

---

462. *Id.* at 565.
463. *Id.* at 564.
464. *Id.* at 580.
465. *Id.* at 574.
466. *Id.*
467. *Id.* at 572.
468. *Id.* at 562-63.
469. *Id.* at 573.
470. *See* Bambauer, *supra* note 414, at 71 (quoting *Sorrell*, 564 U.S. at 570).

identifying information is speech for First Amendment purposes."[471] But the majority went out of its way to say that its finding did not spell the end for all privacy law. Instead, Justice Kennedy, in dictum, affirmed the constitutionality of sectoral privacy laws like the federal health privacy law.[472] He explained if Vermont had "advanced its asserted privacy interest by allowing the information's sale or disclosure in only a few narrow and well-justified circumstances" as in HIPAA, the law would have been constitutional.[473]

Neil Richards contends that the *Sorrell* holding is quite narrow. In his telling, the Court struck down the law not because it regulated data flows amounting to protected speech but because it lacked a "more coherent policy" and imposed impermissible viewpoint restrictions.[474] Richards has the better reading here. The majority explained that it had "no need to determine whether all speech hampered by [the law] is commercial" or pure speech.[475] Instead, it focused on the viewpoint discrimination—that the law sought to "suppress a disfavored message"—and the State's failure to show that the law directly advanced a substantial government interest and that the measure was drawn to achieve that interest.[476] Crucially, as Richards explains, the Court made clear that "the statute would have been less problematic if it had imposed *greater* duties of confidentiality" (as well as requirements of explicit consent and use restrictions) on the data.[477]

## CONCLUSION

This is an auspicious time to call for a new compact for sexual privacy. Dozens upon dozens of privacy bills are under consideration at the federal and state levels.[478] Privacy law reform should provide

471. *Sorrell*, 564 U.S. at 570. Jane Bambauer argues that if data is speech than privacy regulations always burden the production of knowledge. Bambauer, *supra* note 414, at 63.

472. *Sorrell*, 564 U.S. at 573.

473. *Id.*

474. RICHARDS, *supra* note 201, at 83.

475. *Sorrell*, 564 U.S. at 571.

476. *Id.* at 572.

477. Richards, *supra* note 418, at 1523.

478. Sarah Rippy, *US State Comprehensive Privacy Law Comparison*, INT'L ASS'N OF PRIV. PRO. (Mar. 22, 2021), https://iapp.org/resources/article/state-comparison-table/ [https://perma.cc/YBG3-J42K]; CONGR. RSCH. SERV., WATCHING THE WATCHERS: A COMPARISON OF PRIVACY BILLS IN THE 116TH CONGRESS 1, 3 (2020), https://crsreports.congress.gov/product/pdf/LSB/

special protections for intimate information to protect the values that sexual privacy secures and to prevent certain harms to people's well-being, including their ability to work, study, get loans, obtain insurance, and find housing. Those protections should include limitations on collection and the recognition of no-collection zones. We should widen the available remedies to include injunctive relief. This Article aims to begin the conversation about why a new compact for sexual privacy is needed and how we might go about doing that.

---

LSB10441 [https://perma.cc/GE44-XBCK].